Installation and Administration

Advanced Server for DIGITAL UNIX®

Part Number: AA-R777A-TE

December 1997

Product Version:	Advanced Server for DIGITAL UNIX Version 4.0
Operating System and Version:	DIGITAL UNIX Version 4.0A or higher
	DIGITAL UNIX Version 4.0D or higher for international support

This guide describes how to install, configure, and administer the Advanced Server for DIGITAL UNIX (ASDU) software.

Digital Equipment Corporation
Maynard, Massachusetts

© Digital Equipment Corporation 1997

All rights reserved.

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

Possession, use or copying of the software described in this publication is authorized only pursuant to a valid writing license form DIGITAL or an authorized sublicensor.

The following are third-party trademarks:

AT&T is a registered trademark of AT&T Corporation. Microsoft, MS, MS-DOS, Windows, and Windows NT either are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. OS/2 is a registered trademark of International Business Machines Corporation. PostScript is a registered trademark of Adobe Systems, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through I/Open Company, Ltd.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Restricted Rights: Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii).

Contents

About This Guide

Installation and Administration explains how to install, configure, and administer the Advanced Server for DIGITAL UNIX (ASDU) software.

Audience

This guide is intended for anyone who is responsible for the installation, configuration, and administration of the ASDU server.

Organization

The guide is organized as follows:

Chapter 1	Describes: ▪ The tasks that you must perform before installing the ASDU software. ▪ How to install the ASDU software. ▪ The tasks that you must perform after installing the ASDU software.
Chapter 2	Describes how the ASDU server is configured. It also describes ASDU registry parameters and how you modify them.
Chapter 3	Describes the administrative interfaces that you use to manage the ASDU server and environment.
Chapter 4	Describes how you configure an ASDU server in a TruCluster environment.
Chapter 5	Describes ASDU troubleshooting tools and tasks that you can perform to resolve common problems.
Appendix A	Describes the parameters in the `lanman.ini` file and how you can modify them. It also shows how earlier versions of the parameters in the `lanman.ini` file are mapped to ASDU registry keys.

Related Documentation

The following documents provide more information about the ASDU software:

- *Concepts and Planning* – Describes the concepts related to planning and administering the ASDU server and environment.
- *Release Notes* – Describes the latest information about the ASDU product that may not be documented elsewhere.

Readers's Comments

DIGITAL welcomes any comments and suggestions you have on this and other DIGITAL UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-881-0120 Attn: UBPG Publications, ZK03-3/Y32
- Internet electronic mail: `readers_comment@zk3.dec.com`
- A Reader's Comment form is located on your system in the following location:

  `/usr/doc/readers_comment.txt`

- Mail:

  Digital Equipment Corporation

  UBPG Publications Manager

  ZK03-3/Y32

  110 Spit Brook Road

  Nashua, NH 03062-9987

A Reader's Comment form is located in the back of this guide. The form is postage paid if you mail it in the United States.

Please include the following information along with your comments:

- The full title of the book and the order number.
- The section and page numbers of the information on which you are commenting.
- The version number of DIGITAL UNIX that you are using.
- If known, the type of processor that is running the DIGITAL UNIX software.

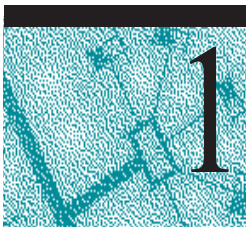
The DIGITAL UNIX Publications group cannot respond to system problems or technical support inquiries. Please address technical questions to your local system vendor or to the appropriate DIGITAL technical support office. Information provided with the software media explains how to send problem reports to DIGITAL.

Conventions

The following typographical conventions are used in this guide:

`%` `$`	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells.
`#`	A number sign represents the system prompt when you are logged in as root.
`>>>`	The console subsystem prompt is three right angle brackets.
`file`	Italic (slanted) type indicates variable values, placeholders, and function argument names.
`[ | ]` `{ | }`	In syntax definitions, brackets indicate items that are optional and braces indicate items that are required. Vertical bars separating items inside brackets or braces indicate that you choose one item from among those listed.
`. . .`	In syntax definitions, a horizontal ellipsis indicates that the preceding item can be repeated one or more times.
`cat(1)`	A cross-reference to a reference page includes the appropriate section number in parentheses. For example, cat(1) indicates that you can find information on the cat command in Section 1 of the reference pages.
`[Return]`	In an example, a key name enclosed in a box indicates that you press that key.
`[Ctrl/x]`	This symbol indicates that you hold down the first named key while pressing the key or mouse button that follows the slash. In examples, this key combination is enclosed in a box (for example, [Ctrl/C]).

CHAPTER 1



Installing the Advanced Server for DIGITAL UNIX

The Advanced Server for DIGITAL UNIX (ASDU) software provides seamless interoperability between a DIGITAL UNIX server, Windows NT servers, and Microsoft Windows clients. The ASDU software enables a DIGITAL UNIX system to run the services that make it appear as a Microsoft NT server. Microsoft users connect to the ASDU server and use DIGITAL UNIX resources without modification to their software.

Installing the ASDU software requires you to prepare the DIGITAL UNIX server, then install and configure the ASDU software.

This chapter discusses these tasks in the following sections:

- Preinstallation tasks
- Installation tasks
- Postinstallation tasks

Preinstallation Tasks

Before you install the ASDU software, you must complete the following tasks:

1. Review the ASDU documentation.
2. Ensure that the DIGITAL UNIX system on which you will install the ASDU software meets the ASDU system requirements.

Reviewing the ASDU Documentation

In addition to this document, the ASDU documentation includes product *Release Notes* and the Advanced Server for DIGITAL UNIX *Concepts and Planning* guide.

The *Release Notes* contain the latest information about the ASDU product that may not be documented elsewhere.

The Advanced Server for DIGITAL UNIX *Concepts and Planning* guide contains information that helps you plan, implement, and administer the ASDU server and domain.

These documents are located on the Associated Products Volume 2 CD-ROM and are available in hypertext markup language (HTML) format for viewing on line with a web browser and in PostScript format.

Use the instructions and examples below to locate the ASDU documentation:

1. Insert and mount in read-only mode the Associated Products Volume 2 CD-ROM:

   ```
   # mount -r  /dev/device_name /directory_name
   ```

2. Change to the mounted directory and display the directory's contents:

   ```
   # cd  /directory_name
   # ls
   ```

   The system displays the directories.

3. Change to the `/Advanced_Server` directory and display the directory's contents:

   ```
   # cd  Advanced_Server
   # ls
   ```

   The system displays the directories, which include `/doc` and `/kit`.

4. Change to the `/doc` directory and display the directory's contents:

   ```
   # cd  doc
   # ls
   ```

5. The system displays the directories. Change to the directory that contains the documentation you want, then to the directory that contains the format you want:
   - The `html` directory contains the on line format. Open the `index.htm` file in a web browser to begin veiwing the documentation on line.
   - The `ps` directory contains the PostScript format.
6. After you access the documentation, change from the mounted directory and unmount the Associated Products Volume 2 CD-ROM:

   ```
   # cd ~
   # umount /directory_name
   ```

Ensuring ASDU System Requirements

Before you install the ASDU software be sure that:

- The system on which the ASDU software will be installed is running DIGITAL UNIX Version 4.0A or later.

  Note: The system must be running DIGITAL UNIX Version 4.0D or later if the ASDU server will be configured to use international support.

- Previous PATHWORKS for DIGITAL UNIX (Advanced Server) or ASDU software subsets are removed.

  Use the instructions and examples below to remove installed Advanced Server subsets:

  1. Log in to the DIGITAL UNIX system using the `root` account and notify PC users that the Advanced Server will be unavailable.

     Display the PATHWORKS for DIGITAL UNIX (Advanced Server) subsets that are installed:

     ```
     # /usr/sbin/setld -i | grep PWK | grep installed
     ```

     Display the ASDU subsets that are installed:

     ```
     # /usr/sbin/setld -i | grep ASU | grep installed
     ```

  2. Enter the `/usr/sbin/setld -d` command followed by the name of the subset(s) that you want to remove.

     For example, to remove the ASDU subsets enter:

     ```
     # /usr/sbin/setld –d ASUADM400 ASUBASE400 ASUTRAN400
     ```

To remove the PATHWORKS for DIGITAL UNIX (Advanced Server) subsets enter:

```
# /usr/sbin/setld -d PWKBASE611 PWKDNA4611 \
PWKNBU4611 PWKRPL611 PWKTCP4611
```

Note: Do not remove the following PATHWORKS subsets if the server is running the PATHWORKS for DIGITAL UNIX (NetWare) product:

PATHWORKS Subset	**Subset Name (*nn* is the product version number)**
License Server	PWKLIC6*nn*
Reference Pages	PWKMAN6*nn*
Configuration	PWKCONFIG6*nn*
NetWare System Volume	PWKNW3SVOL6*nn*
NetWare Services	PWKNWBASE6*nn*
NetWare Transports	PWKNWTRAN46*nn*

3. Informational messages display as the subsets are removed. You may be prompted to save the following data files depending on the Advanced Server subsets that were installed:

   - User-created files located in the system ASTOOLS and PRINTLOG disk shares
   - Customized print processor scripts
   - Disk and printer share information
   - Advanced Server user account information
   - Server configuration files including `lanman.ini, lmhosts, pathworks.ini,` and various log files

You can save these data files and convert and use them to recreate the previous Advanced Server environment on the ASDU server.

Installation Tasks

You must decide which ASDU software components (subsets) to install and then run the DIGITAL UNIX installation utility, `setld`, to install the subsets from the Associated Products CD-ROM and onto the disk of a system that is running the DIGITAL UNIX software.

ASDU subsets are categorized as either core subsets or optional subsets. The ASDU server will not operate properly if the core subsets are not installed. The optional subsets provide information about and tools to manage the ASDU server; they do not affect the performance of the ASDU server.

Table 1-1describes the ASDU core subsets. Table 1-2 describes the optional ASDU subsets.

Table 1-1: ASDU Core Subsets

ASDU Core Subset	Provides	Subset Name
Base server	ASDU server functions.	ASUBASE400
Transports	The NetBEUI and NetBIOS over TCP/IP and DECnet transports that the ASDU server uses for network communications.	ASUTRAN400

Table 1-2: ASDU Optional Subsets

ASDU Optional Subset	Provides	Subset Name
Client-based Advanced Server administration tools (English)	English language version of the Nexus tools, which are Microsoft client-based utilities that are used to administer the ASDU server from a Windows PC. This subset also contains a password management utility.	ASUADM400
Client-based Advanced Server administration tools (Japanese)	Japanese language version of the Nexus tools, which are Microsoft client-based utilities that are used to administer the ASDU server from a Windows PC.	ASUADMJP400
Release notes	The latest information about the ASDU product that may impact the installation or operation of the software.	ASURNOTE400
Reference pages (English)	English language version of the reference pages that describe the ASDU commands and utilities.	ASUMANPAGE400
Reference pages (Japanese)	Japanese language version of the reference pages that describe the ASDU commands and utilities.	ASUMANJP400

Use the instructions and examples below to install the ASDU subsets:

1. Log in to the DIGITAL UNIX system using the `root` account.
2. Ensure the system is in multiuser mode.
3. Insert and mount, in read-only mode, the Associated Products CD-ROM:

   ```
   # mount -r  /dev/device_name /directory_name
   ```

4. Run the `setld` installation utility and follow the instructions on the screen:

   ```
   # setld –l /directory_name/Advanced_Server/kits
   ```

   Informational messages appear on the screen while the ASDU subsets are installed.

5. When the installation completes, change from the mounted directory and unmount the Associated Products CD-ROM.

   ```
   # cd ~
   # umount /directory_name
   ```

Postinstallation Tasks

After you install the ASDU software, you must:

1. Configure the ASDU software, which allows you to verify that the ASDU subsets were correctly installed and configured, and start the server.

You can also choose to:

2. Configure the `lmhosts` file if you choose to use an `lmhosts` file for Wide Area Network (WAN) support.
3. Load additional ASDU licenses into the License Management Facility (LMF).
4. Configure the ASDU server for international support.

Configuring the ASDU Software

You can use the `/usr/sbin/asusetup` utility to:

- Optionally configure the ASDU server into a TruCluster environment if the TruCluster software is installed on the same system.
- Convert saved PATHWORKS for DIGITAL UNIX data files for reuse.
- Provide configuration information for the ASDU server.
- Run the `asuivp` utility to verify that the ASDU subsets were correctly installed and configured.
- Start the ASDU server.

Configuring an ADSU Server for a TruCluster Environment

If the `asusetup` utility detects that the TruCluster software is installed on the system, then it assumes that you want to use it and that you already created a TruCluster disk service for the ASDU server. The `asusetup` utility prompts you for the TruCluster disk service and mount point information. If you choose not to use the TruCluster software, do not provide the information.

For More Information

For more information on configuring the ASDU server in a TruCluster environment see Chapter 4.

Converting Data Files

The `asusetup` utility determines if data files were saved from a previous PATHWORKS for DIGITAL UNIX (Advanced Server) installation. If the `asusetup` utility locates these data files, you are prompted to convert them for reuse by the ASDU server. Converting these data files restores the previous Advanced Server environment on the ASDU server. If you choose not to the convert the data files, then they are saved in the `/usr/net/servers/lanman`*`mmddyy.hhmmss`* directory and subdirectories. *`mmddyy.hhmmss`* reflects the current date.

Providing Configuration Information

To configure the ASDU server, you assign values to ASDU parameters. Most of the ASDU parameters are assigned default values, however some require administrative input when the ASDU server is first configured. The `asusetup` utility prompts you for these required values, which include:

- Network parameters that identify which transports, controllers, and methods of wide area name (WAN) resolution the ASDU server will use if systems reside in different TCP/IP subnets. If the primary domain controller (PDC) and backup domain controllers (BDCs) reside on different TCP/IP subnets, then you must configure them so that they know the TCP/IP name and address for each other by using any one or more of the following methods:
  - A domain name server (DNS) server – See your DIGITAL UNIX documentation for more information on DNS servers.
  - A WINS server – See your Windows documentation for more information on WINS servers.
  - An `lmhosts` file, which is a local file created as a result of using the `asusetup` utility if you choose to use an `lmhosts` file. See the Configuring the `lmhosts` File section later in this chapter.

- General parameters that identify the ASDU server name, domain, role in a domain, and an administrative password.

Using Default Values

The `asusetup` utility provides default values for the network and general parameters that you can use to configure the ASDU server.

If PATHWORKS for DIGITAL UNIX (Advanced Server) data files were converted or if ASDU data files were saved, then those values become the default values. If no previous data files were converted or saved, then the `asusetup` utility determines the default values as described in Table 1-3 and Table 1-4.

Table 1-3: Default Network Parameters

Parameter	Default Value
Transports	NetBEUI and NetBIOS over TCP/IP.
Controller	The default network controller.
Method of name resolution	Using a domain name server (DNS) and an `lmhosts` file, which is created as a result of the configuration.

Table 1-4: Default General Parameters

Parameter	Default Value
Server name	The name that is displayed when you enter `hostname -s` at the DIGITAL UNIX command prompt.
Server role	Primary domain controller
Domain name	The server name followed by a `.dom` extension (*`name.dom`*).
Administrative password	There is no default value for the administrative password. You are prompted to enter one. Passwords can be up to 14 alphanumeric English language characters. Passwords are case sensitive.

Using Custom Values

You can choose to provide custom values for network parameters, general parameters, or both to configure the ASDU server as described in Table 1-5 and Table 1-6.

Table 1-5: Custom Network Parameters

Parameter	The custom values can be:
Transports	Any or all of the following: ▪ NetBEUI ▪ NetBIOS over TCP/IP ▪ NetBIOS over DECnet (if DECnet is installed)
Controller	Any network controller that is configured for TCP/IP or DECnet.
Method of name resolution	Any or all of the following: ▪ The `lmhosts` file, which is created as a result of the configuration. ▪ NetBIOS name service (NBNS) (WINS Client) ▪ Domain name service (DNS)

Table 1-6: Custom General Parameters

Parameter	The custom values can be:
Server name	Up to 15 alphanumeric English language characters and the following symbols: ~ ! # $ % ^ & _ ( ) . –
Server role	Primary domain controller or backup domain controller **Note:** The primary domain controller must be the first server installed in a domain and must be up and running before you install a backup domain controller.
Domain name	Up to 15 alphanumeric English language characters and the following symbols: ~ ! # $ % ^ & _ ( ) . –
Administrative password	Up to 14 alphanumeric English language characters. Passwords are case sensitive.

Changing Configuration Values

You can reconfigure the ASDU server by running the `asusetup` utility again or by using the DIGITAL UNIX commands in Table 1-7 at the DIGITAL UNIX command prompt.

Table 1-7: Configuration Commands

Parameter	Use this command to change the value:
Server name	`/usr/sbin/setservername` **Note:** Do not edit the `ComputerName` parameter in the ASDU registry or the `listenname` parameter in the `lanman.ini` file to change the server name.
Domain	`/usr/sbin/joindomain`
Domain name	`/usr/sbin/setdomainname`
Administrative account password	`/usr/bin/net password`
Transport controllers	`/usr/sbin/ctlrsetup` **Note:** When using the `ctlrsetup` utility you must restart the transports before the changes take effect.

ASDU Directory Structure

The ASDU server on disk structure is:

`/usr/net/servers/lanman`

Beneath this directory are several subdirectories relating the ASDU server.

For More Information

For more information on configuring the ASDU server, see the Advanced Server for DIGITAL UNIX *Concepts and Planning* guide.

For more information about commands that change ASDU parameters, install the ASDU Reference Pages subset and enter `man` and the name of the command at the DIGITAL UNIX prompt.

Verifying the Installation and Configuration

The `asusetup` procedure prompts you to run the /`usr/bin/asuivp` utility to verify that the ASDU software was correctly installed and configured.

You can run the `asuivp` utility independently of the `asusetup` utility by entering /`usr/bin/asuivp` at the DIGITAL UNIX command prompt. Status messages display on the screen while the verification utility checks the ASDU subsets. If a

failure is reported, then you should remove the ASDU subsets and reinstall and configure the ASDU software as described earlier in this chapter.

If the `asuivp` utility continues to report a failure, see Chapter 5 or contact your DIGITAL representative.

For More Information

For information on the `asuivp` verification utility, install the ASDU Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
# man asuivp
```

Starting the ASDU Server

The `asusetup` procedure prompts you to start the server, which starts the ASDU processes.

ASDU servers and Microsoft servers and clients communicate by using the Server Message Block (SMB) protocol. The ASDU server receives the client's request, interprets it, and performs the DIGITAL UNIX system commands that satisfy the client's request.

To achieve efficient distribution of work and system resources, the ASDU server uses one master control program (`lmx.ctrl`), some specialized auxiliary processes (`lmx.dmn` and `lmx.repl`), and a flexible pool of client service processes (`lmx.srv`) to handle client requests. Table 1-8 describes the ASDU processes.

Table 1-8 ASDU Processes

Process	Purpose
`lmx.srv`	The `lmx.srv` is a required process that must be running. There can be multiple `lmx.srv` processes. Each `lmx.srv` process services the needs of a set of clients. The `lmx.srv` process polls for incoming SMB requests from clients and for requests from the `lmx.ctrl` process. You define the number of clients each `lmx.srv` process services.
`lmx.ctrl`	The `lmx.ctrl` is a required process that must be running. Responsibilities of the master control process include: ▪ Polling for events on the network or by other processes. ▪ Receiving instructions from the operating system. ▪ Accepting requests from new clients and passing them to `lmx.srv` process. ▪ Creating new `lmx.srv` processes as necessary.

	▪ Handling administrative actions that are not associated with a single client. ▪ Listening and routing nonguaranteed datagram broadcasts. ▪ Announcing the ASDU server's presence to the domain and retaining the announcements from other servers. ▪ Scheduling printer start and stop activity. ▪ Tracking the time of day. ▪ Reminding the `lmx.srv` process to check for autodisconnect timeouts. ▪ Coordinating transactions between client and server applications.
`lmx.dmn`	The `lmx.dmn` is a required process that must be running. Handles client log in requests.
`lmx.netrun`	Handles remote execution requests from clients.
`lmx.repl`	Provides export and import file replication services. If the server is an import server, this process listens to broadcasts from the export server and connects to the exports server when updates are needed.
`lmx.nbd`	NetBIOS daemon.
`lmx.alerter`	This process is started if the ASDU server is running the Alerter service.
`lmx.browser`	Handles browsing requests.

You can enter the following command at the DIGITAL UNIX command prompt to see what ASDU processes are running on your system:

```
# ps –ef | grep lmx
```

A report similar to the following displays the ASDU processes that are running:

```
  root   17726  1      0   12:03:36      0:00   lmx.alerter
  root   17713  17461  0   12:03:32      0:00   lmx.srv -s 1
  root   17722  17874  0   12:03:35      0:00   lmx.srv -s 2
  root   17726  1      0   12:03:36      0:01   lmx.dmn
  root   17728  1      0   12:03:36      0:01   lmx.browser
  root   17744  1      0   12:03:28      0:00   lmx.ctrl
```

This report indicates that the three required server processes are running, the netlogon daemon (`lmx.dmn`), the control process (`lmx.ctrl`), and the `lmx.srv` server processes.

Additional `lmx.srv` processes, each with a unique number at the end of the line, may be displayed as in the preceding example. The server spawns new `lmx.srv` processes based on the number of clients supported by the server. As more client sessions start, more `lmx.srv` processes may be started, each with a unique process ID and number.

Information about other processes, such as `lmx.browser` and `lmx.alerter`, may be displayed depending on the services that the ASDU server has been configured to run.

Configuring the `lmhosts` File

If you choose to use an `lmhosts` file as the method of WAN name resolution for your server, then you must edit the file to add an entry that includes the TCP/IP name and address for each system that is located on a different TCP/IP subnet with which the controller must communicate. You must add a special entry for the PDC.

The following example shows a sample `lmhosts` file where an ASDU server named Summer is the PDC in a domain called Summer.dom and the Advanced Servers called Fall, Winter, and Spring are BDCs.

```
12.100.4.13   Spring  #dom:summer.dom
12.100.5.17   Fall    #dom:summer.dom
12.100.5.36   Winter  #dom:summer.dom
12.100.5.42   Summer  #dom:summer.dom
12.100.5.42   “summer.dom     \0x1b”# Entry for the PDC
```

Note that the format for the entry that identifies the domain is padded with extra spaces to fill 15 characters, which is the maximum length for domain name. In the previous example `summer.dom` is 10 characters, followed by 5 spaces, followed by `\0x1b` all within quotes.

Loading ASDU Licenses

The ASDU server must have an available ASDU license before a client can access domain resources offered by the server.

ASDU licenses are provided as product authorization keys (PAKs) that you load into the DIGITAL UNIX License Manager Facility (LMF). After being loaded into LMF, the ASDU licenses are managed by the ASDU server.

A client uses an ASDU license from each ASDU server to which it connects. The client retains the license until all its connections to the server are terminated at which time the license is free to be reassigned.

ASDU licenses are assigned on an as-requested basis and cannot be reserved for a particular user or client. If all licenses are assigned, then no other clients can connect to that ASDU server until a license becomes available.

Provided with the ASDU software is a complimentary two-user ASDU PAK that can be used by two clients after the ASDU software has been successfully installed and configured. Because these licenses are provided with the ASDU software, they are readily available and do not need to be loaded into LMF.

Use one of the following methods to learn about the status of ASDU licenses:

- To show what license a client has and to list the number of licenses available, enter the following command at the DIGITAL UNIX command prompt:

  ```
  # /usr/sbin/lmstat –L
  ```

- To list the client names and the type of license each client has, enter the following command at the DIGITAL UNIX command prompt:

  ```
  # /usr/sbin/lmstat –c
  ```

  A license type of zero indicates that a license has not been issued to a client that is performing a system service. For example, a license would not be assigned if a client were browsing the server.

- To view the system event log to show if a client was issued or denied a license, enter the following command at the DIGITAL UNIX command prompt:

  ```
  # /usr/sbin/elfread –d system | more
  ```

For More Information

The ASDU server accepts PATHWORKS licenses. See the ASDU *Release Notes* for information on which PATHWORKS licenses the ASDU server accepts.

For information on the `lmstat` command, install the ASDU Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
# man lmstat
```

For information on `lmf`, install the DIGITAL UNIX Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
# man lmf
```

Configuring International Support

Follow these steps to configure the ADSU server to use a language other than English when providing file, directory, share, user, and group names to clients:

1. Ensure that the system is running DIGITAL UNIX Version 4.0D or later.

2. Install and configure the ASDU software as described earlier in this chapter. However do not start the ASDU server when prompted by the `asusetup` utility.

3. Use a text editor and set the `lang` parameter in the `lmxserver` section of the `lanman.ini` file. If the `lang` parameter does not exist, then enter it under the `lmxserver` section.

   The `lang` parameter sets the character set and locale that the ASDU server uses to communicate. For example, if the PC clients are running the French edition of Windows, then you can configure the ASDU server to correspond in French by setting the `lang` parameter to fr_FR.ISO8859-1, which is the DIGITAL UNIX French locale, in the `lanaman.ini` file as follows:

   ```
   [lmxserver]

     lang=fr_FR.ISO8859-1
   ```

   The ASDU server supports all of the DIGITAL UNIX locales listed in the `l10n_intro` reference page except for Korean, Japanese SJIS, and Traditional Chinese. For information on the supported locales, install the DIGITAL UNIX Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

   ```
   # man l10n_intro
   ```

4. Install the Unicode support for the locale. The Unicode support includes codeset converters that the ASDU server uses to convert names between the PC and DIGITAL UNIX character set. The Unicode support is in the DIGITAL UNIX Worldwide subsets. For information on installing codeset subsets, see the Worldwide Installation chapter in the DIGITAL UNIX *Installation* guide.

5. Start the ASDU server by entering the following command at the DIGITAL UNIX command prompt:

   ```
   # net start server
   ```

CHAPTER 2

Configuring the ASDU Server

You configure the ASDU server by assigning values to entries in keys that are stored in a central database called the registry. You assign some of these values when the ASDU server is first configured. However, most of the entries are assigned default values.

This chapter discusses the ASDU server configuration default values for registry entries in the following sections:

- Registry Structure
- Default Environment
- Registry Keys and Values
- Registry Administrative Interfaces

The ASDU registry largely replaces the `lanman.ini` configuration file, which was used to configure the PATHWORKS product. For information about the ASDU parameters that are stored in the `lanman.ini` file and how `lanman.ini` file parameters are mapped to ASDU registry keys, see Appendix A, The `lanman.ini` File.

Registry Structure

The ASDU registry is the foundation for system administration of the ASDU server. The ASDU registry is a database, organized in a hierarchical structure that contains configuration information about the ASDU server and the environment. The registry is composed of subtrees and their keys, and value entries. A key can contain subkeys.

Table 2-1 identifies and defines the ASDU registry subtrees.

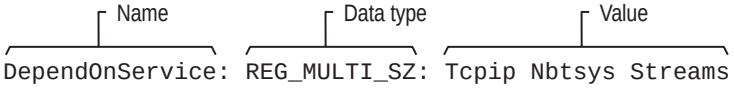
Table 2-1: Registry Subtree

Subtree	Contains
HKEY_LOCAL_MACHINE	Parameters that configure the local computer system, including hardware and operating system data such as bus type, system memory, device drivers, and startup control data.
HKEY_USERS	Parameters that configure a user's profile and the default profile. Users who access a server remotely and do not have profiles under this subtree on the server use the profiles that are loaded into the registry on their own computers.

Each registry key entry contains data items called value entries. A value entry has three parts:

- The name of the entry
- The data type of the entry
- The value for the entry, which can be data of any length.

The three parts of a value entry always appear in the following order:



The ASDU registry is stored in the `/usr/net/servers/lanman/datafiles` directory.

Table 2-2 lists and defines the data types currently used by the system.

Table 2-2: Registry Data Types

Data Type	Description
REG_BINARY	Binary data. For example: `Component Information : REG_BINARY : 00 00 00...`
REG_DWORD	Data represented by a number that is 4 bytes long. Many keys for device drivers and services are this type and can be displayed in the registry editor in binary, hexadecimal, or decimal format. For example, entries for service error controls are this type: `ErrorControl : REG_DWORD : 0x1`
REG_EXPAND_SZ	An expandable data string, which is text that contains a variable to be replaced when called by an application. For example, in the following value, the string *%SystemRoot%* will be replaced by the actual location of the directory containing the ASDU system files: `File : REG_EXPAND_SZ : %SystemRoot%\file.exe`
REG_MULTI_SZ	A multiple string. Values that contain lists or multiple values in readable text are usually this type. Entries are separated by NULL characters. `AlertNames : REG_MULTI_SZ : Administrator tom`
REG_SZ	A sequence of characters representing readable text. For example, a component's description is usually this type: `DisplayName : REG_SZ : Alerter`

Default Environment

The ASDU server is configured with default values for registry entries that you can change at any time. The following sections describe the default values for some of the entries that are used to configure the ASDU server.

Domain User Accounts

Each user who participates in a domain must have a domain user account that identifies the user to the ASDU server. A domain user account contains information about the user including name, password, and optional entries that determine when the user can log in and how their desktop settings are stored.

You can control user access to domain resources by granting or denying permission for a user's domain user account to access a resource.

Default Domain User Accounts

Table 2-3 describes the domain user accounts that are automatically created when you install the ASDU server.

Table 2-3 Default Domain User Accounts

Account	Purpose
Administrator	You use this account initially to administer the server and domain and to create user accounts.
Guest	This account allows users without accounts in the domain or in a trusted domain to log on to the network. This account is disabled by default.

To ease administration, domain users who have similar needs can be grouped together and administered as one group.

Table 2-4 describes the ASDU groups that are automatically created when you install the ASDU server.

Table 2-4: Default Domain Groups

Group	Purpose
Domain Admins	Members of this group can administer the domain, servers, and workstations in the domain and in a trusting domain that has added the Domain Admins global group from this domain to the local Administrators group. However, members of the Domain Admins group do not automatically gain administrative privileges in other domains when a trust relation is established.
Domain Users	Members of this group have normal user access to and capabilities for the domain and the computers in the domain running Windows NT software.
Domain Guests	Members of this group have less access and fewer rights than users in the Domain Users group.

Creating New Domain User Accounts

When you create a domain user account it is associated with a DIGITAL UNIX user account. The `ForceUniqueUserAccount` entry is set so that if a DIGITAL UNIX account exists with the same user name as the domain user account, then the two accounts are associated. The `CreateUnixUser` entry is set so that if a DIGITAL UNIX account does not exist with the same user name, then it is

automatically created (using lowercase letters) and associated with the user's domain user account. You can use the `/usr/sbin/mapuname` command at the DIGITAL UNIX command prompt to change the mapping between a domain user account and a DIGITAL UNIX user account.

The `NewUserShell` entry is set so that each DIGITAL UNIX account that you create is assigned a `/bin/sh` login shell. This shell enables the user to use a terminal emulation application to interactively log in to the server once you set the password for the user's DIGITAL UNIX account. In the case of an upgrade, the default user shell is specified by the `newusershell` parameter in the `lmxserver` section of the `lanman.ini` file.

Domain user account names can contain up to 20 characters, however the maximum number of characters for a DIGITAL UNIX user account is 8. If a domain user account name exceeds 8 characters, then the associated DIGITAL UNIX user account uses the first 6 characters (in lowercase) and substitutes special characters for the last 2 characters. The user uses this shorter name to log in to the DIGITAL UNIX server. For example, if a domain user account name is `longusername`, then the DIGITAL UNIX account (in the `/etc/passwd` file) might be `longush3`, and the user uses `longush3` to log in to the DIGITAL UNIX server.

For More Information

For information on domain user accounts and groups, see Chapter 3 in the Advanced Server for DIGITAL UNIX *Concepts and Planning* guide.

For more information on user-related configuration entries, see the User Service Parameters section later in this chapter.

For more information on the `mapuname` command, install the ASDU Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
# man mapuname
```

Disk Shares

You can share any of the following DIGITAL UNIX file systems with Microsoft users as disk shares:

- POLYCENTER Advanced File System (AdvFS)
- UNIX File System (UFS)
- Network File System (NFS)
- CDROM File System (CDFS), read only

Default Disk Share

Table 2-5 lists the special disk shares that are automatically created when you installed the ASDU server. The list may differ depending on the subsets that are installed. Do not remove or modify these shares.

Table 2-5: Default Disk Shares

Name of Disk Share	Contains
ADMIN$	Administrative utilities for remote administration
IPC$	Named pipes that are used for communication with the server
C$	The directories and files that are located on the `root` file system
D$	Files and libraries that are required by MS-DOS, OS/2, and Windows NT computers
PRINT$	Printer drivers
ASTOOLS	Microsoft client-based utilities that are used to administer the ASDU server from a Microsoft client
DOSUTIL	MS-DOS administrative commands including: `clipcach`, `clispool`, `uchmod`, `ud`, `udir`, and `uren`
NETLOGON	Logon scripts
OS2UTIL	OS/2 administrative commands including: `uchmod`, `ud`, `udir`, and `uren`
PRINTLOG	LP printer messages
USERS	Users home directories, which by default is the `/usr/users` directory

Disk shares with names ending with a dollar sign ($) are hidden and do not display when the server is browsed. You can connect to a hidden share if you specify the share name as follows:

`\\`*`servername`*`\`*`sharename$`*

For More Information

For information on disk shares, see Chapter 5 in the Advanced Server for DIGITAL UNIX *Concepts and Planning* guide.

Creating Disk Shares for Users

The HomeDirectoryAccess entry is set so that if one does not exist, a DIGITAL UNIX directory is created for each user when you create their domain user account. The ASDU server creates the users' home directory in the path specified by the UserPath entry, which by default is the /usr/users directory. The directory is created by using the user's name or the shortened name if applicable. Each user is granted full access (RWCXDAP) permission to their DIGITAL UNIX directory.

By default, the /usr/users directory is offered as the USERS special disk share. This means that you do not need to create individual disk shares for each user. A users' home directory is available as a subdirectory in the USERS disk share. If you use a directory other than /usr/users for the users' home directories, then you may want to modify the USERS disk share and redirect it to the new location.

Users connect to the *server*\USERS disk share from their Windows PC and navigate to their directory. Users can view all of the user directories but have permission to access only their own directory.

For More Information

For more information on the HomeDirectoryAccess entry, see the File Service Parameters section later in this chapter.

For more information on the UserPath entry see the Lanman Server Parameters section later in this chapter.

Securing Disk Shares

By default, the IgnoreUnixPermissions entry is set so that both DIGITAL UNIX and ASDU access permissions are checked when a user accesses directories and files on the server. Together, these permissions determine whether a user can read, write, or create directories and files on the server. However, the DIGITAL UNIX system access permissions can prevent a user's access to a file or directory even if ASDU access permissions grant access.

For example, if a user has ASDU change permission for a file, then this file must have the DIGITAL UNIX system equivalent of change permission (RWXCD) in order for the user to perform the operations allowed by the ASDU server change permission (read, write, create, and execute).

If you change the file's DIGITAL UNIX system permissions to eliminate write (W) permission for everyone other than the file's owner, then no one but the owner can alter or remove the file, regardless of the ASDU permissions.

By default, the UnixFilePerms entry is set to read and write permission for the owner and group, and read only for the world when files are created on the server from a Microsoft client.

By default, the `UnixDirectoryPerms` entry is set to read, write, and execute permission for the owner and group, and read and execute for the world when directories are created on the server from a Microsoft client.

Table 2-6 describes how to change DIGITAL UNIX and ASDU access permissions for a disk share.

Table 2-6: How to Change Permissions

From:	Change ASDU access permissions by using:	Change DIGITAL UNIX access permissions by using:
A Microsoft Client	Windows Explorer or the `attrib` command at the MS-DOS prompt.	The `uchmod` and `udir` commands, which are located on the server in the `dosutil` and the `os2util` disk shares.
The DIGITAL UNIX command prompt	The `net access perms` command.	The `chmod` command.

For More Information

For more information on ASDU disk share permissions, see Chapter 5 in the Advanced Server for DIGITAL UNIX *Concepts and Planning* guide.

For more information on the disk share configuration entries, see the File Service Parameters section later in this chapter.

For more information on the DIGITAL UNIX directory and file permissions, install the DIGITAL UNIX References Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
# man chmod
```

For more information on the `uchmod` command, connect to the `dosutil` or `os2util` disk share, depending on the client type you are connecting from, and enter `uchmod` at the command prompt.

More Information on the `udir` Command

The `udir` utility is located on the server in the `dosutil` disk share and is executed from a Windows client. It displays DIGITAL UNIX user, owner, and group system access permissions as described in following table:

Permission	Description
r	Permission to display or read the file or directory.
w	Permission to modify or write to the file or to create or remove files.

x	Permission to execute the file or move to the directory. Client applications do not need execute permission since they execute on the client computer's operating system, not the DIGITAL UNIX system.
-	The specified permission is denied.
l	Mandatory locking is enabled.
s	Regardless of who executes a file with this permission the invoked process takes on the identity of the file's owner (or group) for the duration of the execution.

Automatically Sharing Disk Shares

By default, the `ShareNFSExports` entry is set so that if you use the Network File System (NFS) to share DIGITAL UNIX file systems with DIGITAL UNIX users, you can use the `nfsshare` utility to share those file systems as disk shares with Windows users. The `SyncNFSExports` entry is set to synchronize NFS exports with disk shares each time that the ASDU server starts. Note that NFS exports are not shared with Microsoft users if the `IgnoreUnixPermission` entry is enabled.

By default, the `NFSExportFile` entry defines the `/etc/exports` file. The `nfsshare` utility creates a disk share for each entry in the file by using the following characteristics:

- Name – The name of the exported file system or subdirectory.
- Remark – "NFS Export".
- Path – The path identified for a resource in the `/etc/exports` file is converted to DOS style and preceded with C:.

  For example, if the `/etc/exports` entry is `/home/nfs/usr/src` then the ASDU server uses the `home\nfs\usr\src` path.

  If a disk share exists with the same name as the exported resource but with a different path, then a new disk share is created with an underscore (_) followed by numeric counter appended to the disk share name. For example, if the entry in the `/etc/exports` file is `/home/nfs/usr/src` and a disk share called `src` exists but with a different path, then a disk share with the path of `C:\home\nfs\usr\src_0` is created.

  If a disk share exists with the same name and path as the exported resource then no new disk share is created.
- Number of users that can access the share – No Limit.

Export file entries may have identifiers that define the permission a remote host has when exporting the file system or directory. Table 2-7 describes how the NFS permissions are converted to disk share permissions.

Table 2-7: NFS to Disk Share Permissions

If the NFS permission is:	Then the disk share permission is:
Read (r) and write (w)	Full access
Not specified	Full access
Read only (ro)	Read and execute
None	No access

Table 2-8 provides examples of how the `nfsshare` utility converts NFS permissions to disk share permissions.

Table 2-8: Converting Permissions

If the type of entry in the /etc/exports file is:	The Disk share permission is:
`/usr/local`	Full access for all clients
`/user/local –ro client1`	Read and execute for client1 and no access for all other clients
`/usr/local client1 client2 client3`	Full access for client1, client2, and client3 and no access for all other clients
`/usr/local –rw=client1`	Full access for client1 and read and execute for all other clients
`/usr/local –access=client1:16.20.20.1`	Full access for client1 and 16.20.20.1 and no access for all other clients

The ASDU server does not support the following types of exported entries:

- `/usr/local –root=0 client1`
- `/usr/local –root=client1`
- `/usr/local –anon=0`
- Entries that contain NIS netgroups names

For More Information

For information on the `nfsshare` utility, install the ASDU Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
# man nfsshare
```

Printer Shares

The `ShowUnixQueue` entry is set so Microsoft users can view the printer queues that were created by the ASDU server and the default `osfqueue` queue, which displays all print jobs not submitted through the ASDU server. Users cannot view all of the DIGITAL UNIX printer queues.

DIGITAL UNIX printer queues are not automatically created as ASDU printer shares. To create an ASDU print share you must check the `/etc/printcap` file to be sure that the DIGITAL UNIX operating system recognizes the printer. If an entry does not exist in the `/etc/printcap` file for the printer, then use the `lprsetup` utility. The `lprsetup` utility prompts you for information about the printer, creates a spool directory, links the output filter, and adds an entry in the `/etc/printcap` file for the printer.

Once an entry for the printer is in the `/etc/printcap` file, you can create a printer share for it by using Windows NT utility or by using a `net` command:

- To create a printer share from Windows NT, either browse the Network Neighborhood or by use the `Run` or `Find` option from the `Start` button to locate and double click on the ASDU server on which you want to create the printer share. A window is displayed listing the disk shares and a Printers folder. Double click on the Printers folder. Click on the Add Printer icon and follow the instructions on the screen.
- Enter the following `net` command:

  `net share` *`printersharename=printername`* `/print`

You can create printer shares for printers that are connected to Microsoft clients by using the `asduclient` command. After the client's printer is configured as a printer share, it can print jobs that are sent from any type of user.

For More Information

For more information on ASDU printer shares, see Chapter 6 in the Advanced Server for DIGITAL UNIX *Concepts and Planning* guide.

For more information on creating a printer shares for a client printer, install the ASDU reference page subset and enter the following command:

```
# man asduclient
```

For more information on the printing configuration entries, see the Parameters section later in this chapter.

Registry Keys and Values

As the ASDU server administrator, you should be familiar with the registry key descriptions in this section.

The ASDU registry keys described in this chapter are defined in subkeys located in the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

\AdvancedServer

\Alerter

\Browser

\EventLog

\LanmanServer

\Netlogon

\Netrun

\Replicator

\UPS
```

Advanced Server Parameters

The advanced server subkey of the ASDU registry contains the following subkeys:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
AdvancedServer

  \AlertParameters

  \FileServiceParameters

  \NetAdminParameters

  \Parameters

  \ProcessParameters

  \RpcParameters

  \ShareParameters
```

`\UnixAuditParameters`

`\UserServiceParameters`

The following sections describe the entries contained within advanced server subkey.

Alerter Parameters

The registry path that contains entries for the ASDU alerter service is as follows:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdvancedServer\AlertParameters`

`AlertAdminOnLicenseOverflow` `REG_DWORD` *0 or 1*

Specifies whether the server sends an administrative alert message when the maximum allowable number of clients is exceeded.

Default: 0 (message will not be sent)

`AlertUserOnLicenseOverflow` `REG_DWORD` *0 or 1*

Specifies whether the server sends a message to a client that tries to link but failed when the maximum allowable number of clients is exceeded.

Default: 0 (message will not be sent)

File Service Parameters

The registry path that contains entries for the ASDU file service is as follows:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdvancedServer\FileServiceParameters`

`AclCacheSize` `REG_DWORD` *0 - 100*

Specifies the number of entries in ACL cache, which tracks the results of recent access checks performed on ASDU resources.

Default: 6

`EAFilePrefix` `REG_SZ` *Character string*

Specifies the prefix used to name files containing extended attribute data. For example, by default, the extended attributes for file *foo* are stored in `.ea@foo`.

Default: `.ea@`

`EnableSoftCompat` `REG_DWORD` *0, 1, or 2*

Specifies how the ASDU server handles file opens in read-only compatibility mode.

Number:	Meaning:
0	Keep the compatibility mode.
1	Translate to read-only/DenyWrite mode for files with special extensions (for example, .EXE, .COM, and .BAT) specified by the value of the `EnableSoftFileExtensions` key.
2	Translate to read-only/DenyWrite mode for all file opens.

Default: 2 (translate file opens to read-only/DenyWrite mode)

`EnableSoftFileExtensions` `REG_MULTI_SZ` *List*

Specifies the file extensions for which the compatibility mode is translated to read-only/DenyWrite when the value of the EnableSoftCompat key is set to 1.

Default: bat com exe dll cmd

`ForceDirectoryAcl` `REG_DWORD` *0 or 1*

Determines whether the ASDU server creates an access control list for a newly-created directory if an explicit access control list is not provided by the client computer. If an access control list is not created, one is inherited from its parent directory whenever it is needed.

Default: 1 (create new access control list)

`ForceFileAcl` `REG_DWORD` *0 or 1*

Determines whether the ASDU server creates an access control list for a newly-created file if an explicit access control list was not provided by the client computer. If an access control list is not created, one is inherited from its parent directory whenever it is needed.

Default: 0 (will not create new access control list)

`ForceFileFlush` `REG_DWORD` *0 or 1*

Specifies whether to force a DIGITAL UNIX `fsync(2)` system call when an SMB flush request is received. Not forcing `fsync(2)` system call improves file server performance; files are periodically flushed to disk by the DIGITAL UNIX `fsflush` daemon, regardless of the key setting.

Default: 0 (will not force fsync system call)

`HomeDirectoryAccess` `REG_DWORD` *0 or 1*

Specifies whether or not to add a full access (RWCXDAP) record on the user's DIGITAL UNIX home directory when their domain user account is created.

Default: 1 (add access record)

`IgnoreUnixPermissions` `REG_DWORD` *0 or 1*

Specifies to ignore DIGITAL UNIX permissions and enforce only ASDU permissions when Microsoft users access DIGITAL UNIX files and directories. Regardless of how this key is set, users are denied access when they attempt to write to a file or directory that has the DIGITAL UNIX read-only permission.

Note: NFS exported directories cannot automatically be made available as disk shares if this key is enabled.

Default: 0 (enforce DIGITAL UNIX permissions)

`MappingSeparator` `REG_SZ` *Character string up to 7 characters*

Specifies the string that is appended to the file name before its unique suffix to indicate that the name is mapped. This value matters only when mapping file names from DIGITAL UNIX to Windows NT. The default is a tilde (~), the same as in DIGITAL UNIX system to 8.3 file name mapping, but it is possible to set it to enable the client to easily identify files containing characters illegal in Windows NT. By default, a file named "my?" is mapped to "my_~xyz." When the value of this key is set to "~asu~", the name is mapped to "my_~asu~xyz". If an invalid parameter is placed in the registry, the MappingSeparator is replaced by the default value.

Default: ~

`MaxEASize` `REG_DWORD` *1 - infinity*

Specifies the buffer size in bytes that is allocated for extended attributes.

Default: 4096 bytes

`MaxFileSizeInKB` `REG_DWORD` *100 - infinity*

The maximum file size, in KBytes, that a user can create on an ASDU server.

Default: 0xffffffff Kbytes

`MaxZeroFillinInKB` `REG_DWORD` *0 - infinity*

The maximum number of bytes in units of Kbytes that are filled with zeros when initializing a file.

Default: 50000

`MemoryMapFiles` `REG_DWORD` *0 or 1*

Specifies whether the server uses the DIGITAL UNIX `mmap` system call to memory map file data into the server's address space for efficiency. File mapping is attempted only for read-only files.

Default: 1 (memory map read-only files)

`MixedCaseSupport` `REG_DWORD` *0 or 1*

Specifies whether mixed-case support is enabled on the server. Mixed-case support allows clients to access file names containing uppercase characters on the DIGITAL UNIX system. Enabling mixed-case support may negatively affect the server's performance.

Default: 1 (enable mixed-case support)

`NameSpaceMapping` `REG_DWORD` *0, 1, 2, or 3*

Specifies the type of file name space mapping enabled on the server:

0 – Indicates that there is no name space mapping enabled.

1 – Specifies that only DIGITAL UNIX system to 8.3 mapping is enabled. This allows 8.3-style clients, such as MS-DOS, Windows 3.1, and Windows for Workgroups, to access files with long file names and file names containing characters that are invalid in DOS: (+ , ; = [ ] ? " \ < > * | : . [space])

2 – Specifies that only DIGITAL UNIX system to Windows NT mapping is enabled. This allows Windows NT-style clients, such as Windows 95, Windows NT, and OS/2, to access files with file names containing characters that are illegal in Windows NT: (? " \ < > * | :).

3 – Specifies that both DIGITAL UNIX system to 8.3 and DIGITAL UNIX system to Windows NT mappings are enabled.

Default: 3

`NFSExportFile` `REG_SZ` *Character string*

Specifies the name of the NFS export file.

Default: `/etc/exports`

`OplockTimeout` `REG_DWORD` *1 - infinity*

The interval of time, in seconds, that the server waits for acknowledgment from a client of an `oplock` broken notification.

Default: 30 seconds

`ReadAheadCount` `REG_DWORD` *0 - infinity*

The number of sequential file accesses by a client that the server must detect before it begins reading ahead. A value of zero (0) means to always read ahead.

Default: 2 (sequential file access)

`ReportNTFS` `REG_DWORD` *0 or 1*

Specifies whether to report share DIGITAL UNIX system volumes as NTFS or the DIGITAL UNIX file system type.

Default: 1 (report as NTFS)

`RootOwnsFilesCreatedOnNFS` `REG_DWORD` *0 or 1*

Specifies whether files on NFS are owned by root or user.

Default: 0 (files are owned by the user's DIGITAL UNIX user ID)

`ShareNFSExports` `REG_DWORD` *0 or 1*

Determines whether disk shares are created for resources exported through NFS.

Default: 1 (enable sharing)

`SyncAclFileOnWrite` `REG_DWORD` *0 or 1*

Determines whether the server will force changes to the access control list (ACL) file to be written to disk using an `fsync(2)` system call or whether the server normally permits the operating system to write the changes to disk.

Default: 0 (write ACL changes to disk normally)

`SyncNFSExports` `REG_DWORD` *0 or 1*

Determines whether the server will synchronize NFS exports with disk shares when the ASDU server starts. If this entry is disabled, then all disk shares that were created from the NFS exports are deleted, and new disk shares are recreated from the NFS exports.

Default: 1 (synchronize at ASDU server startup)

`TruncatedExtensions` `REG_DWORD` *0 or 1*

Specifies whether to replace the last character of the file extension of a mapped file name with a tilde (~). This key applies to file extensions longer than 3 characters. This feature can be used to distinguish longer file extensions from similar 3-character extensions that were unchanged. For example, enabling this feature prevents a file named *`file1.document`* from being mapped to a file named *`file~xyz.doc`* which could cause some clients to consider this file a Microsoft Word file. (This key affects only DIGITAL UNIX system to 8.3 file mapping.)

Default: 1 (do not replace last character with a tilde)

`UniqueSuffixLength` `REG_DWORD` *0 to 7*

Specifies the length of the alpha-numeric suffix appended to the file name to guarantee mapping uniqueness. The longer the suffix, the higher the probability that the mapped name is unique. If the mapped name is not unique within a directory, name collisions may occur causing the client to be denied access to the file it needs, or giving access to a different file from the one requested.

It is not advisable to set UniqueSuffixLength to a value less than 3, unless the preservation of a longer file name prefix outweighs possible name collision problems.

Default: 3 characters

`UnixCloseCount` `REG_DWORD` *1 - 20*

The number of least recently accessed open files that the server closes transparently to avoid reaching the DIGITAL UNIX system's per-process limit. The server uses file descriptor multiplexing to allow clients to open more files than the per-process limits normally allows.

Default: 5 files

`UnixDirectoryCheck` `REG_DWORD` *0, 1, or 2*

Specifies whether the ASDU server allows clients to write to DIGITAL UNIX system directories without write permission. Microsoft client software treats the read-only attribute as advisory and does not limit the behavior of directories. In contrast, the DIGITAL UNIX system treats read-only permissions as mandatory and prohibits users from writing in directories for which they do not have write permission.

0 – Allows writing only to directories with write permissions.

1 – Allows writing to directories owned or created by the ASDU server (as determined by checking group memberships of the directory).

2 – Ignores DIGITAL UNIX system directory permissions.

Default: 1 (allow writing to directories owned or created by the ASDU server)

`UnixDirectoryPerms` `REG_DWORD` *0 - 511*

Specifies the DIGITAL UNIX system permissions for newly-created directories.

Default: 509 (0775 octal)

`UnixFilePerms` `REG_DWORD` *0 - 4095*

Specifies the DIGITAL UNIX system permissions for newly-created files.

Default: 1460 (02664 octal)

`UnixQuotas` `REG_DWORD` *0 or 1*

Specifies whether the ASDU server provides DIGITAL UNIX system disk quota support. This support ensures that creating or writing to the file is performed under the DIGITAL UNIX system UID of the DIGITAL UNIX system user to which the ASDU user is mapped. Each action counts toward that user's quota; an error message is sent to the client when the quota is exceeded. Two quotas are supported: i-node and block quotas for UFS and NFS file systems.

Default: 0 (no support for disk quotas)

`UseEAs` `REG_DWORD` *0 or 1*

Specifies support for OS/2 extended attributes.

Default: 0 (no support for extended attributes)

`UseNfsLocks` `REG_DWORD` *0 or 1*

Specifies whether the server tries to set DIGITAL UNIX system record locks in files as requested by clients. Record locks may not work on NFS files on a server running NFS. If the value of the `UseUnixLocks` key is zero, this feature has no effect on the server.

Default: 0 (do not set locks)

`UseOplocks` `REG_DWORD` *0 or 1*

Specifies whether the ASDU server grants opportunistic locks to clients that request them on file opens.

Default: 1 (use opportunistic locks)

`UseUnixGroups` `REG_DWORD` *0 or 1*

Specifies whether or not the ASDU server uses the DIGITAL UNIX group field to store MS-DOS file and directory attributes. Enabling this key enhances security by enforcing DIGITAL UNIX group permissions, and causes the MS-DOS Archive, Hidden, and System attributes to be ignored by the server.

Default: 0 (do not use the DIGITAL UNIX group field)

`UseUnixLocks` `REG_DWORD` *0 or 1*

Specifies whether record locks created by clients are reflected in the DIGITAL UNIX file system.

Default: 1 (locks are reflected in DIGITAL UNIX file system)

`WriteBehind` `REG_DWORD` *0 or 1*

Specifies whether the DIGITAL UNIX system performs writes before or after the server responds to the client. If the DIGITAL UNIX system performs writes before the server responds to the client, then the server can report disk full errors to clients. The server appears to be slower because the response is delayed. If the DIGITAL UNIX system performs writes after the response is sent, disk full errors during write server message blocks (SMBs) are not reported to the client.

Default: 1 (enable write behind)

Net Administration Parameters

The registry path that contains entries for the ASDU net administration is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
AdvancedServer\NetAdminParameters
```

`NetAdminGroupName` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX system group name assigned to the network administration `\\servername /c` command.

Default: `DOS----`

`NetAdminPath` `REG_SZ` *Character string up to 256 characters*

Specifies the DIGITAL UNIX system path used to find commands submitted by the network administration `\\servername /c` command.

Default: `/usr/net/servers/lanman/bin:/bin:/usr/bin`

`NetAdminUserName` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX system user account name assigned to a process executed by the network administration `\\servername /c` command.

Default: `lmxadmin`

Parameters

The registry path that contains entries for the ASDU parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
AdvancedServer\Parameters
```

`CheckPrintQueueInMinutes` `REG_DWORD` *1 - infinity*

Specifies the interval in minutes at which the server determines whether to start a printer queue.

Default: 10 minutes

`DefaultPrintQueue` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX queue name that displays for locally submitted jobs when the `ShowUnixQueues` key is set to zero (0).

Default: `OSFqueue`

`DisableUpLevelPrinting` `REG_DWORD` *0 or 1*

Specifies whether to disable or enable Windows NT-style printing. If you chose to disable Windows NT-style printing during an upgrade procedure by setting this value to 1, then you can enable this feature by changing this value to zero (0).

Default: 0 (enables Windows NT-style of printing)

`MaxDirectoryBufferSize` `REG_DWORD` *1 - infinity*

Specifies the maximum buffer size that the server uses for a `getdents(2)` system call to read the contents of a DIGITAL UNIX system directory. Because the ASDU server attempts to allocate these buffers using the GC memory allocator, you should consider increasing the `SizeGcBufferPoolInKB` key if you increase this value.

Default: 32768 bytes

`MaxIpcTryCount` `REG_DWORD` *1 - infinity*

Specifies the number of `read()` system calls after which the server checks to see if other work can be done by the server. There is a considerable amount of interprocess communication (IPC) between server processes. The server uses the `read` system call to receive IPC messages, but the `read` system call does not always return the entire message. This key ensures that the server does not keep trying to get an IPC message at the expense of other process activities.

Default: 20 (`read` ( ) calls)

`MaxMailslotReadTime` `REG_DWORD` *1 - infinity*

Specifies the amount of time in seconds to wait for a local mailslot application to read a class 1 mailslot. Setting this value prevents the server from waiting indefinitely for a message to be delivered.

Default: 90 seconds

`MaxMessageSize` `REG_DWORD` *1024 - infinity*

Specifies the maximum amount of data that a client can exchange with the server per message.

Default: 4156 bytes

`MaxPrintQueueNameLength` `REG_DWORD` *1 - 255*

Provides dynamic control of the allowable length of the name of a printer queue. LP subsystem commands currently allow class names of up to 255 characters, but jobs sent to these classes cannot be controlled; many DIGITAL UNIX system commands used to manipulate these jobs result in a fatal error. Printer queue functions use this key to restrict access to queues based on the length of the queue name.

Default: 14 characters

`MaxRawSize` `REG_DWORD` *8192 - infinity*

Specifies the maximum size, in bytes, of the raw send or receive buffers that the ASDU server uses to process Read Block Raw, Write Block Raw, Transaction, Transaction 2, or NT Transaction server message blocks (SMBs).

Default: 32768 bytes

`MaxServiceWaitTime` `REG_DWORD` *5 - infinity*

Specifies the amount of time, in seconds, the server waits for a service to respond before it changes the following service statuses: pause, continue, install, uninstall.

Default: 60 seconds

`NativeLM` `REG_SZ` *Character string*

Specifies an additional field in the session setup request/response. This field is generated at run time.

Default: (Advanced Server V4.0 for DGITAL UNIX)

`NativeOS` `REG_SZ` *Character string*

Specifies an additional field in the session setup request/response. This field is generated at run time.

Default: DIGITAL UNIX V4.0 (Rev.564)

`SendByeMessage` `REG_DWORD` *0 or 1*

Specifies whether the server sends a message to every client in the domain if it is going to stop for any reason other than a normal shutdown. The message states that the ASDU server has stopped.

Default: 1 (send a message)

`ShowUnixQueues` `REG_DWORD` *0 or 1*

Specifies whether the server shows DIGITAL UNIX queues to clients.

Default: 0 (do not show DIGITAL UNIX queues)

`SizeGcBufferPoolInKB` `REG_DWORD` *1 - infinity*

Specifies the buffer size, in KBytes, allocated for each server process for client files.

Default: 200 KBytes

`TestBits` `REG_DWORD` 0 - *infinity*

Not currently used.

Default: 0

Process Parameters

The registry path that contains entries for the ASDU process parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\ProcessParameters
```

`CoreOk` `REG_DWORD` *0 or 1*

Specifies whether the server creates a core dump file on disastrous failures.

Default: 1 (create core file)

`KeepSpareServer` `REG_DWORD` *0 or 1*

Specifies whether the server should have a spare `lmx.srv` process available for another client. New client connections will be faster if this key is enabled.

Default: 1 (start spare `lmx.srv` process)

`LockNapInMSec` `REG_DWORD` *1 - infinity*

Specifies the length of time in milliseconds that the server sleeps when a shared memory lock contention occurs. The server retries busy locks at intervals specified by this key until the length of time specified in the value of the MaxLockTimeInSeconds key elapses.

Default: 10 milliseconds

`MaxLockTimeInSeconds` `REG_DWORD` *5 - infinity*

Specifies the maximum interval in seconds that a server process waits for a shared memory lock to become available.

Default: 60 seconds

`MaxVCPerProc` `REG_DWORD` *0 - 101*

Specifies the maximum number of virtual circuits that each `lmx.srv` process handles. This limit normally is calculated by the ASDU server using the value of the `VCDistribution` registry key and the value of the `maxclients` parameter in the `lanman.ini` file. If the value of this key is non zero, its value is used instead of the calculated value.

Default: 0 (use value of `VCDistribution` key)

`MaxVCs` `REG_DWORD`

Specifies the maximum number of virtual circuits that can be established to an ASDU server. This key permits you to manually override the sizing of shared memory. Do not change the value of this key.

`MinSmbWorkerTasks` `REG_DWORD` *0-100*

Determines how many SMBWORKER tasks are preallocated by `lmx.srv` processes on startup. Do not change the value of this key.

Default: 3 worker tasks

`MinVCPerProc` `REG_DWORD`

Specifies the minimum number of virtual circuits that each lmx.srv process can handle. This limit normally is calculated by the ASDU server using the value of the `VCDistribution` registry parameter and the value of the `maxclients` parameter in the `lanman.ini` file. If this value is non-zero, its value is used instead of the calculated value.

Default: 0 (Use value of VCDistribution key)

`NumCIStructs` `REG_DWORD`

Specifies the size of the CLIENTINFO array in shared memory. Do not change the value of this key.

Default: 12

`NumCLIENT_SESSION` `REG_DWORD` *5 - 128*

Limits the number of trust relationships that a server can maintain with other domains. This value should be at least one greater than the number of domains trusted by the server's domain.

Default: 5 trust relationships

`NumHashTables` `REG_DWORD` *8 - infinity (powers of 2)*

Specifies the number of buckets for the hash table in shared memory to keep track of the various modes that clients have used to open files and set record locks. Do not change the value of this key.

Default: 128 buckets

`NumSERVER_SESSION` `REG_DWORD` *5 - infinity*

Limits the number of servers and Windows NT clients that can authenticate with the server. This value should be large because it limits the number of Windows NT clients that can contact the server. On a primary domain controller, the value must be at least the number of servers and Windows NT clients in the domain.

Default: 100 clients

`NumUStructs` `REG_DWORD` *1 - infinity*

Specifies the number of structures allocated in shared memory to handle record lock and open file records. The sum of open files and record locks cannot exceed the value of this key.

Default: 1000 open files and record locks

`SpareServerTime` `REG_DWORD` *0 - infinity*

Specifies the interval in seconds that a spare `lmx.srv` process is allowed to run without serving a client before being terminated.

Default: 120 seconds (2 minutes)

`StopOnCore` `REG_DWORD` *0 or 1*

Specifies whether the `lmx.ctrl` process is to stop, and therefore all other `lmx.srv` processes, if it finds that an `lmx.srv` process has terminated unexpectedly.

Default: 0 (do not stop the ASDU server)

`VCDistribution` `REG_MULTI_SZ` *List*

Specifies the distribution of virtual circuits or sessions over `lmx.srv` processes. The architecture of the server allows multiple sessions to be served by each `lmx.srv` process on the DIGITAL UNIX system. The server determines if a new session should be handed off to an existing `lmx.srv` process or if a new process should be started. Values are entered in sets of three integers separated by commas, each set of three numbers on a new line. In each set, the first number specifies the number of clients; the second number specifies the minimum number of virtual circuits each `lmx.srv` process should support; the third number specifies the maximum number of virtual circuits each process should support.

Default: 1,2,12
20,2,20
35,2,24
50,3,28
85,4,28
100,5,32
130,6,36
180,8,42
250,9,44
350,10,50
500,10,60
750,10,80
1000,10,101

The following table describes the meaning of the default value:

Number of clients	Minimum sessions per lmx.srv	Maximum sessions per lmx.srv
1-19	2	12
20-34	2	20
35-49	2	24
50-84	3	28
85-99	4	28
100-129	5	32
130-179	6	36
180-249	8	42
250-349	9	44
350-499	10	50
500-749	10	60
750-999	10	80
1000+	10	101

RPC Parameters

The registry path that contains entries for the ASDU RPC parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\RpcParameters
```

`BrowserMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open browser sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`EventlogMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open event log sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`LsarpcMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open LSA RPC sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`NetlogonMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open Netlogon sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`SamrMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open SAM sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`SpoolssMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open print sessions that an `lmx.srv` process can support simultaneously.

Default: 50 sessions

`SrvsvcMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open server sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`SvcctlMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open service control sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`WinregMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open registry sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

`WkssvcMaxCalls` `REG_DWORD` *10 - 10,000*

Specifies the maximum number of open workstation sessions that an `lmx.srv` process can support simultaneously.

Default: 20 sessions

Share Parameters

The registry path that contains entries for the ASDU share parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\ShareParameters
```

`KeepAdministrativeShares` `REG_DWORD` *0 or 1*

Specifies whether administrators are prevented from removing the ADMIN$ and IPC$ shared resources.

Default: 1 (prevented from removing administrative shared resources)

`MakeUnixDirectoriesOnShare` `REG_DWORD` *0 or 1*

Specifies whether the ASDU server should create a directory automatically if one does not exist when creating a new share using the Server Manager.

Default: 1 (create new directory)

`ShareCacheCount` `REG_DWORD` *5 - infinity*

Specifies the number of share names to store in the `sharefile` cache.

Default: 40 cache entries

`ShareReadCount` `REG_DWORD` *1 - infinity*

Specifies the number of share entries to read during `sharefile` operations. Setting this parameter to a value greater than 1 causes the server to read ahead SHAREENTRY structures from the `sharefile`.

Default: 10 share entries

UNIX Audit Parameters

The registry path contains that entries for the ASDU UNIX audit parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\UnixAuditParameters
```

`Access` `REG_DWORD` *0 or 1*

Determines the accessibility of a file.

Default: 1

`chdir` `REG_DWORD` *0 or 1*

Changes the current directory.

Default: 1

`chown` `REG_DWORD` *0 or 1*

Changes the owner of files and directories.

Default: 1

`close` `REG_DWORD` *0 or 1*

Closes the file associated with a file descriptor.

Default: 1

`EnableUnixAuditing` `REG_DWORD` *0 or 1*

Specifies whether the ASDU server uses DIGITAL UNIX auditing, if it has been configured into the kernel.

Default: 1

`getuid` `REG_DWORD` *0 or 1*

Gets the real or effective user ID.

Default: 1

`login` `REG_DWORD` *0 or 1*

Establishes sessions to the server.

Default: 1

`open` `REG_DWORD` *0 or 1*

Opens a file for reading or writing.

Default: 1

`setuid` `REG_DWORD` *0 or 1*

Sets the user ID.

Default: 1

`stat` `REG_DWORD` *0 or 1*

Displays information about a file.

Default: 1

User Service Parameters

The registry path that contains entries for the ASDU user service parameters is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AdvancedServer\UserServiceParameters
```

`CreateUnixUser` `REG_DWORD` *0 or 1*

Specifies whether to automatically create and assign a DIGITAL UNIX user account to every new ASDU user account if a corresponding DIGITAL UNIX account does not already exist. The value of this key must be set to 1 on every server on which DIGITAL UNIX system accounts will be created.

The DIGITAL UNIX account is created with a `/bin/sh` login shell, which enables the user to have interactive sessions to the server by using a terminal emulator. The password for the DIGITAL UNIX account must be set by the root account before the user can interactively log in to the server.

While ASDU account names can contain up to 20 characters, the maximum number of characters for a DIGITAL UNIX user account is 8. If the ASDU user account name exceeds 8 characters, the DIGITAL UNIX user account is created using the first 6 characters, and the last 2 characters are substituted with special characters. The user uses this new, shortened name to log in to the DIGITAL UNIX server.

For example, if an ASDU user account name is `longusername`, then the DIGITAL UNIX account in the `/etc/passwd` file might be `longush3`. The user uses this name to log in to the DIGITAL UNIX server when using a terminal emulator.

If `CreateUnixUser` is set to zero (0), then all new ASDU users are mapped to the DIGITAL UNIX system `lmworld` account, which was created when the ASDU software was installed.

Default: 1 (create DIGITAL UNIX user accounts)

`Exclude` `REG_SZ` *Character string*

Specifies a range of the existing DIGITAL UNIX user IDs that are excluded from being assigned to ASDU user accounts. If an ASDU user account is created with a name that matches an existing DIGITAL UNIX system user account whose ID is contained in the exclude list, a new DIGITAL UNIX system user account is generated and assigned to the ASDU user account. This ensures that certain existing DIGITAL UNIX system user accounts are never assigned automatically to newly-created ASDU user accounts, even if the `ForceUniqueUnixUserAccount` key is set to zero (0).

Default: 0 - 100

`ForceUniqueUnixUserAccount` `REG_DWORD` *0 or 1*

Specifies whether to automatically assign an existing DIGITAL UNIX system user account to a newly-created ASDU user account. If set to 1, then the system does not assign existing DIGITAL UNIX system user accounts. Instead, new DIGITAL UNIX system user accounts are generated and assigned to ASDU user accounts when they are created.

Default: 0 (existing DIGITAL UNIX user accounts can be assigned)

`GroupUpdateTime` `REG_DWORD` *0 - infinity*

Specifies the interval in seconds at which the server checks the DIGITAL UNIX system file `/etc/group` for changes.

Default: 3600 seconds (1 hour)

`NewUserShell` `REG_SZ` *Character string*

Specifies the login shell for new user accounts. Set this key to `/bin/false` to prevent new users from logging in to the DIGITAL UNIX system by using a terminal emulator.

Default: `/bin/sh`

`SyncUnixHomeDirectory` `REG_DWORD` *0 or 1*

Specifies that if the home directory of an ASDU user account changes, then the home directory of the associated DIGITAL UNIX system user account also changes to match it.

Default: 0 (do not synchronize home directories)

`UserComment` `REG_SZ` *Character string*

The ASDU server ignores this key. It is used on other systems to specify the comment for automatically created UNIX accounts.

Default: Advanced Server for DIGITAL UNIX user

`UserRemark` `REG_SZ` *Character string of up to 48 characters*

Specifies the comment string associated with the `USERS` shared directory.

Default: Users Directory

Alerter Service Parameters

The registry path that contains entries for the ASDU alerter service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Alerter\Parameters
```

`AlertNames` `REG_MULTI_SZ` *List*

Specifies a list of the user accounts and computer names that should receive administrative alerts.

Default: None

`CountNotOnNetworkCache` `REG_DWORD` *0 - infinity*

Specifies the number of nonrunning cached clients to which the Alerter service should not attempt to send messages. When the Alerter service tries to send a message to a client, NetBIOS name resolution can cause delays if the client is not on the network. To circumvent this problem, the Alerter service caches the names of clients that are not running and does not send alerts to these clients.

Default: 10 clients

`IncludeMessageHeader` `REG_DWORD` *0 or 1*

Specifies whether the Alerter service should add the sender, recipient, subject, and date information in a header.

Default: 0 (do not include header information)

`NotOnNetworkCacheTimeout` `REG_DWORD` *0 - infinity*

Specifies the length of time, in seconds, that nonrunning clients should remain in the server's cache of clients.

Default: 120 seconds (2 minutes)

Browser Service Parameters

The registry path that contains entries for the ASDU browser service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Browser\Parameters
```

`BackupRecovery` `REG_DWORD` *60 - infinity*

Specifies the length of time, in seconds, that must elapse before a server that has ceased being a backup browser can become a backup browser again.

Default: 1800 seconds (30 minutes)

`BackupUpdate` `REG_DWORD` *60 - infinity*

Specifies the interval, in seconds, at which the backup browser refreshes its browse lists with the master browser.

Default: 720 seconds (12 minutes)

`MasterUpdate` `REG_DWORD` *60 - infinity*

Specifies the interval, in seconds, at which the master browser ages its browse lists and updates its lists with the domain master browser.

Default: 720 seconds (12 minutes)

`MoreLog` `REG_DWORD` *0 or 1*

Specifies whether the Computer Browser service should record additional system log entries for events such as election packets that the Computer Browser service receives, and the role of the browser server (master or backup).

Default: 0 (do not record additional system log entries)

EventLog Service Parameters

The `EventLog` subkey contains at least three subkeys for the Application, Security, and System logs. These logfile subkeys contain subkeys that define the locations of the related event message files and the supported types of events, as follows:

- Application — Perflib, Perfmon, Remote Boot Replicator
- Security — LSA, SC Manager, Security, Security Account Manager, Spooler
- System — Alerter, Browser, Eventlog, NetLogon, Print, Rdr, SAM, Server, Service Control Manager, Srv, Wins, workstation

Each logfile subkey for the EventLog service can contain the value entries described in this section. The registry path for these entries is the following, where *`logfile`* is System, Application, or Security.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\`*`logfile`*

These entries are described for informational purposes only. The Event Viewer usually maintains this information.

`File` `REG_EXPAND_SZ` *Character string*

Specifies the fully qualified path name of the file for this log.

Default: `%SystemRoot%/usr/net/servers/lanman/logs/`*`filename`*

`MaxSize` `REG_DWORD` *0 to infinity in multiples of 64 KBytes*

Specifies the maximum size, in bytes, of the log file. This value can be set using the Event Viewer.

Default: 524288 (512 KBytes)

`Retention` `REG_DWORD` *0 to infinity*

Specifies, in seconds, that records newer than this value will not be overwritten. The value of this entry may causes a log full event. This value can be set using the Event Viewer.

Default: 604800 seconds (7 days)

`Sources` `REG_MULTI_SZ` *List*

Specifies the applications, services, or groups of applications that write events to this log. Each source may be a subkey of the logfile subkey. (The `appsources`, `secsources`, and `syssources` keys are also in the `lanman.ini` file.)

Default: (varies according to log file)

The subkeys under a logfile subkey are created by the applications that write events in the related event log. These subkeys contain information specific to the source of an event under the following types of value entries:

`EventMessageFile` `REG_EXPAND_SZ` *Character string*

Specifies the path and file name for the event identifier text message file.

`CategoryMessageFile` `REG_EXPAND_SZ` *Character string*

Specifies the path and file name for the category text message file. The category and event identifier message strings can be in the same file.

`CategoryCount` `REG_DWORD` *0 to infinity*

Specifies the number of categories supported.

`TypesSupported` `REG_DWORD` *0 to infinity*

Specifies a bitmask of supported types.

Lanman Server Parameters

The registry path that contains entries for the ASDU LAN Manager service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\LanmanServer\Parameters
```

`AccessAlert` `REG_DWORD` *0 - infinity*

Specifies the number of resource access violations that can occur before the server sends an alert to the `alertnames` list.

Default: 5 violations

`AutoDisconnect` `REG_DWORD` *0 - 3600 (60 hours)*

Specifies the interval, in minutes, that the server waits before dropping the virtual circuit to an inactive client.

Default: 0 minutes (no automatic disconnect)

`ErrorAlert` `REG_DWORD` *0 - infinity*

Specifies the number of errors that can occur before the server sends an alert to the `alertnames` list.

Default: 5 errors

`Hidden` `REG_DWORD` *0 or 1*

Specifies whether the server is hidden on the network. If the server is not hidden, it is set in the `SrvAnnounce` and `LmAnnounce` keys.

Default: 0 (server is visible)

`LmAnnounce` `REG_DWORD` *0 or 1*

Specifies whether a server should announce itself with the LAN Manager-type announcement in addition to the Windows NT-type announcement. This key has an effect only if the value of the `Hidden` key is zero (0).

Default: 0 (use only Windows NT-type announcement)

`LogonAlert` `REG_DWORD` *0 - infinity*

Specifies the number of logon violations that can occur before the server sends an alert to the `alertnames` list.

Default: 5 violations

`SrvAnnounce` `REG_DWORD` *1 - infinity*

Specifies the interval, in seconds, at which the server announces its presence to the network. This key has an effect only if the value of the `Hidden` key is zero (0).

Default: 180 seconds (3 minutes)

`SrvComment` `REG_SZ` *String up to 48 characters*

Specifies the descriptive comment that the server sends to announce its presence to the network.

Default: Advanced Server for DIGITAL UNIX Systems

`UserPath` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX system directory on the server to be used as a default parent directory for home directories of new user accounts.

Default: `c:\usr\users`

Netlogon Service Parameters

The registry path that contains entries for the ASDU net logon service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
Netlogon\Parameters
```

`LogonQuery` `REG_DWORD` *60 - infinity*

Specifies the interval, in seconds, at which the server checks if linked clients are still active.

Default: 900 seconds (15 minutes)

`Pulse` `REG_DWORD` *60 - 3600 (1 hour)*

Specifies the interval, in seconds, for sending update notices to the master user accounts database when no updates are occurring. This keyword applies only to a primary domain controller and is ignored by other servers.

Default: 300 seconds (5 minutes)

`QueryDelay` `REG_DWORD` *1 - infinity*

Specifies the interval, in seconds, that a client can wait before responding to the server's inquiry about whether it is active.

Default: 2 seconds

`Randomize` `REG_DWORD` *5 to 120*

Specifies the time period, in seconds, within which a backup domain controller randomizes its request to a primary domain controller for updates after receiving an update notice. This keyword decreases the odds that servers in the same domain will request an update from the primary domain controller at the same time.

Default: 30 seconds

`RelogonDelay` `REG_DWORD` *1 - infinity*

Specifies the interval, in seconds, that a client can wait before logging back on to the server after the server has been stopped and restarted.

Default: 2 seconds

`Scripts` `REG_EXPAND_SZ` *Character string*

Specifies the location of the logon scripts directory.

Default:
`/usr/net/servers/lanman/shares/asu/repl/export/scripts`

`SSIPasswdAge` `REG_DWORD` *86400 (24 hours) - infinity*

Specifies the time, in seconds, at which a backup domain controller must change the password that it sends to the primary domain controller to verify its eligibility to receive user accounts database updates.

Default: 604800 seconds (7 days)

`Update` `REG_DWORD` *0 or 1*

Specifies that the server synchronizes the user accounts database with the primary domain controller every time it starts. This keyword applies only to a backup domain controller and is ignored by the primary domain controller. Note that full synchronization is a very time-consuming operation.

Default: 0 (do not synchronize)

Netrun Service Parameters

The registry path that contains entries for the ASDU netrun service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
Netrun\Parameters
```

`MaxRuns` `REG_DWORD` *1 to 10*

Specifies the the maximum number of `netrun` requests that can run simultaneously.

Default: 3 requests

`RunPath` `REG_SZ` *Character string of up to 256 characters*

Specifies the path where programs accessible via the Netrun service are located. Only programs located in a runpath can be executed from a client or another server. Separate multiple path entries with a colon (:).

Default: `/tmp`

Replicator Service Parameters

The registry path that contains entries for the ASDU directory replicator service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Replicator\Parameters
```

`ExportList` `REG_SZ` *Character string*

Specifies the servers or domains that receive notices when the export directory is updated. These servers subsequently replicate from the export server. If no value is specified, the export server sends a notice to its domain. Separate multiple names with a semicolon (;). This value is ignored if the value of the `Replicate` entry is 2 (import).

Do not use the UNC name to specify a computer name; that is, do not include two backslashes (\\) at the beginning of the name.

Default: (local domain name)

`ExportPath` `REG_SZ or REG_EXPAND_SZ` *Character string*

Specifies the export path. All files to be replicated must be in a subdirectory of the export directory. This value is ignored if the value of the `Replicate` entry is set to 2 (import).

Default: `/usr/net/servers/lanman/shares/asu/repl/export`

`GuardTime` `REG_DWORD` *0 to one-half of Interval*

Specifies the number of minutes an export directory must be stable (no changes to any files) before import servers can replicate its files.

This option applies only to directories with tree integrity.

Default: 2 minutes

`ImportList` `REG_SZ` *Character string*

Specifies the servers or domains from which files and directories are to be replicated. If no value is specified, files and directories are replicated from the server's domain. Separate multiple names with a semicolon (;). This value is ignored if the value of the `Replicate` entry is 1 (export).

Do not use the UNC name to specify a computer name; that is, do not include two backslashes (\\) at the beginning of the name.

`ImportPath` `REG_SZ or REG_EXPAND_SZ` *Character string*

Specifies the path on the import server to receive replicas from the export servers. This value is ignored if the value of the `Replicate` entry is 1 (export).

Default: `C:\var\opt\lanman\shares\asu\repl\import`

`Interval` `REG_DWORD` *1 to 60*

Specifies how often, in minutes, an export server checks the replicated directories for changes. Used in conjunction with the `Pulse` entry. Ignored on import servers.

Default: 5 minutes

`MaxFilesInDirectory` `REG_DWORD` *0 to infinity*

Specifies the maximum number of replicated files in an import directory.

Default: 2000 files

`Pulse` `REG_DWORD` *1 to 10*

Specifies, in minutes, how often the export server repeats sending the last update notice. These repeat notices are sent even when no changes have occurred, so that import servers that missed the original update notice can receive the notice. The server waits the equivalent of (pulse * interval) minutes before sending each repeat notice.

Default: 3 minutes

`Random` `REG_DWORD` *1 to 120*

Specifies the maximum time, in seconds, that the import servers can wait before requesting an update. An import server uses the export server's value of `Random` to generate a random number of seconds (from 0 to the value of `Random`). The import server waits the specified time after receiving an update notice before requesting the replica from the export server. This prevents the export server from being overloaded by simultaneous update requests.

Default: 60 seconds

`Replicate` `REG_DWORD` *1, 2, or 3*

Specifies the Replicator action, according to the following:

1 Export — The server maintains a master tree to be replicated.

2 Import — The server receives update notices from the export server.

3 Both — The server exports and imports directories or files.

Default: 2 (import)

`TryUser` `REG_DWORD` *0 or 1*

Specifies whether the import server should try to update directories when a user is logged on locally.

Default: 0 (do not try to update when user is logged on)

`UnixDirectoryGroup` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX group name for replicated directories.

Default: `DOS----`

`UnixDirectoryOwner` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX user account name for replicated directories.

Default: `lmxadmin`

`UnixFileGroup` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX group account name for replicated files.

Default: `DOS----`

`UnixFileOwner` `REG_SZ` *Character string*

Specifies the DIGITAL UNIX user account name for replicated files.

Default: `lmxadmin`

UPS Service Parameters

The registry path that contains entries for the ASDU uninterrupted power source service is as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\UPS\Parameters
```

`IgnoreSIGPWR` `REG_DWORD` *0 or 1*

Specifies whether uninterrupted power source service will be enabled.

Default: 1 (disables UPS service)

`PowerFailAddress` `REG_SZ` *Character string of up to 15 characters*

Specifies the NetBIOS name to which the server sends a message when it receives a SIGPWR signal.

Default: * (all users)

`PowerFailMessage` `REG_SZ` *Character string of up to 500 characters*

The text of the message sent by the server when it receives a SIGPWR signal.

Default: “The system has experienced a power failure. Please close all applications and files and log off immediately.”

`PowerMessageInterval` `REG_DWORD` *0 - infinity*

Specifies the interval, in minutes, at which the server repeats the message sent when it receives a SIGPWR signal. A value of zero (0) indicates to send the message one time only.

Default: 1 minute

Registry Administrative Interfaces

You use the following interfaces to view and modify registry keys:

- The `regconfig` command, which is typed at the DIGITAL UNIX command prompt.
- The Registry Editor, a windows-based interface
- The AS/U Administrator, a windows-based interface

Note that The ASDU server must be stopped and restarted in order for most changes to the ASDU Registry to take effect.

The `regconfig` Command

You use the `regconfig` command to display detailed information about or to set values for registry keys. For example, to display information about the System/CurrentControlSet/Services/AdvancedServer/FileService/Parameters keys, enter the following command at the DIGITAL UNIX command prompt:

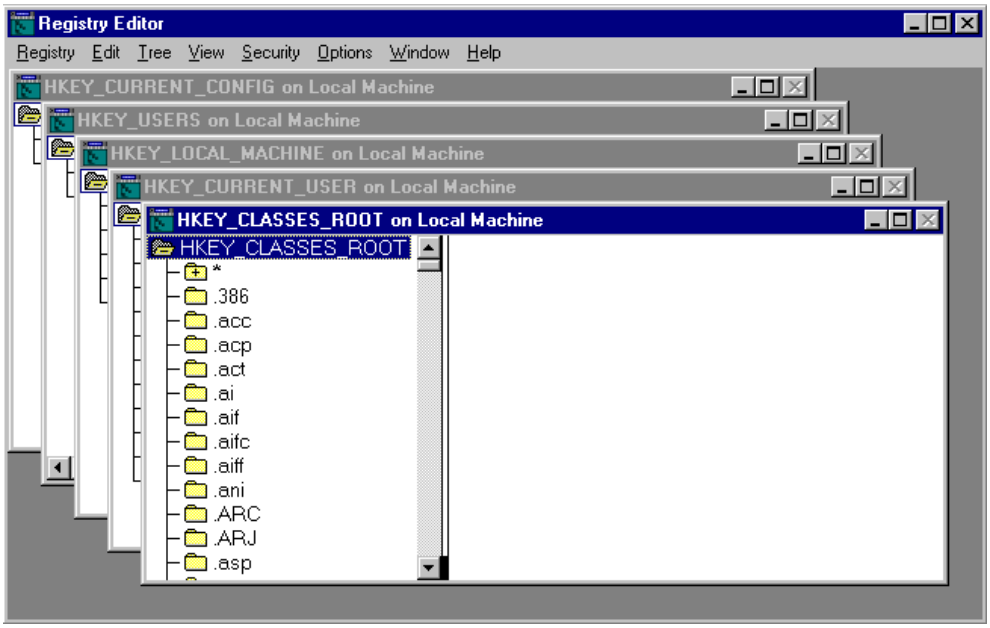
```
/usr/sbin/regconfig System/CurrentControlSet \
/Services/AdvancedServer/FileServiceParameters
```

Registry Editor

You can use the Registry Editor to view and modify registry entries. You start the Registry Editor by running the `Regedt32.exe` application, which is installed automatically in the *%SystemRoot%*`\system32` folder on Windows NT systems.

Warning: DIGITAL recommends that you do not use the Windows 95 Registry Editor to remotely edit the ASDU Registry.

The Registry Editor displays windows similar to the following:



To edit the ASDU registry using the Windows NT Registry Editor, you must use the Select Computer item on the Registry menu of the Registry Editor to connect to the ASDU Server. When you connect to the ASDU Registry remotely, the HKEY_USERS and HKEY_LOCAL_MACHINE subtrees display.

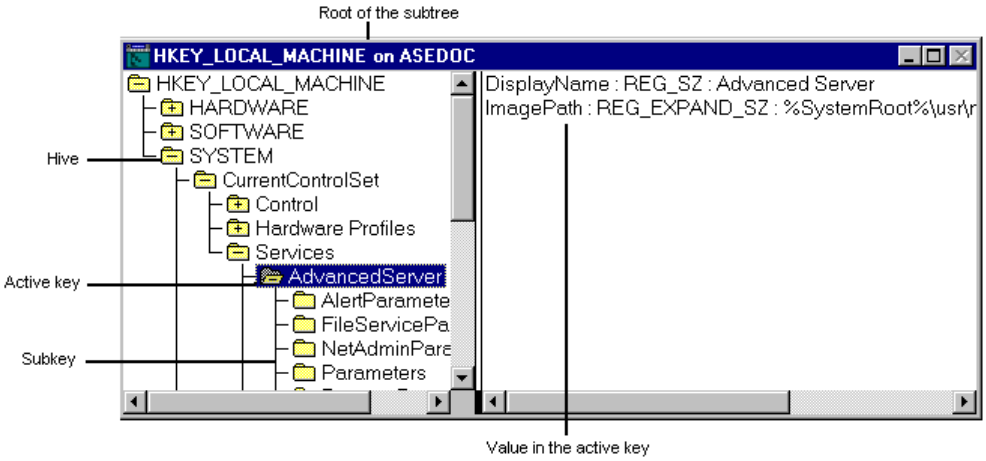
Your ability to change the registry using the Registry Editor depends on your access permissions. Generally, you have the same permission for the Registry Editor as you do for other administrative tools.

For More Information

For more information about connecting to a remote registry, see Accessing the Registry of a Remote Computer in Registry Editor online Help.

Registry Editor Commands

As shown in the following figure, the Registry Editor displays data in two panes. The value entries in the right are associated with the selected key in the left.



You can use the mouse or enter commands to manipulate the windows and panes in the Registry Editor in the same way you do in the Windows NT Explorer. For example:

- Double-click on a key name to expand or collapse an entry or click on commands on the View and Tree menus to control the display of a selected key and its data.
- Use the mouse or arrow keys to move the vertical bar in the window to control the size of the left and right panes.
- Click on the Tile or Cascade items on the Window menu to arrange the Registry Editor windows.
- Click on the Auto Refresh item on the Options menu to continuously update the display. You can also click on one of the `Refresh` commands on the View menu to update the display of registry information when the `Auto Refresh` option is turned off.

The following list shows some keyboard methods for managing the display of data in each Registry Editor window:

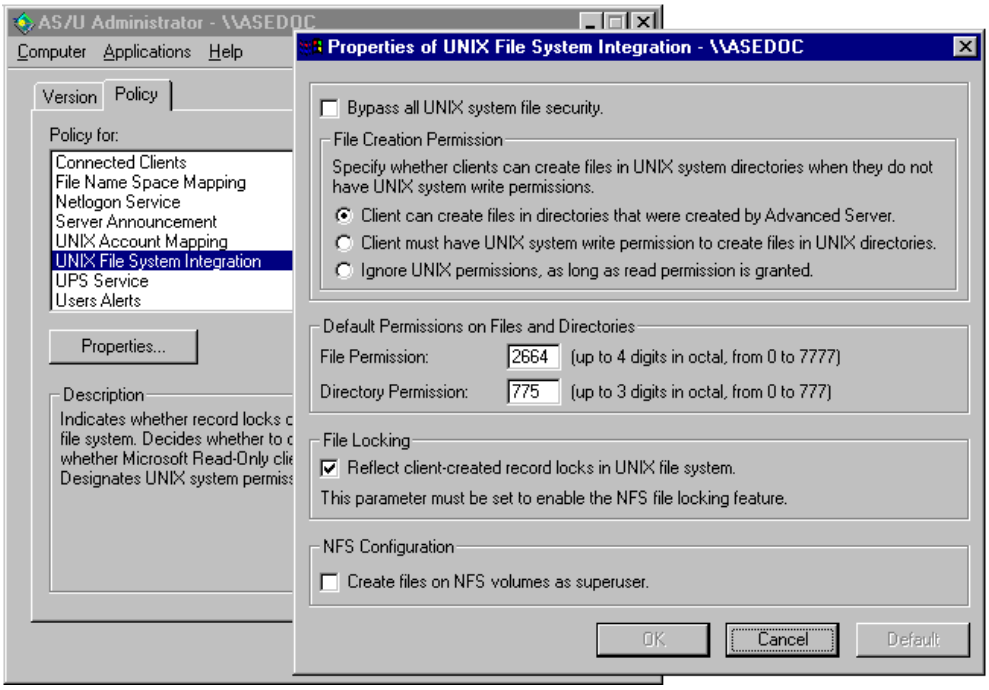
- To expand all of the levels of the predefined handle in the active Registry window, press CTRL + *
- To expand one level of a selected registry key, press ENTER
- To expand a branch of a selected registry key, press the asterisk (*) key on the numeric keypad

- To collapse a branch of a selected registry key, press ENTER or the minus symbol (-)on the numeric keypad

AS/U Administrator

The windows-based AS/U Administrator, which unlike the Registry Editor, allows you to choose from lists of allowable values to modify most keys. In this way, you are less likely to accidentally corrupt the data in your registry file.

You can view and modify registry values by selecting the Policy tab, then a subkey. When you choose a policy, a properties dialog box displays for the policy where administrators view and select values for entries as shown in the following figure:



Installing the AS/U Administrative Utility

Follow these steps to install the AS/U Administrative utility on a Windows NT PC:

1. Ensure that the Client-based Advanced Server Administration Tools subset is installed on the ASDU server.
2. Map a network drive to the `astools` disk share on the ASDU server.
3. Select the `asuadm` folder.
4. Scroll down the directory and run the `setup.exe` program to install the AS/U Administrative utility.
5. Once the AS/U Administrative utility is installed, disconnect the network drive to the `astools` disk share and create an icon for the AS/U Administrative utility.

Run the AS/U Administrator and in the `Select Computer` field enter the name of the ASDU server whose registry you want to configure. Configuration data for the selected computer is displayed on the AS/U Administrator Version tab. To view or change ASDU Registry values, click on the Policy tab.

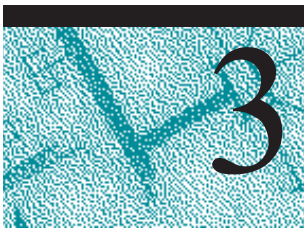
The following lists the policies and their associated ASDU Registry keys that you can modify by using the AS/U Administrator.

- Alerter Service – `(SYSTEM\CurrentControlSet\Services\Alerter\Parameters)`
  - `IncludeMessageHeader`
  - `IncludeMessageHeader`
  - `NotOnNetworkCacheTimeout`
- Computer Browser Service – `(SYSTEM\CurrentControlSet\Services\Browser\Parameters)`
  - `MasterUpdate`
  - `BackupUpdate`
  - `BackupRecovery`
  - `MoreLog`
- Connected Clients – `(SYSTEM\CurrentControlSet\Services\Netlogon\Parameters)`
  - `LogonQuery`
  - `QueryDelay`
  - `RelogonDelay`

- Connected Clients – SYSTEM\CurrentControlSet\Services\LanmanServer \Parameters)
  - AutoDisconnect
- File Name Space Mapping – (SYSTEM\CurrentControlSet\Services\AdvancedServer \FileServiceParameters)
  - NameSpaceMapping
  - UniqueSuffixLength
  - MixedCaseSupport
  - TruncatedExtensions
  - MappingSeparator
- Netlogon Service – (SYSTEM\CurrentControlSet\Services\Netlogon\Parameters)
  - Scripts
  - Pulse (PDC only)
  - Update (BDC only)
  - Randomize (BDC only)
  - SSIPasswdAge (BDC only)
- Server Announcement – (SYSTEM\CurrentControlSet\Services\LanmanServer\ Parameters)
  - Hidden
  - SrvAnnounce
  - LmAnnounce
- DIGITAL UNIX Account Mapping – (SYSTEM\CurrentControlSet\Services\AdvancedServer\ FileServiceParameters)
  - CreateUnixUser
- DIGITAL UNIX File System Integration – (SYSTEM\CurrentControlSet\Services\AdvancedServer\ FileServiceParameters)
  - IgnoreUnixPermissions
  - UnixDirectoryCheck
  - UnixFilePerms
  - UnixDirectoryPerms
  - UseUnixGroups
  - UseUnixLocks
  - RootOwnsFilesCreatedOnNFS

- UPS Service – (SYSTEM\CurrentControlSet\Services\UPS\Parameters)
  - IgnoreSIGPWR
  - PowerFailAddress
  - PowerFailMessage
  - PowerMessageInterval
- Users Alerts – (SYSTEM\CurrentControlSet\Services\AdvancedServer\AlertParameters)
  - AertAdminOnLicenseOverFlow
  - AlertUserOnLicenseOverFlow
- Users Alerts – (SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters)
  - AccessAlert
  - ErrorAlert
  - LogonAlert

CHAPTER 3



ASDU Administrative Interfaces

After you successfully install and configure the ASDU software, the server is ready to share DIGITAL UNIX resources as domain resources with Microsoft PC users. Before you can share resources, you must use an ASDU server-based or client-based administrative interface to create:

- Disk shares that map to the DIGITAL UNIX file systems that Microsoft PC users need to access
- Printer shares that map to the DIGITAL UNIX supported printers that Microsoft PC users need to access
- For each Microsoft PC user, a domain user account that you can use to control access to disk and printer shares

This chapter discusses the tools and utilities that you use to administer the ASDU environment in the following sections:

- Overview of Administrative Interfaces
- Server-Based Administrative Commands
- Client-Based Administrative Interfaces

Overview of Administrative Interfaces

The ASDU software provides interfaces that you can use to administer the ASDU server and domain. These interfaces are summarized in Table 3-1.

Table 3-1: Overview of ASDU Administrative Interfaces

Interface	Purpose	Issued From
Net commands	Administer and view all aspects of the server and domain including users, groups, disk shares, and printer shares	DIGITAL UNIX or MS-DOS command prompt
Advanced Server commands	Administer and view a server's properties and domain settings	DIGITAL UNIX command prompt
Server Manager	Administer and view a server's properties, disk shares, and services	Windows desktop
User Manager	Administer and view a server's user and group accounts and security policies	Windows desktop
System Policy Editor	Administer and view settings that define a login environment for a computer, user, or group of users	Windows desktop
Event Viewer	Administer and view a server's system, security, and application logs	Windows desktop
Password Management	Change a user's Advanced Server and DIGITAL UNIX password simultaneously	Windows desktop

Server-Based Administrative Commands

The ASDU server and domain are administered from the DIGITAL UNIX command prompt by using either the `net` commands or Advanced Server commands.

The `net` Commands

Administrators use the `net` commands to display information about or to manage Advanced Servers and domains. Users use the `net` commands to request information about Advanced Servers and domains.

Windows NT and Windows 95 clients provide `net` commands that you enter at the MS-DOS prompt. However, these commands only display information about an Advanced Server and domain and cannot be used to manage them.

You enter `net` commands in lowercase at the DIGITAL UNIX command prompt on a system running ASDU software, using the following form:

`net` *`command`* `[/option]`

When typing a long command string, do not press [Enter] at the end of the line; continue typing and the text will automatically wrap to the next line on the screen. Press [Enter] only after you are finished typing the entire command string.

Table 3-2 describes the `net` commands that you use to administer security settings.

Table 3-2: The `net` Commands Used to Administer Security Settings

`net` Command	Description
`access`	Displays or modifies resource permissions on servers. Use this command to display and modify permissions on pipes and printer queues. Use the `net perms` command to manage permissions on all other types of resources.
`perms`	Displays or modifies resource permissions and ownership information on servers. This command operates on shares, directories, and files.
`sid`	Performs translations between account names and their corresponding security identifiers (SIDs).

Table 3-3 describes the `net` commands that you use to administer the server and domain.

Table 3-3: The `net` Commands Used to Administer the Server and Domain

`net` Command	Description
`admin`	Runs an Advanced Server command or starts a command processor on a remote server.
`auditing`	Displays and modifies the audit settings of a resource.
`browser`	Displays the list of domains that are visible from a local server or the list of computers that are active in a domain.
`computer`	Displays or modifies the list of computer accounts in a domain. This command also can be entered as `net computers`.
`config`	Displays the controllable services that are running.
`config server`	Displays or changes settings for the Server service while it is running.
`continue`	Reactivates suspended services when typed at a server; reactivates paused shared printers when typed at a client computer.
`device`	Displays list of device names and controls shared printers. When used without options, this command displays the status of all shared printers at the specified server. When used with the printer name option, this command displays only the status of the specified printer.
`file`	Displays the names of all open shared files and the number of file locks, if any, on each file. This command can be used to close shared files. When used without options, this command lists all of the open files at a server. This command also can be entered as `net files`.
`help`	Provides lists of network commands and topics for which you can get help, or provides help for a specific command or topic.
`helpmsg`	Provides help for a network error message.
`pause`	Suspends services or printers at a server.
`print`	Displays or controls print jobs and printer queues; also sets or modifies options for a printer queue.
`send`	Sends a message either to connected client computers on the domain or to the entire network.

`session`	Lists or disconnects sessions between a server and clients. When used without options, this command displays information about all of the sessions on the local server. This command also can be entered as `net sessions`.
`share`	Creates, deletes, modifies, or displays shared resources. Use this command to make a resource available to clients. When used without options, this command displays information about all of the resources being shared on the server.
`start`	Starts a service or, if used without options, displays a list of services that are running. The services that can be started are Alerter, Computer Browser, Directory Replicator, EventLog, Net Logon, Netrun, NvAlert, Server, Time Source, and WINS.
`statistics`	Displays or clears the statistics log.
`status`	Displays a server's computer name, configuration settings, and a list of shared resources.
`stop`	Stops a network service.
`time`	Synchronizes the client's clock with that of a server or domain, or displays the time for a server or domain.
`trust`	Establishes and breaks trust relationships between domains, and lists trust information for a specified domain.
`version`	Displays the version number of the network software currently running on the computer on which the command is issued.
`view`	Displays a list of servers or displays the resources being shared by a server.

Table 3-4 describes the net commands that you use to administer users and groups.

Table 3-4: The net Commands Used to Administer Users and Groups

net Command	Description
accounts	Displays the role of servers in a domain and displays or modifies password and login user requirements.
group	Adds, displays, or modifies global groups. This command can be entered as net groups.
localgroup	Adds, displays, or modifies local groups in domains. This command also can be entered as net localgroups.
logoff	Logs a user account off of the network.
logon	Logs a user account in to the domain and sets the user name and password for the user's client. If you do not specify a user name, the default user name is your DIGITAL UNIX system login name.
password	Changes the password for a user account on a server or in a domain.
user	Adds, modifies, or deletes user accounts or displays user account information.

Online Help for net Commands

Online help provides details about each net command, including syntax, options, and examples.

Use the following commands at the DIGITAL UNIX system prompt to display help for a net command.

To display a list of the net commands for which you can get help, enter net help.

To display the syntax and options for net commands, enter net help *command.*

To display the syntax and options for net commands, enter net*command* /help.

To display the syntax for net commands, enter net *command* /?.

To display a detailed description of the options for the net command you selected, enter net help *command* /options.

Table 3-5 describes the syntax conventions to be aware of when viewing online help for the `net` commands.

Table 3-5: The `net` Commands Syntax Conventions

Symbol	Meaning	Example
Braces ({ })	You must choose an option contained within braces.	`{yes | no}` You must specify yes or no when using the command.
Brackets ([ ])	You do not have to choose the option contained within brackets.	`[`*`password`*`]` A password may be used with the command, if desired.
Forward slash (/)	The item that follows is an option that should be executed.	`net file 1073722830 /close` The file with identification number 1073722830 is to be closed.
Vertical bar (|)	You have a choice of options that are contained in braces and brackets.	`{/hold | /release | /delete}` Only one of the three options must be used.
Ellipsis (. . .)	You can repeat the previous options.	`/route:` *`devicename`* `[, ...]` You can specify more than one device. Separate device names with commas.
Double quotes (“ “)	You can type a string of text.	`net groups “text”` Displays the information contained within the double quotes.
Pound sign (#)	You must replace the pound sign with a number.	`/users:10` Only 10 users can connect.

Using the net Commands

The following sections identify the syntax that you use when entering net commands.

Using Special Characters

Some of the information you supply with net commands may contain DIGITAL UNIX special characters, for example, an ampersand (&). If you use a DIGITAL UNIX special character with a net command, you must precede the character with the back slash escape character (\ ). For example, the following command logs a user named peter with a password of mrkt&dev in to an ASDU server:

```
net logon peter mrkt\&dev
```

Commonly used DIGITAL UNIX special characters include:

- Asterisk (*)
- Semicolon (;)
- Pipe (|)
- Square brackets ([ ])
- Parentheses [( )]
- Question mark (?)
- Ampersand (&)
- Caret (^)
- Back slash (\ )
- Greater-than and less-than signs (< >)
- Blank ( )
- The at symbol (@)

When you enter net commands that contain special characters from a client computer, surround the strings that contain special characters in double quotes (“ “).

Using Command Confirmation

Some `net` commands require a `yes` or `no` confirmation. For example, if you enter the `net logoff` command to log off the network with connections to remote shared resources still active, the ASDU server displays a prompt similar to the following:

```
You have the following remote connections:

  LPT1

Continuing will cancel the connections.

Do you want to continue this operation? (Y/N)  [Y]:
```

You can use the `/yes` and `/no` options with any `net` command to anticipate and respond to a prompt. For example, you are not prompted for confirmation when you enter the following command:

```
net logoff /yes
```

You can use `net` commands with `/yes` and `/no` options to create batch files and shell scripts that are not interrupted by the ASDU server prompts.

Using Passwords

Some `net` commands require a password. You can provide a password as a command option by typing it on the same line as the command itself. For example, to log a user named *`peter`* with the password *`changeme`* on to an ASDU server you would type:

```
net logon peter changeme
```

Optionally, you can replace the password with an asterisk (*), which causes the system to prompt you for a password.

Note: In the DIGITAL UNIX operating system, the asterisk (*) is a special character and must be preceded by a back slash (\ ).

For example, to be prompted for a password, enter:

```
net logon peter \*
```

The following message is displayed:

```
Type your password:
```

The password does not appear on the screen as you type.

Specifying Path Names

When creating a disk share you must specify a path that consists of a drive letter, which is always `c:`, and the location of a directory on the server to which the share will map. If the directory does not exist, it will be created.

Separate the drive from the directory specification with one of the following methods:

- A `c:` and a single forward slash (/). For example:

```
net share test=c:/usr/var/net/servers/lanman/shares/test
```

- A `c:` and single quotes (‘) with a single back slash (\). For example:

```
net share ‘test=c:\usr\var\net\servers\lanman\shares\test’
```

Each of these methods creates a share called `test` in the `/usr/var/net/servers/lanman/shares` directory on the server.

Abbreviating `net` Commands

You can abbreviate a `net` command by typing enough letters to distinguish it from other command options. However, you cannot abbreviate a value for an option. For example, the following is the syntax for the `net accounts` command:

```
net accounts [/forcelogoff:{minutes|no }] [/minpwlen:length]
[/maxpwage:{days|unlimited}][/minpwage:days] [/uniquepw:number]
```

You can enter this command in the following abbreviated form:

```
net accounts /f:10 /minpwl:6 /ma:unlimited /minpwa:7 /u:3
```

Examples of Using net Commands

The following examples show how to use `net` commands to perform common administrative tasks. These examples assume you are logged in to a local ASDU server called Server1. You can use each command to administer a remote server by adding `net admin \\servername` to the beginning of each net command.

To log on to an ASDU server enter the following command:

```
net logon username password
```

To create a user account for a user named `peter` and a password of `changeme` enter the following command:

```
net user peter changeme /add
```

To place the `Peter` user account in the Domain Admins group enter the following command:

```
net group “Domain Admins” peter /add
```

To view the shares that are available on a local Advanced Server enter the following command:

```
net view
```

To view the shares that are available on a remote Advanced Server called `server1` enter the following command:

```
net view \\server1
```

To create a file share called `plans` and map it to the `tmp` directory enter the following command:

```
net share plans=c:/tmp
```

To create a printer share called `print1` that maps to a printer called laser enter the following command:

```
net share print1=laser /print
```

To view the current connections to an ASDU server enter the following command:

```
net session
```

To view resource permissions and ownership on a directory enter the following command:

```
net perms c:/usr/net/servers/lanman/shares
```

Advanced Server Commands

The ASDU software provides Advanced Server commands that you enter at the DIGITAL UNIX command prompt to display information about or to manage ASDU servers and domains.

Table 3-6 identifies the Advanced Server commands that are located in the `/usr/sbin` directory for your use. Most of these commands must be run by the `root` account while the ASDU server is stopped.

Table 3-6: Advanced Server Commands for Administrators

Command	Purpose
`acladm`	Create, check, manage, and remove the Access Control List (ACL) database.
`asuivp`	Verify that the ASDU software is correctly installed and configured.
`asusetup`	Configure the ASDU server.
`blobadm`	Display information, check, and configure blob files.

`chacl`	Change ACL information for Advanced Server users.
`chdomain`	Change domain information for Advanced Server users.
`chgroup`	Change group information for Advanced Server users.
`chuser`	Change user information for Advanced Server users.
`clsetup`	Configure the classes in the DIGITAL UNIX lpr print subsystem.
`ctlrsetup`	Configure transports for ASDU server.
`elfread`	Display and clear event logs on the local Advanced Server computer at the DIGITAL UNIX system console.
`euctosjis`	Convert the coding of characters from Extended UNIX Code (EUC) to Shift-JIS (S-JIS) encoding.
`joindomain`	Configure an Advanced Server into a new domain.
`knbmon`	Monitor activity and status of NetBIOS over the TCP/IP transport on the system.
`lmprobe`	Run a number of system commands and programs and store the results in a text file that can be used for troubleshooting purposes.
`lmshare`	Configure an Advanced Server share file without server intervention.
`lmstat`	Display statistical information retrieved from the Advanced Server's shared memory.
`lsacl`	Display access control lists placed on objects.
`mapuname`	Map and unmap Advanced Server user, global group, and local group names to and from DIGITAL UNIX system user names.
`nbemon`	Monitor activity and status of the NetBEUI transport on the system.
`netevent`	Send administrative or user alerts, or send printing alerts to users submitting print jobs.
`nfsshare`	Create ASDU disk shares from the file systems and directories offered as NFS exports.

`regcheck`	Configure the Advanced Server registry to enumerate registry parameters, dump the contents of the registry, or check and repair registry files.
`regconfig`	Query or set Advanced Server registry key information.
`regload`	Create a registry file if one does not exist. Also used to reinitialize the registry to system defaults.
`rmacl`	Delete entries from ACLs for Advanced Server users.
`samcheck`	Check or fix the security account manager (SAM) database; or dump the change log, built-in, account, or LSA databases.
`setdomainname`	Configure the domain name of the local Advanced Server.
`setservername`	Configure the name of the local Advanced Server.
`sjistoeuc`	Convert the coding of characters from S-JIS to EUC encoding.
`srvconfig`	Display or modify Advanced Server configuration information stored in the `lanman.ini` file.

Table 3-7 identifies the Advanced Server commands that are located in the `/usr/bin` directory for use by administrators and users.

Table 3-7: Advanced Server Commands for Administrators and Users

Command	Purpose
`asduclient`	Configures user access to a printer that is attached to a Microsoft client.
`dos2unix`	Convert MS-DOS text files to DIGITAL UNIX format.
`lmshell`	Create an MS-DOS interface on the DIGITAL UNIX server.
`net`	Request information about Advanced Servers and domains. Administrators can also manage by using the `net` commands.
`ud`	Convert text files between DIGITAL UNIX, MS-DOS, and Macintosh formats.
`unix2dos`	Convert DIGITAL UNIX text files to MS-DOS format.

The following internal Advanced Server commands are reserved for use by the ASDU server only and are not documented or supported for use by administrators. These commands are located in the `/usr/lbin` directory and should not be moved, deleted, or renamed:

- `asuconfig`
- `convblob`
- `delshmem`
- `getrole`
- `jobdonmsg`
- `knblink`
- `lmat`
- `lmxstart`
- `lmxsvc`
- `makemach`
- `nbelink`

For More Information

For more information on an Advanced Server command, install the ASDU Reference pages subset and enter `man` and the name of the command at the DIGITAL UNIX command prompt.

Client-Based Administrative Interfaces

You can administer the ASDU server and domain by using native windows-based interfaces. These interfaces are available in the `astools` disk share after the client-based Advanced Server Administration Tools subset is installed.

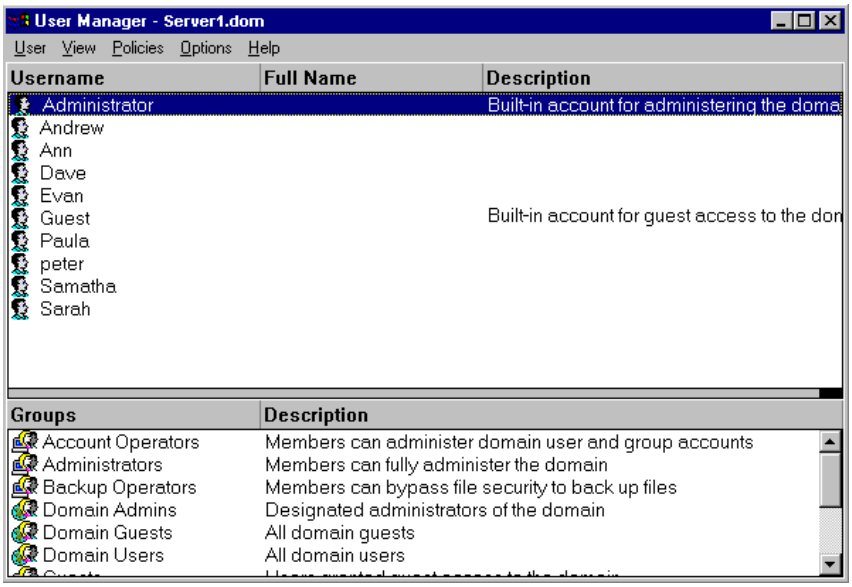
User Manager for Domains Interface

You use the User Manager for Domains interface to create and manage user accounts and groups, and to manage the following security policies for domains:

- Account Policy, which you use to unlock a user's account and define password parameters such as minimum length and expiration date.
- User Rights Policy, which you use to manage the rights that are granted to users and groups to perform actions on the system.
- Audit Policy, which you use to track activity of users.
- Trust Relationship, which you use to establish trusts between domains.

Some capabilities of the User Manager for Domains interface are also offered by the User Manager utility on every Windows NT computer. However, you can use the User Manager for Domains utility to manage both local and remote computers, while the User Manager utility only affects the local computer.

The following figure shows the User Manager for Domains window when it starts. The title bar shows the domain name, and in the body window two lists are displayed. The upper list contains user accounts; the lower list contains groups. One or more user accounts, or one group, can be selected and managed using commands from the menus.



For More Information

See the User Manager for Domain online help for more information on managing user accounts, groups, and security policies.

Server Manager Interface

You use the Server Manager interface to administer a domain and its servers.

When administering a selected server you can:

- View a list of connected users
- View shared and open resources
- Manage directory replication
- Manage the list of administrative alert recipients
- Manage services and shared directories
- Send messages to connected users

When administering a domain you can:

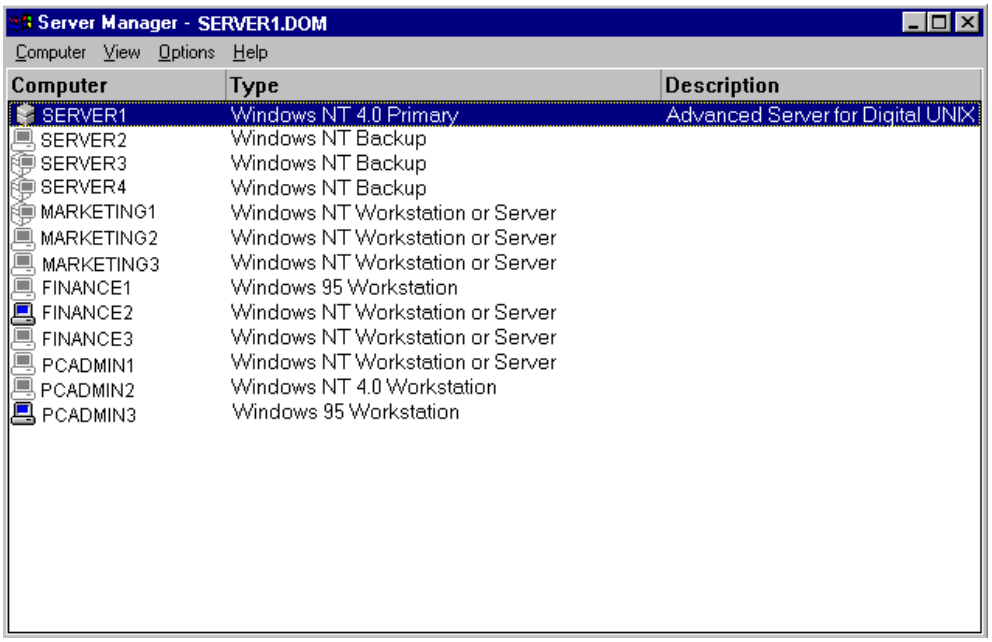
- Promote a backup domain controller to become the primary domain controller
- Synchronize servers with the primary domain controller
- Add computers to and remove computers from the domain

Some capabilities of the Server Manager interface are also offered by the Services and Server options in the Control Panel of every Windows NT computer. However, you can use the Server Manager to manage both local and remote computers, while Control Panel options only affect the local computer.

To use the Server Manager interface to administer a domain and its servers, you must be logged on to a user account that is a member of the Administrators, Domain Admins, or Server Operators group for that domain. Members of the Account Operators group can use the Server Manager only for the purpose of adding computers to the domain.

To use the Server Manager to administer a Windows NT Workstation or a server that is not a domain controller, you must be logged in to a user account that is a member of the Administrators or Power Users group for that computer.

The following figure shows the Server Manager window when it starts. The title bar shows the name of the domain that you are logged in to, and the body of the window lists the computers in that domain. You can select a computer from this list, and then manage it using commands from the menus.



For More Information

See the Server Manager online help for more information on managing servers and domains.

System Policy Editor

You can use the System Policy Editor to manage the following types of policies or registry settings that define the Windows environment for specific computers, users, or groups of users when they log in to a system:

- A user-specific policy that applies to each user or group. Most policies are user-specific. User-specific policies are always merged into the `HKEY_CURRENT_USER` key of the registry.
- A machine-specific policy that applies to all users and does not change according to user since it does not follow users as they move between different computers. Machine-specific policies are always merged into the `HKEY_LOCAL_MACHINE` key of the registry.

You save the System Policy Editor settings in a single policy (.POL) file.

When a user logs on, a program called the policy downloader starts. The policy downloader is installed on every client. The policy downloader looks on the network for the policy file, opens the policy file, looks for an entry using the local computer name or user name, and merges the administrator's registry settings as defined in the policy file, into the local registry.

If the downloader does not find an entry with the local computer name or user name in the policy file, then it looks for the DEFAULT USER or DEFAULT COMPUTER entry and uses those registry settings for the merge. If there are no entries for a specific user or computer and default entries do not exist, then no merge takes place.

The following figure shows the System Policy Editor window when it starts. The main window displays the users and computers that have entries in the policy file.

For More Information

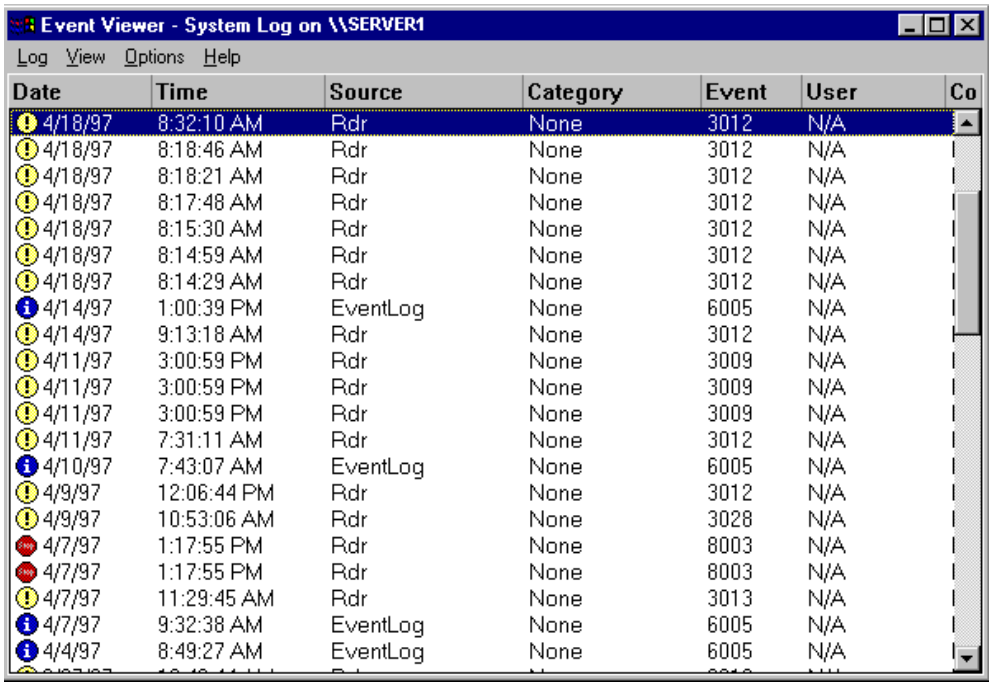
See the System Policy Editor online help for more information on managing policies.

Event Viewer Interface

The event-logging service starts automatically when the ASDU server starts up. Administrators view event logs by using the Event Viewer interface. You can use the Event Viewer interface to view the following event log files:

- System log files, which record events logged by the system components. For example, the failure of a driver or other system components to load during startup.
- Security log files, which record security changes in the system and the events you specified in the Audit Settings using the User Manager for Domains interface. For example, the number of unsuccessful log in attempts by a user. Only administrators can view security logs.
- Application log files, which record events logged by applications.

The Event Viewer interface lists events as shown in the following figure. You can double-click on any listed event to learn more about it.



For More Information

See the Event Viewer online help for more information on viewing events.

Installing the Client-Based Administrative Interfaces

The Windows client-based administrative interfaces can be installed on a PC running Windows NT, Windows 95, Windows for Workgroups, or Windows 3.1 (with networking) as described in the following sections.

Administering from a Windows NT System

You have two choices when administering from a Windows NT system. You can:

- Install the System Policy Editor, User Manager, and Server Manager interfaces locally by following these steps:

  1. Ensure that the Client-Based Advanced Server Administration Tools subset is installed on the ASDU server.
  2. Map a network drive to the `astools` disk share on the ASDU server.
  3. Select the folder that corresponds with your version of the Windows NT operating system. For example the winnt.351 folder for Windows NT 3.51 or the winnt.40 folder for Windows NT 4.0.
  4. Install the interfaces by running the `setup.bat` program.
  5. Once the interfaces are installed, disconnect the network drive to the `astools` disk share and create icons for the Server Manager, User Manager for Domains, and Policy Editor interfaces.

- Run the System Policy Editor, User Manager, and Server Manager interfaces remotely from the server by following these steps:

  1. Ensure that the Client-based Advanced Server Administration Tools subset is installed on the ASDU server.
  2. Connect to the `astools` disk share on the ASDU server.
  3. Select the folder that corresponds with the version of the Windows NT operating system. For example the winnt.351 folder for Windows NT version 3.51 or the winnt.40 folder for Windows NT version 4.0.
  4. Select the folder that corresponds with the system CPU type.
  5. Start the administrative interface you want by double-clicking on the appropriate file.

     `poledit.exe` – System Policy Editor

     `srvmgr.exe` – Server Manager

     `usrmgr.exe` – User Manager for Domains

Installing on a Windows 95 System

Follow these steps to install the User Manager, Server Manager, and Event Viewer interfaces on a PC that is running Windows 95:

1. Ensure that the Client-Based Advanced Server Administration Tools subset is installed on the ASDU server.
2. Map a network drive to the `astools` disk share on the ASDU server.
3. Select the Add/Remove Program icon from the Control Panel.
4. Select the Windows Setup tab.
5. Click on the Have Disk button. Use the Browse button and click on the drive that specifies the connection to the `astools` directory to which you connected in Step 2.
6. Expand the `Win95` directory.
7. Select the `srvtools.inf` file and click on the OK buttons in the Open window and in the Install From Disk window.
8. Install the interfaces by clicking in the box next to the Windows NT Server Tools entry and on the Install button in the Have Disk window.
9. Click on the OK button after the files are copied.
10. Disconnect the network drive to the `astools` disk share and create icons for the Server Manager, User Manager for Domains, and Event Viewer interfaces.

The installation program performs the following tasks:

- Copies the Windows NT Server Tools files to the `srvtools` directory on the boot drive of the PC running Windows 95.
- Adds “Windows NT Server Tools” to the Start button Programs menu.
- Adds a “Windows NT Server Tools” program group to the Program Manager, which is compatible with Windows 3.*x*.
- Adds extensions to the Windows Explorer so that you can change security settings when viewing disk and printer shares on a computer running the ASDU server, Windows NT Server, or Windows NT Workstation.

Note the following Windows 95 considerations:

- Some administrative tasks require that you log on or enter your password for verification before you can perform an action. These password prompts ensure that you have administrative privilege for the server on which you are administering.
- You can create trust relationships between domains but you cannot verify them.
- The following methods for selecting an object to administer do *not* work on a PC running Windows 95:
  - You cannot administer print queues through the Printers list in the My Computer window. These print queue objects represent print queues local to your Windows 95 computer, even if the queue is redirected to an ASDU server print queue.
  - You cannot use the Windows 3.*x* Printer Manager. The Printer Manager does not exist in Windows 95; the Printers icon in the Main group of the Program Manager is a shortcut to the Printers list in My Computer window.
  - You cannot use the File Manager in the Program Manager window. Installing Windows NT Server Tools does not add a Security menu to the File Manager as it does for Windows 3.*x*.

Installing on a Windows 3.x and Windows for Workgroups System

Follow these steps to install the User Manager, Server Manager, and Event Viewer interfaces locally on a PC running Windows 3.x or Windows for Workgroups:

1. Ensure that the Client-based Advanced Server Administration Tools subset is installed on the ASDU server.
2. Map a network drive to the `astools` disk share on the ASDU server.
3. Select the `windows` folder.
4. Install the interfaces by running the `setup.exe` program.
6. Once the interfaces are installed, disconnect the network drive to the `astools` disk share and create icons for the Server Manager, User Manager for Domains, and Policy Editor interfaces.

Note the following Windows 3.x or Windows for Workgroups considerations:

- When you install the Windows NT Server Tools program group on a PC running Windows 3.x or Windows for Workgroups, the File Manager is modified to provide a new option on the Security menu. This option provides you with the

ability to display and set file and directory permissions, and to view and take ownership of files on an ASDU server.

- The Print Manager for Windows NT Server is available, which allows you to manage shared print queues on the ASDU server.

Password Management Utility

The Change Password utility is a windows-based utility that enables a user to set their domain user account and DIGITAL UNIX account or Network Information Service (NIS) passwords at the same time.

You install the Password Management utility independently of the of the Windows NT Administrative interfaces.

Follow these steps to install the Change Password utility on a PC running either Windows NT or Windows 95:

1. Ensure that the Client-based Advanced Server Administration Tools subset is installed on the ASDU server.
2. Map a network drive to the `astools` disk share on the ASDU server.
3. Select to the `asdupass` folder.
4. Change to the `i386` directory.
5. Install the Change Password utility by running the `setup.exe` program. Follow the instructions on the screen.
6. Once the interface is installed, disconnect the network drive to the `astools` disk share.

Using the Password Management Utility on a Windows 95 System

The Password Management utility is integrated with the Windows 95 password utility. Follow these steps to use the Change Password utility to change your passwords:

1. Start the Password Management utility by selecting the Passwords icon from the Control Panel.

   The Password Properties dialog box displays.

2. Click on the Change Other Passwords… button.

   The Select Password dialog box displays.

3. Select either the ASDU UNIX or NIS password option to change your DIGITAL UNIX or NIS password, or select the Microsoft Networking option to change your domain user account password, and click on the Change… button.

   With either option a Change Password dialog box is displayed.

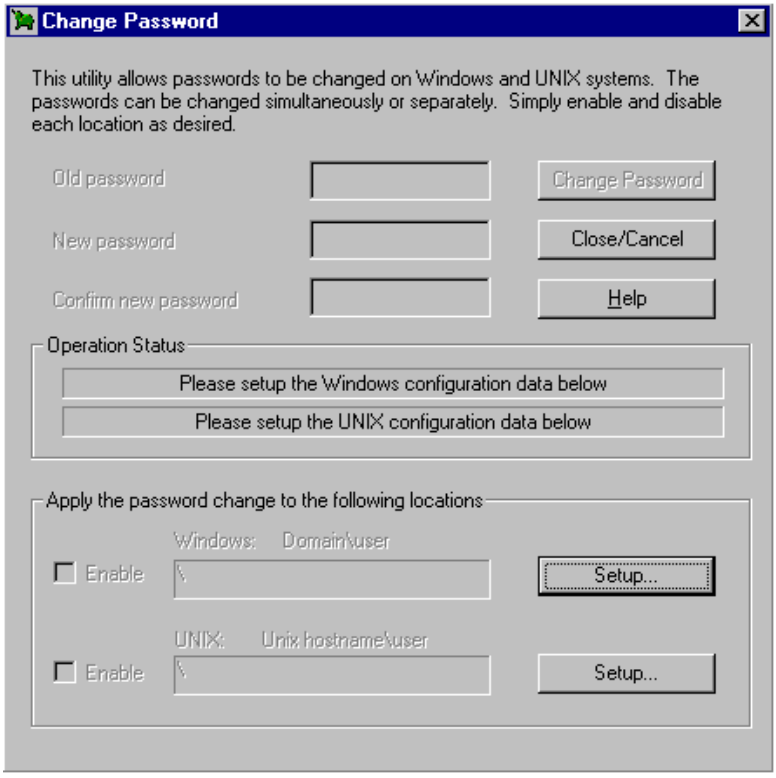
4. Enter your old, new, and confirmed new passwords in the Change Password dialog box.

Using the Password Management Utility on Windows NT System

Follow these steps to start the Password Management utility on a PC running Windows NT:

1. Expand the Programs option from the Start button.
2. Select the ASDU Password option and the Password Management utility starts.

   The following figure shows what the password Management utility looks like when it starts:



Users enter their old and new passwords in the password fields, then choose the account to which they want to apply the change by clicking on the Setup… button. They can then:

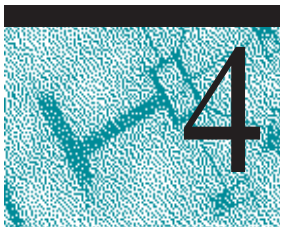
- Click on the Setup… button next to the Windows section to change their domain user account password.
- Click on the Setup… button next to the UNIX section to change their DIGITAL UNIX or NIS password.

In either case a dialog box is displayed in which users supply specific user and server information.

For More Information

For more information install the Password Management utility and read the online help.

CHAPTER 4



Incorporating an ASDU Server in a TruCluster Environment

By using DIGITAL's TruCluster software products, you can build a network infrastructure that enables Microsoft Windows clients to remain connected to and use domain resources when the DIGITAL UNIX system on which ASDU is installed becomes unavailable.

This chapter:

- Introduces to TruCluster family software
- Describes how to configure the ASDU server in a TruCluster environment
- Describes how to remove the ASDU server from a TruCluster environment

Using ASDU in a TruCluster Environment

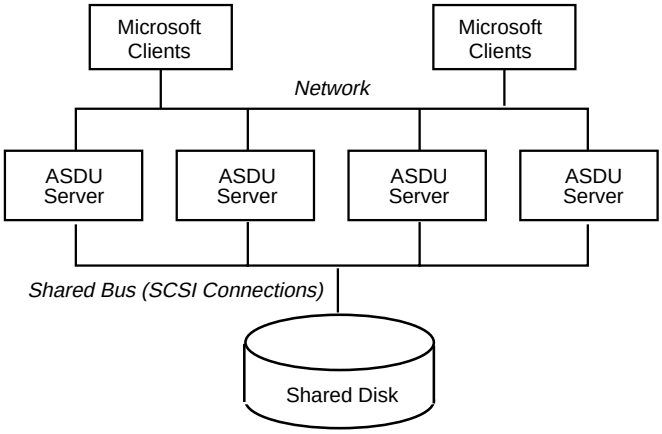
The TruCluster software detects when a DIGITAL UNIX server becomes unavailable and automatically stops the resources that are configured as TruCluster services on that server and restarts them on another eligible DIGITAL UNIX server.

You can configure the ASDU software as a TruCluster disk service. DIGITAL UNIX servers that run the ASDU software as a TruCluster disk service must use a SCSI-connected shared bus to access a common disk that contains ASDU-related configuration and data files, such as the ASDU share database and the user account database.

Systems running the TruCluster software use the director and agent daemons to monitor their own processes, SCSI I/O devices, power circuits, and network components for evidence of failure. When a failure is detected, the TruCluster software runs an ASDU shutdown action script that stops the ASDU server on the failed system and then runs an ASDU startup action script that starts (relocates) the ASDU server on an alternate DIGITAL UNIX system. The alternate system assumes the identity and responsibility of the failed ASDU server and continues with normal ASDU server operations.

ASDU shutdown and startup scripts are supplied with the ASDU software.

The following figure shows a typical TruCluster environment with the ASDU server running on four DIGITAL UNIX servers, which are sharing buses and disk storage:



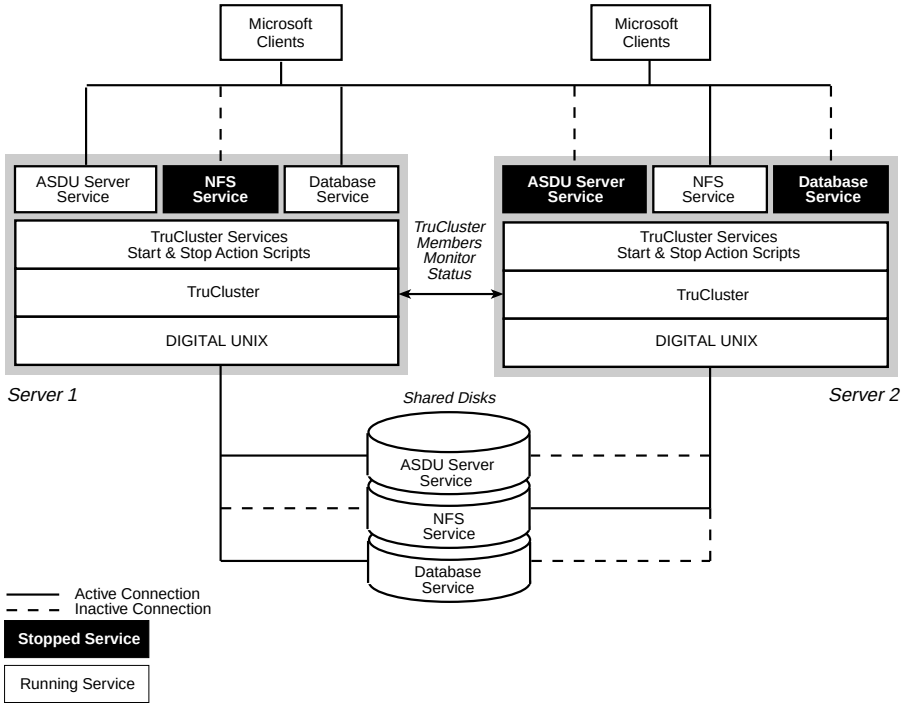
Transferring Services

This section depicts the relationships between two servers named Server1 and Server 2, the shared disk, and the TruCluster services named Advanced Server service, NFS service, and Database service before a failure, during a failure, and after a failure.

The following figures show how TruCluster services transfer when a DIGITAL UNIX server experiences a failure.

Before a Failure

The following figure illustrates the TruCluster services supported by each server before a failure occurs:



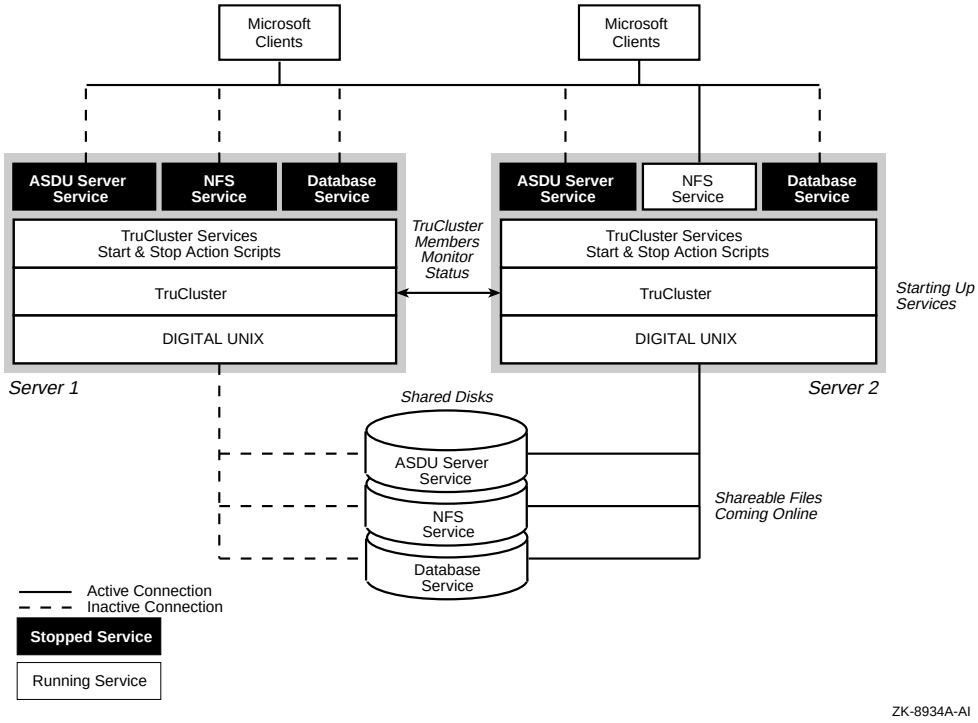
Server1 runs the ASDU server service and a database service. The NFS service is stopped.

Server2 supplies the NFS service. Its ASDU server service and database service are stopped.

The TruCluster software continuously monitors the status of the network and both systems.

During a Failure

The following figure illustrates what happens during a failure:



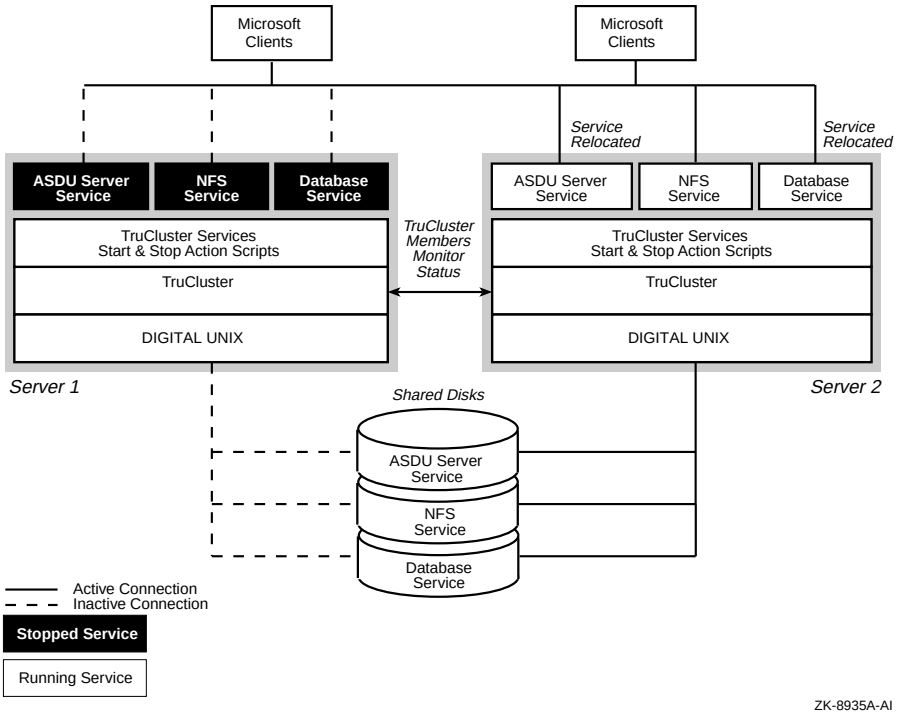
When the TruCluster software detects a failure in Server1, the shutdown action script executes and the ASDU service and database service are immediately stopped.

The startup action script executes on Server2 and it starts the stopped ASDU service and database service. Its NFS service continues without interruption.

The DIGITAL UNIX operating system unmounts the connections to Server1 and mounts the Server2 connections to bring the shareable files online for the relocating services.

After Failover

The following figure illustrates the status and the origin of TruCluster services after the failover action is complete:



Server2 now runs all services: the NFS service and the relocated ASDU server and database services.

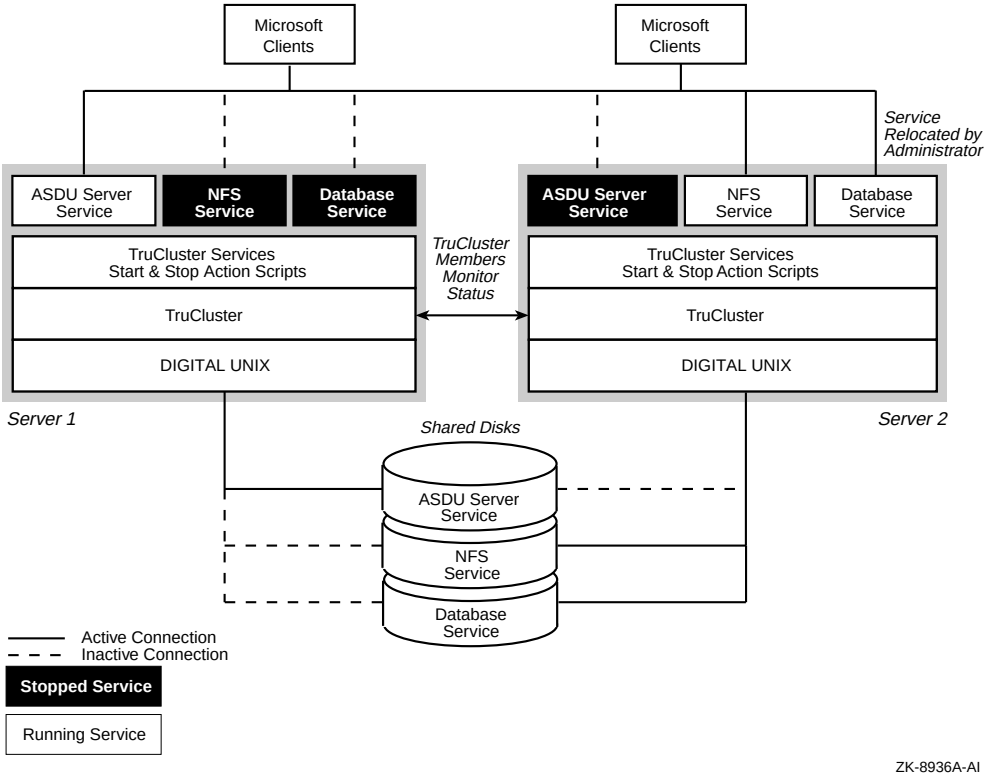
The services on Server1 are inactive.

If no copies were occurring during failover, Microsoft clients do not notice the relocation of the ASDU server from Server1 to Server2 since the ASDU server service running on Server2 assumed the identity and responsibility of the stopped ASDU server that was running on Server1.

Administering the Relocation of a Service

You can use the `asemgr` or `cmon` utility to force the relocation of a service from one server to another for the purposes of load-balancing or to prepare for maintenance activity on a system.

The following figure shows the end result of a typical service relocation. In this example the ASDU service is relocated back to Server1 from Server2.



Recovering from Failover

When the ASDU disk service relocates from one server to another, it may appear to users that the ASDU server experienced a restart or became unavailable for an interval of several seconds.

The way in which shared printers and PC clients respond to such restarts, depends on both the application and the PC operating environment as described in the following sections.

Microsoft Clients

Microsoft clients, in general, reestablish their connections to the ASDU server after an ASDU service failover.

If a client is not using network resources when the failover occurs, the failover process is transparent to you. Connections appear to remain stable and you remain logged in.

If you are using a domain resource during a failover, you are likely to see any number of messages similar to: `Abort, Retry, Fail: Unable to locate primary DC`. If you suspect that a failover is occurring, ignore messages of this type and retry the operation in a few minutes.

The exception to this is when running applications resident on the shared disk. For example, if you are running Microsoft Office from the shared disk, you may receive an error message because the application can no longer access the executable file from the server.

Different applications exhibit different behaviors. In some cases, after a severe error, proper cleanup is not done and you may have to exit and reenter Windows to force a cleanup of memory. Even in this case, connections to the server remain stable and you remain logged on to the server.

In many cases, the best action is to wait until the failover is complete and then continue your activities.

MS-DOS Clients

MS-DOS clients experience a short delay during failover while the TruCluster software relocates services and starts up the ASDU server. If you attempt to access a share before failover is complete, your PC may hang and require rebooting.

Shared Printers

Clients using network-shared printers experience a short delay while the TruCluster software relocates services and starts up the ASDU server. If you attempt to access a network printer before failover is complete, the behavior you witness and the

messages you receive depend on your PC computing environment. It is likely that if a failover occurs, the print job queue is not recoverable.

Printers connected directly to PC clients do not receive failover support.

Configuring an ASDU Server in a TruCluster Environment

You must perform the following tasks to configure the ASDU server in a TruCluster environment:

- Install the TruCluster and ASDU software on all the systems that will participate in the environment

  Note: Do not run the `asusetup` utility to configure the ASDU server.

- Create the TruCluster disk service for the ASDU server on one of the servers
- Configure the ASDU servers

The following sections describe these tasks.

ASDU and TruCluster Software Prerequisites

Decide which systems will participate in the TruCluster and ASDU environment and install the TruCluster and ASDU software on each of them. Minimally you must have two systems; an active ASDU server and an alternate ASDU server. The alternate ASDU server will take over ASDU server responsibility if the active ASDU server fails.

For the TruCluster environment to fail over services from one server to another, compatible versions of all software products must be installed on each server.

In addition, all servers in the TruCluster environment must have firmware at the supported revision levels. If servers have different firmware revision levels, then problems may arise at boot time, particularly when a server with an earlier firmware revision boots before a server with a later firmware revision.

To determine the firmware revision level of a server, enter the following command at the DIGITAL UNIX command prompt as superuser (root):

```
# uerf | grep Firmware
```

For More Information

For information on installing the ASDU server, see Chapter 2 in this guide. For information on installing the TruCluster software, see the TruCluster Software Products *Software Installation* guide.

Creating a Disk Service

You use the `asemgr` utility to create a disk service for the ASDU server. You will need the following information when you create the disk service:

- Network information

  Servers in a TruCluster environment can use either the TCP/IP transport or the NetBEUI transport when failing over.

  If your server uses TCP/IP, it will not failover properly unless the ASDU service for the server has a unique name and TCP/IP address assigned. The name associated with the TCP/IP address must be the same as the ASDU server name.

  All servers in the TruCluster environment and all PC clients interfacing to the ASDU service must know the TCP/IP name and address.

  Each server in the TruCluster environment must have an entry in its `/etc/hosts` file for the ASDU service. The entry must include the TCP/IP address and name for the ASDU service. For example, if the service name is `asdu` and the IP address assigned to the service is `141.116.217.75`, then a line similar to the following must be added to the `/etc/hosts` file:

  ```
  141.116.217.75 asdu
  ```

  Additionally, clients and servers that reside in different subnets must know the name and address of the service either by adding an entry for the service in the local `lmhosts` file or through a DNS or a WINS server.

- The location of the shared disk

  The shared disk may be a single disk, multiple disks, mirrored disks, or a disk array that is accessible to the servers participating in the environment. The capacity of the shared disk resource must be sufficient to accommodate the following:

  – The ASDU files, which requires approximately 37 MB.

  – The shared files area for the client users. This disk space requirement varies considerably depending directly on the number of users and their disk space usage.

- The location of the stop and start scripts, which is:

  ```
  /usr/net/servers/lanman/scripts/asuase_stop
  ```

  ```
  /usr/net/servers/lanman/scripts/asuase_start
  ```

For More Information

For information on creating a disk service, see the TruCluster Software Products *Software Installation* guide.

To create a TruCluster disk service for the ASDU server, perform the following tasks:

1. Edit the `/etc/hosts` file and add the TCP/IP name and address assigned to the service.

2. Log in as superuser (root) and start the TruCluster `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The `asemgr` utility displays the ASE main menu.

3. Choose the Managing ASE Services option.

   The Managing ASE Services menu is displayed.

4. Choose the Service Configuration option.

   The Services Configuration menu is displayed.

5. Choose the Add a new service option.

   The Add a service menu is displayed.

6. Choose the Disk Service option.

   A status message is displayed. You are prompted to enter a name for the disk service.

7. Enter a name for the disk service. This should be the same name that you will use as the ASDU server name when you configure the ASDU server.

   You are prompted to assign a TCP/IP address to the disk service.

8. Enter yes to assign a TCP/IP address.

   The TruCluster software locates the TCP/IP address for the service in the `/etc/hosts` file.

   You are prompted for the location of the shared disk.

9. Enter the location of the shared disk for the service. For example, `/dev/rz10c.`

   You are prompted to enter the mount point for the shared disk.

10. Enter a mount point. For example, `/asdu.`

    You are prompted for the type of access to the mount point.

11. Enter 1, Read-write.

You are prompted to optionally enable user and group quotas.

12. Enable quotas by using the default files provided or supply a full path to a file that you choose. Enter none to disable quotas.

    You are prompted to optionally provide mount options.

13. Enter the options you want or press return to choose the default options, which are listed in the `mount` reference page.

    You are prompted to enter information about another shared disk.

14. Optionally, enter the location of another shared disk to be used by the service and repeat steps 8 through 12. Press return to continue.

    The Modifying user-defined scripts for the service menu is displayed.

15. Choose the Start action script option.

    The Modifying the start script for the service menu displays.

16. Choose the Add a start action script option.

    You are prompted for the full path name for the start action script.

17. Enter the following pathname:

    ```
    /usr/net/servers/lanman/scripts/asuase_start
    ```

    You are prompted to enter an argument list for the script.

18. Press return.

    You are prompted to enter a time out period (in seconds).

19. Press return to choose the default value.

    The Modifying the start script for the service menu is displayed.

20. Choose the Exit option.

    The Modifying user-defined scripts for the service menu is displayed.

21. Repeat steps 14 through 19, replacing the word start with stop in steps 14, 15, and 16.

    The Modifying the stop script for the service menu is displayed.

22. Choose the Exit option until the Selecting an Automatic Service Placement (ASP) Policy menu is displayed.

23. Choose the Favor Members option.

A list of system names is displayed. You are prompted to select the systems to which the service will fail over.

24. Choose the systems in the order in which you want the service to fail over.

    You are prompted to relocate the server to a more highly favored member if one becomes available.

25. Choose no if you want the service to remain on the system that it failed over to even after the system that it was originally running on returns to the cluster.

    You are prompted to add the service.

26. Answer yes.

    The service is added.

Configuring the ASDU Servers

ASDU servers participating in the TruCluster environment share a common set of ASDU user, share, and registry data files. They do not share transport configuration information, and therefore, you must use the `asusetup` utility to configure each ASDU server to provide the transport information.

Decide which system will be the active server. Follow these steps to configure the active ASDU server:

1. Log in as superuser (root) to the system that you want to be the active server and run the `/usr/sbin/asusetup` utility.

   The `asusetup` utility detects if the TruCluster software is installed on the system and, if so, asks if the server will participate in a TruCluster environment.

2. Answer yes.

   The `asusetup` utility prompts you for the TruCluster disk service name and mount point.

3. Enter the disk service name and mount point.

   The configuration proceeds normally.

   See Chapter 2 for more information on configuring the ASDU server.

Follow these steps to configure the alternate ASDU servers:

1. Log in as superuser (root) to the alternate server and run the `/usr/sbin/asusetup` utility.

   The `asusetup` utility detects if the TruCluster software is installed on the system and, if so, asks if the server will participate in a TruCluster environment.

2. Answer yes.

   The `asusetup` utility prompts you for the TruCluster disk service name and mount point.

3. Enter the disk service name and mount point.

   You are prompted for transport information for the ASDU server.

4. Enter the transport information for the ASDU server.

   See Chapter 2 for more information on configuring the transport information for the ASDU server.

   Because the alternate ASDU server assumes the identity and role of the active ASDU server if that server becomes unavailable, no other configuration information is needed.

Administering an ASDU Server in a TruCluster Environment

Use the following information to help you administer an ASDU server in a TruCluster environment.

Maintaining the Shared Disk and Shares

When you set up the ASDU server as a disk service in a TruCluster environment, you automatically establish links to the shared disk in the following directory:

```
/usr/net/servers/lanman/shares
```

Shares that you create in this directory, or in any other directory on the shared disk, are accessible by all systems running the TruCluster software after failover.

You must ensure that shares created prior to setting up the ASDU server as a TruCluster disk service are located on the shared disk. You must create new shares on the shared disk to take advantage of failover protection. Shares created on a nonshared or local disk are not accessible by other systems after a failover.

Maintaining User Accounts

In a TruCluster environment the ASDU server requires that the DIGITAL UNIX `passwd` and `group` files on all systems contain identical user information for ASDU. Each time you add, modify, or delete a domain user account on a system, the ASDU server updates its data files, and the local `passwd` and `group` files. Other systems in the TruCluster environment cannot access this modified information,

even if the environment includes Network Information Service (NIS) master and slave servers.

You can include NIS servers in a TruCluster environment if you create DIGITAL UNIX user accounts for each user on the NIS master server before you create their domain user accounts. The NIS master server propagates the information to a slave server on each system. The ASDU server need not create the DIGITAL UNIX accounts because they exist.

If you do not to include NIS in the TruCluster environment or create the DIGITAL UNIX accounts for domain user accounts in advance, you must manually update the local `passwd` and `group` files. When user account information changes for one system, you must update that information in the `passwd` and `group` files on all other systems.

Maintaining Print Services

In a TruCluster environment, the shared disk maintains information for each shared ASDU printer and print service configured on the active server. If you modify information about print services in the `/etc/printcap` file on the active system, then you must modify the `/etc/printcap` file on the alternate servers to include the same information.

Only printers shared through network connections have failover recovery protection. The TruCluster software has no knowledge of local printers, that is, those connected directly to client PCs.

Removing ASDU Servers from a TruCluster Environment

You may need to alter the configuration of a TruCluster environment by removing the ASDU servers from one or more systems. You can do this in the following ways:

- Remove an ASDU server from the TruCluster environment. This method leaves the data files on the shared disk, which will no longer be accessible to the ASDU server that is being removed from the TruCluster environment.
- Remove all ASDU servers from the TruCluster environment. This method allows you to transfer the ASDU data files on the shared disk to the local disk of an ASDU server of your choice. This ASDU server continues to use and maintain the information.

Removing an ASDU Server

You can remove an ASDU server from a TruCluster environment in by performing the following tasks:

1. If the system you want to remove from the TruCluster environment is currently running the TruCluster ASDU service, then relocate the service to an alternate system.
2. Restrict the system you want to remove from running the TruCluster ASDU service.
3. Either deinstall ASDU from the system or reconfigure the ASDU server to remove it from the TruCluster environment.

Relocating the TruCluster ASDU disk service

Follow these steps to relocate a TruCluster ASDU disk service from the active server to an alternate server:

1. Log in as superuser (root) and start the TruCluster `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.

2. Choose the Managing ASE Services option.

   The Managing ASE Services menu is displayed.

3. Choose the Relocate a service option.

   The Select the service that you want to relocate menu is displayed.

4. Enter the number that represents the ASDU service you want to relocate.

   The Select member to run *'service name'* service menu is displayed.

5. Enter the number that represents the ASDU server to which you want to relocate the service.

   A status message indicates whether or not the relocation was successful.

Restricting a system from running the TruCluster ASDU service

Follow these steps to remove a system from the TruCluster ASDU service:

1. Log in as superuser (root) and start the TruCluster `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.

2. Choose the Managing ASE Services option.

   The Managing ASE Services menu is displayed.

3. Choose the Service Configuration option.

   The Service Configuration menu is displayed.

4. Enter the number that represents the ASDU service.

   A list of modification options is displayed.

5. Choose the Restrict Membership option.

   A list of members displays.

6. Choose to restrict the member you want to remove from running the ASDU TruCluster disk service.

Deinstalling the ASDU server

You can deinstall the ASDU server from a system by removing the ASDU subsets. Follow these steps to remove ASDU subsets:

1. Log in to the DIGITAL UNIX system as superuser (root) and notify PC users that the Advanced Server will be unavailable.

2. Display the installed Advanced Server subsets by entering the following command:

   ```
   # /usr/sbin/setld -i | grep ASU | grep installed
   ```

3. Enter the `/usr/sbin/setld -d` command followed by the name of the subset(s) that you want to remove. For example:

   ```
   # /usr/sbin/setld –d ASUADM400 ASUBASE400 ASUMANPAGE400
   ASURNOTE400 ASUTRAN400
   ```

   During the deinstallation you are prompted to reconfigure the ASDU server, resulting in its removal from the TruCluster environment.

4. Answer yes.

   While the ASDU subsets are being removed you may be prompted to save data files. You can answer no since the data files are saved on the shared disk.

   Deinstalling the ASDU subsets does not remove files and directories that were created in the ASDU directory structure by users. You may want to delete any directories and files still remaining in the `/usr/net/server/lanman` directory path.

Removing the ASDU server from the TruCluster environment

Follow these steps to remove an ASDU server from the TruCluster environment:

1. Log in as superuser (root) and start the ASDU `asusetup` utility as follows:

   ```
   # asusetup
   ```

   The `asusetup` utility detects if the ASDU server was configured to run as a TruCluster service and prompts you to respond whether or not you want to continue to run as part of the TruCluster disk service.

2. Answer no.

   The `asusetup` utility prompts you to reconfigure the ASDU server.

3. Answer yes to configure the ASDU server. The `asusetup` utility continues with normal configuration prompts and procedures.

   Answer no to exit the `asusetup` utility and, if desired, use the `setld` command to delete the ASDU subsets from the system.

   See Chapter 2 for more information on configuring the ASDU server.

Removing All ASDU Servers from a TruCluster Environment

You can remove all of the ASDU servers from a TruCluster environment in by performing the following tasks:

1. Decide on which system will receive the ASDU data files from the shared disk, and if necessary, relocate the TruCluster ASDU service to that system.
2. Restrict the TruCluster ASDU service to run on only the system that will receive the data files in step 1.
3. Reconfigure the alternate ASDU servers to remove them from the TruCluster environment.
4. Reconfigure the active ASDU server to remove it from the TruCluster environment. The ASDU data files are moved from the shared disk to the local disk.
5. Remove the TruCluster ASDU service.

Relocating the TruCluster ASDU disk service

If the ASDU server to which you want to transfer the data files is not the active server, then use the following steps to relocate the ASDU service to that server:

1. Log in as superuser (root) and start the TruCluster `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.

2. Choose the Managing ASE Services option.

   The Managing ASE Services menu is displayed.

3. Choose the Relocate a service option.

   The Select the service that you want to relocate menu is displayed.

4. Enter the number that represents the ASDU service you want to relocate.

   The Select member to run *'service name'* service menu is displayed.

5. Enter the number that represents the ASDU server to which you want to relocate the service.

   A status message indicates whether or not the relocation was successful.

Restricting the TruCluster ASDU service to run on a single system

Follow these steps to restrict the TruCluster ASDU service to run on a single system:

1. Log in as superuser (root) and start the TruCluster `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.

2. Choose the Managing ASE Services option.

   The Managing ASE Services menu is displayed.

3. Choose the Service Configuration option.

   The Service Configuration menu is displayed.

4. Enter the number that represents the ASDU service.

   A list of modification options is displayed.

5. Choose the Restrict Membership option.

   A list of members displays.

6. Choose to restrict all the members from running the ASDU TruCluster disk service leaving as a member only the system to which you want to transfer the data files.

Removing alternate ASDU servers from the TruCluster environment

Follow these steps to remove an ASDU server from the TruCluster environment:

1. Log in as superuser (root) and start the ASDU `asusetup` utility as follows:

   ```
   # asusetup
   ```

   The `asusetup` utility detects if the ASDU server was configured to run as a TruCluster service and prompts you to respond whether or not you want to continue to run as part of the TruCluster disk service.

2. Answer no.

   The `asusetup` utility prompts you to reconfigure the ASDU server.

3. Answer yes to configure the ASDU server. The `asusetup` utility continues with normal configuration questions and procedures.

   Answer no to exit `asusetup` utility and, if desired, use the `setld` command to delete the ASDU subsets from the system.

   See Chapter 2 for more information on configuring the ASDU server.

Removing the active ASDU server from the TruCluster environment

Follow these steps to remove the active ASDU server from the TruCluster environment:

1. Log in as superuser (root) and start the ASDU `asusetup` utility as follows:

   ```
   # asusetup
   ```

   The `asusetup` utility detects if the ASDU server was configured to run as a TruCluster service and prompts you to respond whether or not you want to continue to run as part of the TruCluster disk service.

2. Answer no.

   The `asusetup` prompts you to transfer the data files located on the shared disk to the local disk.

3. Answer yes.

   The `asusetup` utility prompts you to reconfigure the ASDU server.

4. Answer `yes`.

The `asusetup` utility continues with normal configuration prompts and procedures.

See Chapter 2 for more information on configuring the ASDU server.

Note: Be aware that if you configure the ASDU server as back up domain controller, then the user account database that was transferred from the shared disk to the local disk is overwritten by the user account database maintained by the primary domain controller.

Removing the TruCluster ASDU service

Follow these steps to remove the TruCluster ASDU disk service from the system:

1. Log in as superuser (root) and start the TruCluster `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.

2. Choose the Managing ASE Services option.

   The Managing ASE Services menu is displayed.

3. Choose the Service Configuration option.

   The Service Configuration menu is displayed.

4. Choose the Delete a service option.

   The Deleting a Service menu is displayed.

5. Enter the number that represents the ASDU disk service that you want to remove.

   A confirmation message is displayed.

6. Answer yes.

   The service is removed.

CHAPTER 5

Troubleshooting

This chapter describes how to troubleshoot some common problems related to the ASDU server. It identifies the various tools that you can use to learn about problems and offers possible solutions to common problems.

This chapter contains the following sections:

- Preventing Problems
- Learning About a Problem
- Solving ASDU Problems
- Solving Disk Share Problems
- Solving Browsing Problems
- Solving Printing Problems

Preventing Problems

You can use ASDU commands and utilities to track and monitor the status of the ASDU server. By doing so, you get a sense of how the ASDU server works under normal conditions and can watch for indications that the ASDU server may need adjustments before a problem arises.

Knowing the Statistics

You can use the `net statistics` command to display detailed statistics about the ASDU server's current usage and cumulative usage over a period of time. If you review the ASDU server statistics on a regular basis, you will find it easier to recognize and address changes in ASDU server operation.

The ASDU server maintains the following statistics:

Statistic	Shows
Statistics since	The date when this set of statistics began (either at the last server startup or the last time the statistics were cleared).
Sessions accepted	The number of times users connected to the server.
Sessions timed-out	The number of user sessions that were closed because of inactivity.
Sessions errored-out	The number of user sessions that ended because of error.
Kilobytes sent	The number of kilobytes of data the server transmitted.
Kilobytes received	The number of kilobytes of data the server received.
Mean response time (msec)	The average response time for processing remote server requests. This always will be zero (0) for DIGITAL UNIX system servers.
System errors	This statistic does not apply to DIGITAL UNIX system servers.
Permission violations	The number of times that a user attempted to access resources without the required permissions.
Password violations	The number of incorrect passwords that were tried.
Files accessed	The number of files that were used.
Comm devices accessed	This statistic is not supported on the ASDU server.
Print jobs spooled	The number of print jobs that were spooled to printer queues on the server.
Times buffers exhausted	The number of shortages of big and request buffers. Always set to zero (0) for DIGITAL UNIX system servers.

Reviewing Scripts

A benefit of the ASDU server is the availability of scripting features provided by the DIGITAL UNIX operating system. You can combine these features with the data gathering tools provided by the ASDU server to create a powerful tool that can assess the condition of the ASDU server at any given time.

For example, using the DIGITAL UNIX system job scheduling feature (CRON), various data gathering tools provided by ASDU, and some of the standard DIGITAL UNIX system commands for checking file system integrity and free space, you can

write scripts that perform various system and server checks and send the results to DIGITAL UNIX system administrators at regular intervals.

Reviewing Log Files

The ASDU server generates several log files that you can use to determine normal activity for the ASDU server. These log files are discussed in more detail in the following section.

Learning About Problems

You can use the utilities described in the following sections to learn more about ASDU server problems.

Alert Messages

The ASDU server sends a message to a specified list of users when an administrative alert occurs. Administrative alerts are generated by the system, and relate to server and resource use. They warn about security and access problems, user session problems, problems with services, server shutdown because of power loss when the UPS service is available, printer problems, and when registry parameters are exceeded.

The following examples illustrate situations that would generate an alert message:

- The number of server errors exceeds a threshold set in the ASDU registry.
- Errors were encountered during start of the Net Logon service.
- A printer is malfunctioning.

For alerts to be sent, the Alerter and Messenger services, which are usually enabled by default when the system starts, must be running on the computer originating the alert. For alerts to be received, the Messenger service must be running on the destination computer.

You can use the windows-based Server Manager utility to view and manage the list of users and computers that are notified when administrative alerts occur.

Log Files

The ASDU server provides a variety of log files that record server activity. Log files are generated in ASCII format that can be read by using a text editor or, in some cases a utility, to help determine the cause of a problem.

You should develop and implement a policy that includes a review of log files as a regular part of troubleshooting activities.

System, Security, and Application Log Files

A number of events related to the daily operation of the ASDU server can be tracked in one of three event logs: `system, security,` and `application.`

An event is any significant occurrence in the system (or in an application) that requires user notification. Some critical events are noted in on-screen messages. An event that does not require immediate attention is noted in an event log file located in the `/usr/net/server/lanman/logs` directory. Event logging starts automatically every time the ASDU server starts.

You can view event log files by using the windows-based Event Viewer utility or by using the `elfread` command at the DIGITAL UNIX command prompt.

The Event View utility (`eventvwr.exe`) should already be installed on PCs running Windows NT. It is available to PCs running Windows 95 from the `astools` disk share that was created when the Client-Based Advanced Server Administration tools subset was installed.

For More Information

For information about Event Viewer, see Chapter 3 in this guide or Chapter 7 in the Advanced Server for DIGITAL UNIX *Concepts and Planning* guide.

For more information on the `elfread` command, install the ASDU Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
man elfread
```

Printer Log Files

For each printer share and each DIGITAL UNIX system printer, the ASDU server maintains a print log that contains messages generated due to printer faults or print job errors. Printer log files are located in the `/usr/net/servers/lanman/shares/printlog` directory.

You should use a text editor to check these log files periodically to determine whether such errors have occurred.

Server Network Activity Log Files

If you suspect the presence of network problems, you can configure the ASDU server to write all the network packets that are generated or received by the ASDU server to an ASCII file located in the `/usr/net/server/lanman/debug` directory. The file is called `Debug-`*`pid`* where *`pid`* is the process identifier.

You can use a text editor to view the `Debug-`*`pid`* file to learn about the contents of the network packets.

To enable this feature, edit the `lanman.ini` file and set the following parameters in the `[lmxserver]` section:

```
debug=yes

debugsize=99999
```

You must then restart the server for the changes to take effect. When you restart the ASDU server, it will respond slowly since all network activity is being recorded to a file.

DIGITAL recommends that you enable the creation of a `Debug-`*`pid`* file only for the purpose of duplicating a problem. After the problem has been duplicated and a file has been generated, set the `debug` parameter to `no` to disable this feature.

If the problem is caused by a process that abnormally terminates, then a subdirectory specific to that process is created in the `/usr/net/server/lanman/debug` directory. The subdirectory is called `Crash-`*`pid`*, where *`pid`* is the process identifier for the process that terminated abnormally. A `core` file and a file called `StackTrace` are placed in the directory.

For example, if a process with a pid of 512 crashes, a `core` and a `StackTrace` are created in the following directory:

```
/usr/net/server/lanman/debug/Crash-512
```

You can use a text editor to view the `StackTrace` file to learn about the process termination.

Solving Common ASDU Server Problems

This section contains some of the common problems and recommended resolutions relating to the ASDU server.

Problem

The following message is displayed when the ASDU server starts:

```
unable to post servername on any network
```

Resolution

The NetBIOS network is not available. Run the `/usr/sbin/asuivp` utility to verify that NetBIOS installed correctly.

Problem

A large portion of the user community is having difficulty accessing the server.

Resolution 1: Verify the status of the physical network

Most of today's networking hardware provides status indicators that you can use to assess the state of the various network links (for example, 10-Base-T Hubs use LEDs). Check these links for signs of problems with the physical network such as excessive retransmissions, link integrity mismatches, and jabber conditions.

If a client cannot "see" anything on a network that is otherwise functioning without incident, then it is safe to assume that the problem is related to that client's network configuration. If however, that client can see other nodes on the network but cannot connect to a particular server, then the network path to that server, the server itself, or the account being used by that client are likely candidates for trouble.

Several third-party products are available that you can use to monitor the activity of the physical network. It is worthwhile to check network traffic periodically to see whether problems are occurring with the physical network.

Resolution 2: Verify that the server can communicate using TCP/IP

If the physical network appears to be functioning properly, then you should determine whether the various computers on the network can communicate with each other by using the TCP/IP transport protocol.

You can use the DIGITAL UNIX `ping` utility to test whether or not the TCP/IP transport protocol is working properly on clients and server.

If you cannot `ping` an ASDU server from a particular client, then that client will not be able to connect to the ASDU server when using the TCP/IP transport protocol. If you cannot `ping` an ASDU server from several client computers, then one of the following conditions may be present:

- The server is not running.

- The TCP/IP transport protocol is not running on the server.
- A configuration problem is disrupting network connectivity.

If the `ping` utility fails, run the `/usr/sbin/asuivp` utility to verify that the TCP/IP protocol is installed correctly.

For More Information

Review the recommendations in your transport protocol software documentation.

For more information on the `ping` utility, install the DIGITAL UNIX Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
man ping
```

Resolution 3: Verify that the server can communicate using NetBIOS

All ASDU server communications are based on NetBIOS name sessions. Therefore, connectivity between nodes using TCP/IP may be available but, if connectivity between NetBIOS names is not working, then the ASDU server will not work.

To determine if the server is communicating over the network, enter the following command at the DIGITAL UNIX command prompt:

```
net view
```

The name of the server and other servers operating in the same domain are displayed. If the server name is displayed, execute the same command, adding the server name. For example:

```
net view \\asutrial
```

The system displays a list of shared resources offered by the server.

Resolution 4: Verify DIGITAL UNIX system functionality

If all of the network connectivity modules are working properly, then verify the functionality of the DIGITAL UNIX operating system on the computer hosting the ASDU server. The operating system provides a variety of log files and system checks that you can use to verify proper operation. For information on these checks, see your DIGITAL UNIX system administration documentation.

The ASDU server is particularly sensitive to the following system problems:

- Insufficient disk space in critical file systems such as `root( / )` or `/var`
- Insufficient system memory, causing excessive swapping
- CPU bound conditions
- Unbalanced disk loads
- Improperly tuned kernel parameters, such as maximum number of open files

Resolution 5: Verify that the ASDU server is running

It is worthwhile to verify that the server is running. You can do this by entering the following command at the DIGITAL UNIX command prompt:

```
ps -ef | grep lmx
```

Executing this command generates a display similar to the following:

```
root   17726  1      0   12:03:36      0:00   lmx.alerter
root   17713  17461  0   12:03:32      0:00   lmx.srv -s 1
root   17722  17874  0   12:03:35      0:00   lmx.srv -s 2
root   17726  1      0   12:03:36      0:01   lmx.dmn
root   17728  1      0   12:03:36      0:01   lmx.browser
root   17744  1      0   12:03:28      0:00   lmx.ctrl
```

This report indicates that the three required server processes are running, the netlogon daemon (`lmx.dmn`), the control process (`lmx.ctrl`), and the `lmx.srv` server processes. Additional `lmx.srv` processes, each with a unique number displayed at the end of the line, may be displayed as in the preceding example. The server spawns new `lmx.srv` processes based on the number of clients supported by the server. As more client sessions are started, more `lmx.srv` processes may be started, each with a unique process ID and number. Information about other processes, such as `lmx.browser` and `lmx.alerter`, may be displayed.

Use the `lmstat` command to gather data from the server's shared memory image about the current state of the server. Executing the `lmstat -c` command usually provides information on which `lmx.srv` process is a connected client, for example:

```
Clients:
BANANA.SERVE~X (nwnum=0, vcnum=0) on 17713
ORANGE (nwnum=0, vcnum=0) on 17713
PEAR (nwnum=0, vcnum=0) on 17722
```

Notice that each client name has an associated process ID number. This is the process ID of the `lmx.srv` process that currently is serving that client. The `vcnum` value specifies whether this is the client computer's first VC or an additional one.

Being able to determine the process ID of the `lmx.srv` process that is serving a client is particularly useful when using `lmstat -w` or the DIGITAL UNIX system `truss( )` command. Both commands require a process ID as part of their startup arguments.

If the server is not running, enter the following command at the DIGITAL UNIX command prompt:

```
net start server
```

Resolution 6: Verify that all of the server services are running

If one of the required server processes is not running, determine whether all of the server services started properly. A situation can occur when several ASDU server processes are running but the server cannot be accessed because a particular service did not start. This is especially true for the Net Logon service. To check which services are running, enter the following command at the DIGITAL UNIX command prompt:

```
net start
```

A list of the services that currently are active on the server is displayed. If the Net Logon and Server services are not shown, then there is a problem with ASDU. Often the Net Logon service will not start because of a problem with the ASDU server name, domain name, or domain configuration.

Check the error logs for problems as described earlier in this chapter.

Resolution 7: Verify that all of the server resources are shared

Some ASDU server resources are automatically shared every time the ASDU server starts. These resources are used in the background by clients while performing other server activities. Resources that are shared as disk shares by default include:

```
ADMIN$
C$
D$
DOSUTIL
IPC$
NETLOGON
OS2UTIL
PRINTLOG
PRINT$
USERS
```

Disk shares ending in a dollar sign ($) are hidden and do not display when you browse the server. You can connect to a hidden share if you specify the share name as follows:

```
\\servername\sharename$
```

The `REPL$` disk share displays if the Directory Replicator service is running. The `ASTOOLS` disk share displays if the Client-Based Advanced Server Administrative Tools subset was installed.

Do not attempt to delete or reshare these resources. If any of these resources are absent, the server will not function properly. If you detect that one of these resources is missing, stop and restart the server to determine whether they are shared at server startup. If they are not displayed, contact your DIGITAL representative.

The remaining resources are default resources typically used by clients during logon (NETLOGON), to connect to home directories (USERS), and to access utilities or error logs (DOSUTIL, OS2UTIL, PRINTLOG). These items may be deliberately absent from your ASDU server. However, if you did not unshare them, then a problem with the ASDU server caused them to be removed.

Resolution 8: Determine if the ASDU registry has been corrupted

Execute the `regcheck -C` command to determine whether the internal format of the registry file has been corrupted. If corruption if found, execute the `regcheck -R` command to repair the registry file.

If invalid values were entered in the ASDU registry, then use the `regload` command to reinitialize all registry values to their defaults.

Use the `regconfig` command to query or change ASDU registry key information. You can use this command to change any value in the registry. (The Windows NT Registry Editor and the AS/U Administrator can also be used to change registry key values.) You can also use the `regconfig` command to reinitialize the ASDU registry with system defaults.

Resolution 9: Verify the parameters in the `lanman.ini` file

You can use the `srvconfig` command to display the settings of all the server parameters in the `lanman.ini` file.

Default settings are used for most of the parameters in the `lanman.ini` file. However, some of them can be changed, overriding the default values set at server installation.

To display a list of the parameters in the `lanman.ini` file and their settings, enter the following command at the DIGITAL UNIX command prompt:

```
srvconfig -p | more
```

For More Information

For more information about the `lanman.ini` file, see Appendix A.

Resolution 10: Determine if the user account database has been corrupted

You can use the `samcheck` command to check, dump, and fix the user accounts database. You use this command to determine whether the user accounts database has been corrupted and optionally, to fix it.

You can also use the `samcheck` command to output the contents of the user accounts database to `stdout` format, so you can view the contents from a terminal window.

Resolution 10: Determine if the ACL file has been corrupted

You can use the `acladm -c` command to determine whether the user `acl` file has been corrupted and optionally, to fix it.

Solving Common Share Problems

This section lists some common problems and recommended resolutions relating to the shared resources.

Problem

A user cannot connect to a share.

Resolution

Ensure that the ASDU server has not exceeded the maximum number of clients that it is configured to support. This number is indicated by the `maxclients` parameter in the server `lanman.ini` file. Enter the following command at the DIGITAL UNIX command prompt to display the value assigned to the `maxclients` key:

```
srvconfig “server, maxclients”
```

Problem

A user cannot access a file.

Resolution 1: Verify access

Use the Server Manager utility or the net commands to verify and set user’s ASDU permission to the file.

Use the DIGITAL UNIX `chmod` command to set the user’s DIGITAL UNIX permission to the file.

For More Information

For more information on setting ASDU permissions, see Chapter 3.

For more information on the `chmod` command, install the DIGITAL UNIX References Pages and enter the following command at the DIGITAL UNIX command prompt:

```
man chmod
```

Resolution 2: Check for open locks

When a user uses a shared file, the file is open. Sometimes a file will be left open, perhaps even with a lock on it, because of an application program error or some other problem. Such files remain open and unavailable to other users.

You can close these files to correct the access problem by using the `net session` command at the DIGITAL UNIX command prompt or from a Windows PC by following these steps:

1. Start the Server Manager utility.
2. Choose the Select Domain option from the Computer menu.
3. Specify the server that you want to administer in the Select Domains dialog box. Either type in the name of the server in the Domain: field or browse for the server in the Select Domain: section.
4. Double lick on the server name or highlight the name of the server and from the Computer menu select Properties.
5. Click on the IN USE button.
6. Highlight the open resource and select the Close Resource button.

Problem

Users can communicate with the server but cannot access a resource.

Resolution 1: Verify that the share exists

Verify that the shared resource exists by entering the following command at the DIGITAL UNIX command prompt:

`net view \\`*`servername`*

If the shared resource name is not displayed, then it does not exist and the resource must be shared again.

Resolution 2: Verify access

You should verify that the ASDU and DIGITAL UNIX group and user access permissions on the resource allow the user to perform the desired action. For example, the user may have read-only permission and be attempting to edit a file.

You should also ensure that DIGITAL UNIX system permissions are set to read and execute (RX) on all directories in the path leading to the file that users must access.

For More Information

For more information on setting permissions, see Chapter 3.

Resolution 3: Temporary files

Some programs, such as Microsoft Word, maintain temporary files by renaming the source file to a temporary name. Then, when the user saves the file, these programs create a new file with the name of the source file, and the temporary file is deleted.

The permissions that were assigned to a specific file are not assigned to the new file, which has the same file name. These permissions apply only to the original file, which was renamed to the temporary file name and then deleted. The ASDU server treats the updated file as a completely new file and it inherits the permissions of the directory in which it resides.

Files that are likely to be updated this way should be maintained in directories that have the permissions you want these files to inherit.

Solving Common Browsing Problems

This section lists some of the common problems and recommended resolutions relating to the Computer Browser service.

Problem

Information does not display when browsing an ASDU server.

Resolution

Restart the browser server by entering the following commands at the DIGITAL UNIX command prompt:

```
net stop browser
```

```
net start browser
```

Problem

The results from executing the `net view` command from a LAN Manager server do not display ASDU servers that are in the domain.

Resolution

Edit the ASDU registry and change the value of the `LmAnnounce` keyword to 1 (yes). The ASDU server then will broadcast LAN Manager-style server announcements. The `LmAnnounce` keyword is in the following key:

```
System\CurrentControlSet\Services\LanmanServer\Parameters
```

You must restart the server for the change to take effect.

Problem

The browse list on the backup domain controller does not contain all of the domain servers. For example, the list of servers that is displayed as a result of executing the `net view` command from a backup domain controller is incomplete.

Resolution

It can take as long as 12 minutes for the system to update the browse list. You can edit the ASDU registry on the backup domain controller to change the value of the

`BackupUpdate` parameter to the value (in seconds) for which updates are desired. Note that increasing the browse update time generates increased network traffic.

The `BackupUpdate` parameter is located in the following path:

`SYSTEM\CurrentControlSet\Services\Browser\Parameters`

You must restart the Computer Browser service for the change to take effect.

For More Information

For more information on changing registry values, see Chapter 2.

Solving Common Printing Problems

This section lists some of the common problems and recommended resolutions relating to the shared printer queues.

Problem

Windows NT client computers cannot connect to the printer.

Resolution

You must associate the printer with an appropriate printer driver. From a Windows NT client computer, follow these steps to change the printer driver association:

1. Select the printer whose driver you wish to change in the Printers folder.
2. Click on File Properties. If you receive a Printer Properties error, select "No." This may occur if a valid printer driver already has been installed.
3. Select the correct printer driver.
4. Share the printer if it is not already shared.

You may need to insert the Windows NT CD to obtain the appropriate driver. The system will confirm that the printer driver is being uploaded to the ASDU server.

Problem

Changes made to Windows NT client printers and jobs do not automatically display.

Resolution

Manually refresh the screen by pressing the F5 key. You should do this to update the screen whenever you pause, resume, delete, or add printers.

Problem

Printer name is invalid.

Resolution

Ensure that the printer name does not contain any spaces, and that the share name is the same as the printer name.

Problem

There is no separator page.

Resolution

You cannot use Windows NT to create separator pages for an ASDU server. Use the `net print` command at the DIGITAL UNIX command prompt to create and modify separator pages.

Problem

Print jobs in the queue are not printing.

Resolution

Ensure that:

- The printer cable is connected according to the printer manufacturer's instructions.
- The printer is turned on, selected (on line), has paper, is not jammed, and has no other obvious problems.
- The printer or printer queue has not been paused, held, or is in error. If it has been paused or held, continue or restart the printer or print queue.
- You can print from the DIGITAL UNIX system console. If not, consult your DIGITAL UNIX system documentation.

Problem

Characters sent to the printer are printing incorrectly.

Resolution

Refer to your printer manual to set the printer for "no parity."

Problem

A shared client printer is connected to parallel port LPT1 or PRN on your client computer. Print jobs sent to that printer over the network (rather than locally) do not print, although print jobs sent from your owner client computer do print, indicating that the printer itself is operational.

Resolution

Enter the `net use` command. If the display shows that the LPT1 or PRN port ID is linked to the printer, unlink that port ID; then link an unused port ID to the printer. The LPT1 or PRN port must be reserved for the physical connection to the printer.

Problem

You are using an application on a client to which a shared client printer is connected and occasionally your keyboard locks for a few seconds, especially when a print job is in progress.

Resolution

This hesitation at the keyboard is normal under these circumstances, especially when the printer is connected to a serial port.

Problem

Users cannot access ASDU printer shares and are receiving the following message:

```
"access denied"
```

Resolution 1: Verify access

You should verify that the ASDU and DIGITAL UNIX group and user access permissions allow the user to print.

For More Information

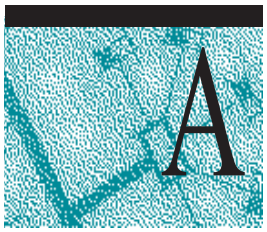
For more information on setting permissions, see the `net share` command in Chapter 3.

Resolution 2: Verify that the printer driver is available

Be sure that the printer driver that the client is using is installed on the ASDU server in the PRINT$ printer share.

APPENDIX A

The lanman.ini File



This appendix describes the `lanman.ini` file parameters that you can modify to improve ASDU server performance. It also contains tables that indicate the disposition of parameters that in earlier versions were in the `lanman.ini` file and now are in the ASDU registry.

When you install the ASDU server, the `lanman.ini` file contains some default parameter values. Additional parameters and the titles of the sections in which they reside are added when you change the ASDU server configuration. Only parameters with default values that have been changed are added to the `lanman.ini` file. If a parameter is not listed in the file (or is commented out with a semicolon), it is set to its default value.

Before you attempt to change any of the parameters in the `lanman.ini` file, you should understand the relationship between the entries and the server defaults.

Each server parameter has a default setting. To display and edit default settings, you can use the `srvconfig` utility, which is provided in the `/usr/net/servers/lanman/bin` directory.

You can edit the `lanman.ini` file to set parameters to values other than the defaults by locating (or adding) the appropriate section title in the file, and then adding the desired “parameter=value” entry.

The value assigned to any parameter in the `lanman.ini` file always supersedes the default value for that parameter.

File Syntax

Within each section of the `lanman.ini` file, parameters are specified as follows:

- The name of each parameter is at the beginning of a line, followed by an equal sign and the value assigned to it:

  ```
  parameter=value
  ```

- Comments start with a semicolon (;). If a semicolon precedes a parameter on the line, that parameter is ignored.

- When a list of values is assigned to a parameter, the values are separated by commas:

  ```
  parameter=value,value,value, ...
  ```

  (Exceptions to this rule display in the description of the appropriate parameter)

- When a value consists of a path, the path may be absolute, starting with a slash (/). If a path does not start with slash (/), it is assumed to be relative to the `lanman` directory.

- If a numeric value begins with zero (0) it is octal; if it begins with X it is hexadecimal; if it begins with a number from 1 to 9 it is decimal.

- When a parameter has no assigned value (nothing to the right of the equal sign), the value is zero (0) for a parameter that requires a number and null for a parameter that requires a character string.

- A null value is not valid for all parameters.

Follow these steps to change a parameter in the `lanman.ini` file:

1. Display the default settings for the server parameters by using the `srvconfig` command:

   ```
   /usr/net/servers/lanman/bin/srvconfig -p | more
   ```

2. Edit the `lanman.ini` file using the `vi` editor or a similar text editor. You may need to add a section heading to the file, for example `[lmxserver]`. You then need to add a “parameter=value” pair to the appropriate section of the `lanman.ini` file.
3. Stop and restart the server in order for the new values to take effect.

Alternatively you can use the `srvconfig -s` command to set parameter values in the `lanman.ini` file, as follows:

```
/usr/net/servers/lanman/bin/srvconfig -s \
“section,parameter=value”
```

For More Information

For more information on the `srvconfig` command, install the ASDU Reference Pages subset and enter the following command at the DIGITAL UNIX command prompt:

```
man srvconfig
```

File Parameters

The following tables describe the configurable parameters in the `lanman.ini` file, grouped according to the section of the file in which they reside.

Note: The `lanman.ini` file contains additional parameters that are not included in the following tables. These parameters are for debugging purposes and should not be modified

[server] Section Parameters

Parameter	Description, Values, and Default Setting
`listenname`	If set, this is the server's name on the network. If not set, the ASDU server may receive client connections from the DIGITAL UNIX listener on the DIGITAL UNIX machine name with a `.serve` extension (such as `liberty.serve`). The DIGITAL UNIX system machine name can be determined using the `uname -n` command. To change the value of the `listenname` parameter, use the `setservername` command. For more information about this command, install the ASDU Reference Pages subset and enter `man setservername` at the Advanced Server command prompt. Values: Any name of up to 15 English language characters, including letters, numbers, and the following characters: ! # $ % & ( ) - . ^ _ { } ~ ; Default: null
`maxclients`	Identifies the maximum number of simultaneous client sessions that the server can support. By default this number is equal to the number of ASDU licenses that are installed on the server computer.
`srvservices`	The list of keywords for the services that start automatically when the server is started. Because services are started in the order they appear in the `srvservices` entry, you must ensure that `netlogon` service appears before any services that require it. Default: `alerter, netlogon, browser`

[workstation] Section Parameters

Parameter	Description, Values, and Default Setting
`domain`	The name of the domain that includes the server. Values: Any name of up to 15 English characters, including letters, numbers, and the following characters: ! # $ % & ( ) - . ^ _ { } ~ ; Default: domain

[lmxserver] Section Parameters

Parameter	Description, Values, and Default Setting
`anncmailslot`	The name of the mail slot used for periodic server announcements. Values: A path up to a maximum of 256 characters. Default: *\MAILSLOT\LANMAN Note that back slashes must be doubled on input or else the entire input line must be enclosed in single quotation marks. (Type *`text`*`\\`*`text`* or *`'text\text'`* to enter text with a single back slash.)
`appsources`	The names of the modules that can write to the application log. Default: The server initializes the value of this parameter at startup.
`country`	The country code for server-generated messages. Values:

Country	Code	Country	Code
Asia	099	Latin America	003
Australia	061	Netherlands	031
Belgium	032	Norway	047
Canada	002	Portugal	351
Denmark	045	Spain	034
Finland	358	Sweden	046
France	033	Switzerland	041
Germany	049	United Kingdom	044
Italy	039	United States	001
Japan	081		

Default: 001

`lang`	Defines the character set that the ASDU server uses to process client requests. Default: C, which is U.S. English
`listenextension`	The extension that the DIGITAL UNIX system Listener program applies to the name of the server computer by default. This parameter is ignored if the `listenname` parameter in the `[server]` section is set. Values: 0-13 characters and a null value are acceptable. Default: .SERVE
`listennamechk`	If set to yes, this parameter forces any name specified with the `listenname` parameter to be different from the DIGITAL UNIX machine name or to be the DIGITAL UNIX machine name with a `.serve` extension in order to avoid name conflicts with the DIGITAL UNIX Listener. Default: no
`listenqlen`	Maximum number of client connection requests outstanding. If the server supports numerous clients that all attempt to connect to the server simultaneously, and some get refused, you should raise the value of this parameter. Only applicable if the `listenname= parameter` is used. Values: 1 – unlimited Default: 3
`maxfilesize`	The maximum file size, in KBytes, that the DIGITAL UNIX system redirector will allow a “local DIGITAL UNIX user” to create on a local system. Values: 100 – unlimited Default: 20000

`msdoscodepage` Sets the MS-DOS code page that the ASDU server uses when responding to a client's request.

The setting should be set to correspond to the locale to which the `lang` parameter is set to as described in the following table:

If the `lang` parameter is:	**Using this character set:**	**The default value for the `msdoscodepage` parameter is:**
Western European	ISO8859-1	cp850, however when using the en_US.ISO8859-1 locale, the default is cp437
Eastern European	ISO8859-2	cp852
Baltic	ISO8859-4	cp775
Cyrillic	ISO8859-5	cp866
Greek	ISO8856-7	cp737
Hebrew	ISO8859-8	cp862
Turkish	ISO8859-9	cp857
Japanes Shift-JIS	SJIS	SJIS
Japanese DEC Kanji	deckanji	SJIS
Japanese EUC	eucJP	SJIS
Japanese Super DEC Kanji	sdeckanji	SJIS
Thai	TACTIS	cp874
Simplified Chinese	dechanzi	dechanzi

`msgforward` Specifies if the ASDU server implements message forwarding between clients. DIGITAL recommends that you do no implement message forwarding.

Values: yes (implement forwarding) or no (do not implement forwarding)

Default: no

`nativelm` An additional field in the session setup request/response.

Default: ( )

`nativeos` An additional field in the session setup request/response.

Default: (DIGITAL UNIX)

`netmsgwait` The interval, in seconds, that the server waits for a response when it sends a message that requires one.

Values: 0 – unlimited

Default: 30

`network` The network device names and NetBIOS name-passing type for the network(s) the server should use.

Values: Sets four items separated by commas, each set of four separated from the next by a space. The following four items are in each set:

1. The device name for virtual circuit access.
2. The device name for datagram network access.
3. A digit identifying the NetBIOS interface convention used by the above two devices. There are two conventions compiled into the server: 0 = OSI NetBIOS convention; 1 = Wollongong TCP-IP NetBIOS convention.
4. The name of the transport provider, as returned by the nlsprovider system call. (For networks not configured to accept incoming connections through the DIGITAL UNIX system Listener program, this can be any arbitrary string.)

`prebinduxredir`	Controls the name that the DIGITAL UNIX system `net` command binds when it uses the DIGITAL UNIX system redirector (`uxredir`). If this parameter is set to yes, the server prebinds a NetBIOS name that will be used by all DIGITAL UNIX system `net` commands. Because this name is prebound, the `net` command, it does not need to bind its own name, and this quickens the DIGITAL UNIX system's network access to the server. If this parameter is set to no, then each `net` command uses its own unique name resulting in slower performance. Values: yes, no Default: yes
`secsources`	The names of the modules that can write to the security log. Default: The server initializes the value of this parameter at startup.
`stacksize`	The size of the stack, in bytes, for each task internal to the server. Values:12000 – unlimited Default: 20000
`syssources`	The names of the modules that can write to the system log. Default: The server initializes the value of this parameter at startup.

The lanman.ini File Parameter Mapping to Registry Keys

The following tables list the parameters in the `lanman.ini` file that existed in earlier versions of the Advanced Server software and indicates whether they have been moved to the ASDU registry, to the new `lanman.ini` file, or are obsolete. The parameters that were moved to the ASDU registry are listed with their new value names.

The `lanman.ini` file parameters are listed according to the sections in which they reside in the file.

[server] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
`accessalert`	LanmanServer\Parameters	AccessAlert
`alertnames`	Alerter\Parameters	AlertNames
`autodisconnect`	LanmanServer\Parameters	AutoDisconnect
`enablesoftcompat`	AdvancedServer\FileServiceParameters	EnableSoftCompat
`enable_soft_file_ext`	AdvancedServer\FileServiceParameters	EnableSoftFileExtensions
`erroralert`	LanmanServer\Parameters	ErrorAlert
`listenname`[1]	Control\ComputerName\ComputerName	ComputerName
`logonalert`	LanmanServer\Parameters	LogonAlert
`maxauditlog`	EventLog\Security	MaxSize
`maxclients`	None (`lanman.ini` file)	
`maxerrlog`	EventLog\System	MaxSize
`srvannounce`	LanmanServer\Parameters	SrvAnnounce
`srvcomment`	LanmanServer\Parameters	SrvComment
`srvhidden`	LanmanServer\Parameters	Hidden
`srvservices`	None (`lanman.ini` file)	
`userpath`	LanmanServer\Parameters	UserPath

[1] The listenname parameter is in the `lanman.ini` file as well as the ASDU registry under \SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName.

[workstation] Section Parameter Mappings to Registry Keys

Parameter	ASDU Registry Key Name	Value Name
`domain`	None (`lanman.ini` file)	

[uidrules] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
`exclude`	AdvancedServer\UserServiceParameters	Exclude
`forceunique`	AdvancedServer\UserServiceParameters	ForceUniqueUnixUserAccount
`maxuid`	AdvancedServer\UserServiceParameters	MaxUnixUid[1]
`minuid`	AdvancedServer\UserServiceParameters	MinUnixUid[1]
`usrcomment`	AdvancedServer\UserServiceParameters	UserComment

[1] These values are not displayed by default but can be configured in the ASDU registry.

[netlogon] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
`logonquery`	Netlogon\Parameters	LogonQuery
`maxclisess`	AdvancedServer\ProcessParameters	NumCLIENT_SESSION
`maxquery`	None (obsolete)	
`maxsrvsess`	AdvancedServer\ProcessParameters	NumSERVER_SESSION
`pulse`	Netlogon\Parameters	Pulse
`querydelay`	Netlogon\Parameters	QueryDelay
`randomize`	Netlogon\Parameters	Randomize
`relogondelay`	Netlogon\Parameters	RelogonDelay
`scripts`	Netlogon\Parameters	Scripts
`ssipasswdage`	Netlogon\Parameters	SSIPasswdAge
`update`	Netlogon\Parameters	Update

[lmxserver] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
aclfile	None (obsolete)	
aclgroup	None (obsolete)	
aclowner	None (obsolete)	
aclperms	None (obsolete)	
admingroupid	AdvancedServer\NetAdminParameters	NetAdminGroupName
adminpath	AdvancedServer\NetAdminParameters	NetAdminPath
adminuserid	AdvancedServer\NetAdminParameters	NetAdminUserName
alertadmin	None (obsolete)	
alerterrorlog	None (obsolete)	
alertmessage	None (obsolete)	
alerton	None (obsolete)	
alertprinting	None (obsolete)	
alertuser	None (obsolete)	
anncmailslot	None (lanman.ini file)	
appretention	Eventlog\Application	Retention
appsources	Eventlog\Application	Sources
auditretention	Eventlog\Security	Retention
blobmapping	None (obsolete)	
byemessage	AdvancedServer\Parameters	SendByeMessage
cntsharecache	AdvancedServer\ShareParameters	ShareCacheCount
cntsharereads	AdvancedServer\ShareParameters	ShareReadCount
controllock	None (obsolete)	
coreok	AdvancedServer\ProcessParameters	CoreOK
country	None (lanman.ini file)	
cpipgroup	None (obsolete)	
cpipname	None (obsolete)	
cpipowner	None (obsolete)	

(*continued*)

[lmxserver] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
cpipperms	None (obsolete)	
creatunixuser	AdvancedServer\UserServiceParameters	CreateUnixUser
dirperms	AdvancedServer\FileServiceParameters	UnixDirectoryPerms
eafileprefix	AdvancedServer\FileServiceParameters	EAFilePrefix
errorretention	Eventlog\System	Retention
errsources	None (obsolete)	
feabufsize	AdvancedServer\FileServiceParameters	MaxEASize
fileflush	AdvancedServer\FileServiceParameters	ForceFileFlush
fileperms	AdvancedServer\FileServiceParameters	UnixFilePerms
forcediracl	AdvancedServer\FileServiceParameters	ForceDirectoryAcl
forcefileacl	AdvancedServer\FileServiceParameters	ForceFileAcl
gcbuffer	AdvancedServer\Parameters	SizeGcBufferPoolInKB
getapipe	None (lanman.ini file)	
groupadd	None (obsolete)	
groupdel	None (obsolete)	
grpupdate	AdvancedServer\UserServiceParameters	GroupUpdateTime
hashsize	AdvancedServer\ProcessParameters	NumHashTables
ignoresigpwr	UPS\Parameters	IgnoreSIGPWR
ipctries	AdvancedServer\Parameters	MaxIpcTryCount
keepadmshares	AdvancedServer\ShareParameters	KeepAdministrativeShares
listenextension	None (lanman.ini file)	
listennamechk	None (lanman.ini file)	
listenqlen	None (lanman.ini file)	
lmaddonpath	None (lanman.ini file)	
lmxsrv	None (obsolete)	
lmxtimesource	None (obsolete)	
locale	None (obsolete)	
locknap	AdvancedServer\ProcessParameters	LockNapInMSec

(*continued*)

[lmxserver] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
lsafile	None (obsolete)	
lsagroup	None (obsolete)	
lsaowner	None (obsolete)	
lsaperms	None (obsolete)	
mailslotgroup	None (obsolete)	
mailslothold	AdvancedServer\Parameters	MaxMailslotReadTime
mailslotowner	None (obsolete)	
mailslotperms	None (obsolete)	
maxadminoutput	None (obsolete)	
maxapplog	EventLog\Application	MaxSize
maxdirbufsize	AdvancedServer\Parameters	MaxDirectoryBufferSize
maxfilesize	AdvancedServer\FileServiceParameters	MaxFileSizeInKB
maxlocknap	AdvancedServer\ProcessParameters	MaxLockTimeInSeconds
maxmsdepth	None (obsolete)	
maxmsgsize	AdvancedServer\Parameters	MaxMessageSize
maxmux	None (obsolete)	
maxopenfiles	None (obsolete)	
maxrawsize	AdvancedServer\Parameters	MaxRawSize
maxvcperproc	AdvancedServer\ProcessParameters	MaxVCPerProc
maxsvcwait	AdvancedServer\Parameters	MaxServiceWaitTime
maxvcs	AdvancedServer\ProcessParameters	MaxVCs
memorymap	AdvancedServer\FileServiceParameters	MemoryMapFiles
minsmbworkers	AdvancedServer\ProcessParameters	MinSmbWorkerTasks
minvcperproc	AdvancedServer\ProcessParameters	MinVCPerProc
msdirgroup	None (obsolete)	
msdirname	None (obsolete)	
msdirowner	None (obsolete)	

(*continued*)

[lmxserver] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
msdirperms	None (obsolete)	
msgforward	None (lanman.ini file)	
msgheader	Alerter\Parameters	IncludeMessageHeader
nativelm	None (lanman.ini file)	
nativeos	None (lanman.ini file)	
netaddonpath	None (lanman.ini file)	
nethelpfile	None (lanman.ini file)	
nethmsgfile	None (obsolete)	
netmsgwait	None (lanman.ini file)	
network	None (lanman.ini file)	
newusershell	AdvancedServer\UserServiceParameters	NewUserShell
nfslocks	AdvancedServer\FileServiceParameters	UseNfsLocks
nonexistusers	Alerter\Parameters	CountNotOnNetworkCache
nosendtime	Alerter\Parameters	NotOnNetworkCacheTimeout
numnetsndbufs	None (obsolete)	
oplocktimeout	AdvancedServer\FileServiceParameters	OplockTimeout
packageid	None (obsolete)	
passmgmt	None (obsolete)	
polltime	None (obsolete)	
prebinduxredir	None (lanman.ini file)	
qnamelen	AdvancedServer\Parameters	MaxPrintQueueNameLength
qsched	AdvancedServer\Parameters	CheckPrintQueueInMinutes
queuealloc	None (obsolete)	
rdatrend	AdvancedServer\FileServiceParameters	ReadAheadCount
relmajor	(\SOFTWARE\Microsoft\LanmanServer CurrentVersion (and elsewhere))	MajorVersion
relminor	(\SOFTWARE\Microsoft\LanmanServer CurrentVersion (and elsewhere))	MinorVersion
samdir	None (obsolete)	

(*continued*)

[lmxserver] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
samgroup	None (obsolete)	
samowner	None (obsolete)	
samperms	None (obsolete)	
sbstelladmin	AdvancedServer\AlertParameters	AlertAdminOnLicenseOverflow
sbstelluser	AdvancedServer\AlertParameters	AlertUserOnLicenseOverflow
schedlogfilename	None (obsolete)	
secsources	Eventlog\Security	Sources
sharefile	None (obsolete)	
sharegroup	None (obsolete)	
sharemkdir	AdvancedServer\ShareParameters	MakeUnixDirectoriesOnShare
shareowner	None (obsolete)	
shareperms	None (obsolete)	
shmgroup	None (obsolete)	
shmowner	None (obsolete)	
shmperms	None (obsolete)	
spareserver	AdvancedServer\ProcessParameters	KeepSpareServer
sparesrvtime	AdvancedServer\ProcessParameters	SpareServerTime
spipe	None (obsolete)	
srvstathelpfile	None (lanman.ini file)	
stacksize	None (lanman.ini file)	
startscript	None (obsolete)	
stoponcore	AdvancedServer\ProcessParameters	StopOnCore
svcinit	None (obsolete)	
svcscript	None (obsolete)	
syncaclfile	AdvancedServer\FileServiceParameters	SyncAclFileOnWrite
synchomedir	AdvancedServer\UserServiceParameters	SyncUnixHomeDirectory
syssources	Eventlog\System	Sources
terminator	None (obsolete)	

(*continued*)

[lmxserver] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
tokensidlimit	None (obsolete)	
unixdirchk	AdvancedServer\FileServiceParameters	UnixDirectoryCheck
unixlocks	AdvancedServer\FileServiceParameters	UseUnixLocks
useoplock	AdvancedServer\FileServiceParameters	UseOplocks
userremark	AdvancedServer\UserServiceParameters	UserComment
ustructs	AdvancedServer\ProcessParameters	NumUStructs
uxclosecount	AdvancedServer\FileServiceParameters	UnixCloseCount
vcdistribution	AdvancedServer\ProcessParameters	VCDistribution

[ups] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
poweraddr	UPS\Parameters	PowerFailAddress
powermessage	UPS\Parameters	PowerFailMessage
powertime	UPS\Parameters	PowerMessageInterval

[replicator] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
exportlist	Replicator\Parameters	ExportList
exportpath	Replicator\Parameters	ExportPath
guardtime	Replicator\Parameters	GuardTime
importlist	Replicator\Parameters	ImportList
importpath	Replicator\Parameters	ImportPath
interval	Replicator\Parameters	Interval
logon	Replicator	ObjectName
password	None (obsolete)	
pulse	Replicator\Parameters	Pulse

(*continued*)

[replicator] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
random	Replicator\Parameters	Random
repl_dirgroup	Replicator\Parameters	UnixDirectoryGroup
repl_dirowner	Replicator\Parameters	UnixDirectoryOwner
repl_dirperms	None (obsolete)	
repl_filegroup	Replicator\Parameters	UnixFileGroup
repl_fileowner	Replicator\Parameters	UnixFileOwner
repl_fileperms	None (obsolete)	
replicate	Replicator\Parameters	Replicate
tryuser	Replicator\Parameters	TryUser

[fsi] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
closeinodecnt	None (obsolete)	
fsaddonpath	None (lanman.ini file)	
fslibname	None (lanman.ini file)	
fslibpath	None (lanman.ini file)	
fsmap	None (lanman.ini file)	
fsnosupport	None (lanman.ini file)	
maxfstypes	None (obsolete)	
nfsroot	AdvancedServer\FileServiceParameters	RootOwnsFilesCreatedOnNFS
ntfs	AdvancedServer\FileServiceParameters	ReportNTFS
remotemounts	None (lanman.ini file)	

[psi] Section Parameter Mappings to Registry Keys

Parameter	ASDU Registry Key Name	Value Name
`maxspoolers`	None (obsolete)	
`psaddonpath`	None (`lanman.ini` file)	

[version] Section Parameter Mapping to Registry Key

Parameter	ASDU Registry Key Name	Value Name
`lan_manager`	None (obsolete)	

[netrun] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
`maxruns`	NetRun\Parameters	MaxRuns
`runpath`	NetRun\Parameters	RunPath

[browser] Section Parameter Mappings to Registry Keys

File Parameter	ASDU Registry Key Name (\SYSTEM\CurrentControlSet\Services)	Value Name
`backuprecovery`	Browser\Parameters	BackupRecovery
`backupupdate`	Browser\Parameters	BackupUpdate
`lmannounce`	LanmanServer\Parameters	LmAnnounce
`masterupdate`	Browser\Parameters	MasterUpdate
`morelog`	Browser\Parameters	MoreLog

Index

A

C

D, E, F

U