Advanced Server for UNIX

Installation and Administration Guide

September 2002

Product Version: Advanced Server for UNIX Version 5.1B or higher

Operating System and Version: Tru64 UNIX Version 5.1A or higher

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

Hewlett-Packard Company
Palo Alto, California

Contents

About This Guide

1 Installing the ASU Software

1.1 Preinstallation Tasks 1–1
1.1.1 Reviewing the ASU Documentation 1–1
1.1.2 ASU Software and Hardware Requirements 1–2
1.1.3 Determining a Method for User Account Authentication . 1–2
1.1.3.1 Windows 2000 Server Authentication 1–2
1.1.3.2 Windows NT Server Version 4.0 Authentication 1–3
1.1.4 Overview of ASU Administrative Interfaces 1–3
1.1.4.1 The ASU Commands 1–3
1.1.4.2 The net Commands 1–4
1.1.4.3 The Tru64 UNIX Commands and GUIs 1–4
1.1.4.4 The Windows GUIs 1–4
1.2 Upgrading the ASU Software 1–5
1.3 Installing the ASU Software 1–6
1.4 Postinstallation Tasks 1–7
1.4.1 Configuring ASU Network Information 1–8
1.4.2 Configuring ASU Server Information 1–10
1.4.3 Configuring Listen Names 1–11
1.4.4 Starting the ASU Server 1–12
1.4.5 Verifying the ASU Software Installation 1–12
1.4.6 Reconfiguring the ASU Software 1–13
1.5 ASU Directories 1–13
1.6 ASU Services 1–13
1.7 ASU Processes 1–14
1.8 Installing the Windows Based Interfaces 1–15
1.8.1 Installing or Running Administrative Interfaces on Windows NT 1–16
1.8.2 Installing Administrative Interfaces on a Windows 95 or Windows 98 System 1–16
1.9 ASU Licenses 1–18
1.10 Configuring International Support 1–19

2 Configuring the ASU Software

2.1 ASU Registry Overview 2–1
2.1.1 Value Entries 2–4
2.2 Viewing and Changing Registry Value Entries 2–5
2.2.1 The regconfig Command 2–6
2.2.2 Registry Editor 2–7
2.2.3 System Policy Editor 2–8
2.2.4 ASU Administrator 2–9
2.2.4.1 Installing the ASU Administrator Interface 2–9
2.2.4.2 Using the ASU Administrator Interface 2–10

3 Creating User Accounts

3.1 Domain User Account Attributes 3–1
3.2 Tru64 UNIX User Accounts Created by ASU 3–4
3.2.1 ASU and Tru64 UNIX User Account Attributes 3–5
3.2.2 ASU and Tru64 UNIX User Account Home Directories 3–6
3.2.3 Local or NIS Tru64 UNIX User Accounts 3–7
3.2.4 Tru64 UNIX and Domain Password Synchronization 3–9
3.2.4.1 Enabling the `SyncUnixPassword` Entry 3–9
3.2.4.2 Installing the Change Password Utility 3–10
3.2.4.2.1 Using the Password Management Utility on a Windows 95 System 3–11
3.2.4.2.2 Using the Password Management Utility on a Windows NT System 3–11
3.3 Disabling ASU from Creating Tru64 UNIX User Accounts 3–12
3.4 Creating a Domain User Account 3–12
3.4.1 Using the net user Command 3–13
3.4.2 Using the User Manager for Domains 3–15
3.5 Domain and Tru64 UNIX User Account Mapping 3–16
3.6 Using Windows NT Server Version 4.0 Authentication 3–17
3.6.1 Logging In To a Tru64 UNIX Application 3–17
3.6.2 Specifying Only Tru64 UNIX Authentication 3–18
3.6.3 Changing Passwords 3–19
3.7 Deleting a Domain User Account 3–19
3.8 Grouping Domain User Accounts 3–20
3.8.1 Creating and Administering a Domain Group 3–20
3.8.1.1 Using the net Command 3–21
3.8.1.2 Using the User Manager for Domains 3–21
3.8.2 Deleting a Domain Group 3–22
3.8.2.1 Using the net Command 3–22

3.8.2.2 Using the User Manager for Domains 3–22

4 Creating ASU Disk Shares

4.1 Default Disk Share Attributes 4–1
4.1.1 Disk Shares Created By ASU for NFS Exported File Systems 4–1
4.1.1.1 Converting NFS Permissions 4–2
4.1.1.2 Managing NFS Related Disk Shares Created by ASU 4–3
4.1.1.3 Controlling the ASU Creation of NFS-Related Disk Shares 4–3
4.1.1.4 Configuring ASU to Not Create NFS-Related Disk Shares 4–4
4.2 Special Disk Shares 4–4
4.3 Disk Share Attributes 4–5
4.4 Creating a Disk Share 4–6
4.4.1 Using the lmshare Command 4–6
4.4.2 Using the net share Command 4–8
4.4.3 Using the Server Manager 4–9
4.5 Disk Share Permissions 4–10
4.5.1 Windows NT Permissions 4–11
4.5.1.1 Setting Windows NT Permissions 4–12
4.5.1.1.1 Using the net perms Command 4–12
4.5.1.1.2 Using the Server Manager Utility 4–12
4.5.2 Windows NTFS Permissions 4–13
4.5.2.1 Controlling ASU and ACLs 4–16
4.5.2.2 Restoring ASU ACLs 4–17
4.5.2.3 Setting Windows NTFS Permissions 4–17
4.5.2.3.1 Using the net perms Command 4–17
4.5.2.3.2 Using the Windows Explorer GUI 4–18
4.5.3 Setting Tru64 UNIX Permissions 4–18
4.5.3.1 Tru64 UNIX Groups or DOS Groups 4–21
4.5.3.2 Configuring the ASU Server to Not Check Tru64 UNIX Permissions 4–21
4.6 Creating Personal Disk Shares for Users 4–22
4.7 Creating a Disk Share for a Remote File System 4–23
4.7.1 Running the NFS Service with the Lock Option 4–23
4.7.2 Enabling the UseNfsLocks Entry 4–24
4.7.3 Exporting File Systems 4–24
4.7.4 Mounting Remote Directories 4–24
4.7.5 Enabling LanManager Only Security for NFS Shares 4–26
4.8 Deleting a Disk Share 4–26

4.8.1 Using the net share Command 4–27
4.8.2 Using the Server Manager 4–27

5 Creating ASU Printer Shares

5.1 Before Creating a Printer Share 5–1
5.2 Printer Share Attributes 5–1
5.3 Configuring Print Jobs 5–2
5.4 Creating Printer Shares 5–3
5.4.1 Using the net share Command 5–3
5.4.2 Using the Windows Printer Wizard 5–4
5.5 Deleting Printer Shares 5–4
5.6 Installing Alternate Printer Drivers 5–4
5.7 Setting Printer Share Permissions 5–5
5.7.1 Using the net perms Command 5–5
5.7.2 Using the Windows Printer Properties GUI 5–5
5.8 Viewing the Status of ASU Print Jobs 5–6
5.9 Configuring Client Printers as ASU Printer Shares 5–6
5.9.1 Configuring the ASU Server 5–6
5.9.2 Configuring the PC 5–7
5.9.2.1 Loading Spooler Agent Software 5–7
5.9.2.1.1 Attaching a Text Printer 5–7
5.9.2.1.2 Attaching a PostScript Printer 5–8
5.9.2.2 Configuring a Persistent Connection 5–8

6 Configuring ASU in a TruCluster Environment

6.1 ASU Server Modes in a TruCluster Server Version 5.x Environment 6–1
6.1.1 Configuring the ASU Server in Multi Mode 6–2
6.1.1.1 Configuring Additional ASU Servers in Multi Mode .. 6–9
6.1.1.2 Multi lanman.ini File 6–10
6.1.1.3 Multi transports.ini File 6–10
6.1.1.4 Managing ASU Servers Configured in Multi Mode 6–11
6.1.2 Configuring the ASU Server in Single Mode 6–12
6.1.2.1 Configuring Additional ASU Servers in Single Mode .. 6–20
6.1.2.2 Single lanman.ini File 6–20
6.1.2.3 Single transports.ini File 6–20
6.1.2.4 Managing ASU Servers Configured in Single Mode ... 6–21
6.1.3 Configuring the ASU Server in None Mode 6–22
6.1.3.1 None lanman.ini File 6–27
6.1.3.2 None transports.ini File 6–28
6.1.3.3 Managing ASU Servers Configured in None Mode 6–29

6.2 ASU Licensing in a TruCluster Environment 6–29

7 Tuning ASU

7.1 Specifying the Number of Clients 7–1
7.2 Specifying the Number of Transport Sessions 7–1
7.3 Specifying the Number of Server Processes 7–2
7.4 Specifying the Number of NetBIOS Names 7–3
7.5 Support for HSM 7–4
7.6 Specifying the Number of Open Files and Record Locks 7–4

8 Troubleshooting the ASU Software

8.1 Preventing Problems 8–1
8.1.1 Reviewing Statistics 8–1
8.1.2 Gathering Transaction Statistics 8–2
8.1.3 Using Scripts 8–3
8.1.4 Generating Alert Messages 8–3
8.1.5 System, Security, and Application Log Files 8–3
8.1.5.1 Windows Event Viewer 8–4
8.1.5.2 The elfread Command 8–4
8.1.6 Printer Log Files 8–4
8.1.7 Logging ASU Network Errors 8–5
8.1.7.1 Computer Name Conflicts 8–5
8.1.7.2 Connection Problems Between a WINS Server and an ASU Server 8–5
8.1.7.3 NetBIOS over TCP/IP Runs Out of Names 8–5
8.1.7.4 NetBEUI Runs Out of Datalinks 8–5
8.1.7.5 NetBEUI Runs Out of Names 8–6
8.1.8 Capturing All Network Packets 8–6
8.1.9 Generating StackTrace and Core Files for ASU Processes 8–7
8.1.10 Generating StackTrace and Core Files for ASU Transport Link Processes 8–8
8.2 Solving Common ASU Server Problems 8–8
8.2.1 The ASU Software Might Be Corrupt 8–8
8.2.2 The ASU Server Will Not Start 8–8
8.2.3 Difficulty Accessing the ASU Server 8–9
8.2.3.1 Verify Network Links 8–9
8.2.3.2 Verify that the Required ASU Processes Are Running 8–9
8.2.3.3 Verify that the Required ASU Services Are Started ... 8–10
8.2.3.4 Verify that ASU Can Communicate Using TCP/IP 8–11
8.2.3.5 Verify that ASU Can Communicate Using NetBIOS .. 8–11

8.2.3.6 Verify Tru64 UNIX System Functionality 8–12
8.2.3.7 Verify that ASU Special Disk Shares Are Shared 8–12
8.2.3.8 Determine If the ASU Registry Is Corrupt 8–13
8.2.3.9 Verify the Parameters in the lanman.ini File 8–14
8.2.3.10 Determine If the User Account Database is Corrupt .. 8–14
8.2.3.11 Determine If the ACL Database Is Corrupt 8–15
8.3 Solving Common Share Problems 8–15
8.3.1 User Cannot Connect to a Share 8–15
8.3.1.1 Verify That the Share Exists 8–15
8.3.1.2 Determine the Maximum Number of Clients 8–15
8.3.2 User Cannot Access a File 8–16
8.3.2.1 Viewing and Changing Windows NT Share Permissions 8–16
8.3.2.2 Viewing and Changing Windows NTFS Permissions .. 8–16
8.3.2.3 Checking Tru64 UNIX Permissions 8–17
8.3.2.4 Check for Open Locks 8–17
8.3.2.5 Check for Insufficient UStructs 8–18
8.4 Solving Common Browsing Problems 8–18
8.4.1 Browser Does Not Display ASU Shares 8–18
8.4.2 LAN Manager Servers Do Not Show the ASU Server 8–18
8.4.3 BDCs Browse Lists Do Not Show All Controllers 8–19
8.5 Solving Common Printing Problems 8–19
8.5.1 Client Printers and Jobs Do Not Display 8–19
8.5.2 Printer Name Is Invalid 8–19
8.5.3 No Separator Page 8–19
8.5.4 Print Jobs Do Not Print 8–20
8.5.5 Characters Print Incorrectly 8–20
8.5.6 Trouble Printing to a Shared Client Printer 8–20
8.5.7 Keyboard Locks When Printing 8–20

A Sample ASU Installation and Configuration

B ASU Registry Entries

B.1 AdvancedServer B–1
B.1.1 AlertParameters B–1
B.1.2 FileServiceParameters B–2
B.1.3 NetAdminParameters B–9
B.1.4 Parameters B–9
B.1.5 ProcessParameters B–12
B.1.6 RpcParameters B–16
B.1.7 ShareParameters B–17

B.1.8 UnixAuditParameters B–17
B.1.9 UserServiceParameters B–18
B.2 Alerter B–23
B.3 Browser B–23
B.4 EventLog B–24
B.5 LanmanServer B–25
B.6 Netlogon B–27
B.7 Replicator B–29
B.8 UPS B–31

C The lanman.ini File

C.1 File Syntax C–1
C.2 File Parameters C–2
C.2.1 server Parameters C–2
C.2.2 workstation Parameters C–3
C.2.3 lmxserver Parameters C–4
C.3 Mappings of lanman.ini Parameters to Registry Entries C–9
C.3.1 server Parameters C–9
C.3.2 workstation Parameters C–10
C.3.3 uidrules Parameters C–10
C.3.4 netlogon Parameters C–11
C.3.5 lmxserver Parameters C–11
C.3.6 ups Parameters C–17
C.3.7 replicator Parameters C–18
C.3.8 fsi Parameters C–18
C.3.9 psi Parameters C–19
C.3.10 version Parameters C–19
C.3.11 netrun Parameters C–19
C.3.12 browser Parameters C–20

D The net Commands

D.1 Online Help for net Commands D–3
D.2 Using Special Characters D–4
D.3 Using Passwords D–5
D.4 Using Command Confirmation D–6
D.5 Specifying a Path Name D–6
D.6 Abbreviating net Commands Options D–7
D.7 Administering a Remote ASU Server D–7
D.8 Examples of Using net Command D–8

E ASU Commands

F Configuring ASU in a Version 1.x Cluster

F.1 ASU and TruCluster Software Prerequisites F–1
F.2 Creating a TruCluster Disk Service F–2
F.3 Configuring the ASU Software F–4
F.4 ASU Licensing in a TruCluster Cluster F–5
F.5 Managing ASU Resources in a TruCluster Cluster F–5
F.5.1 Creating Disk Shares F–5
F.5.2 Maintaining User Accounts F–5
F.5.3 Maintaining Print Services F–6
F.6 Removing ASU from a TruCluster Cluster F–6
F.6.1 Removing One ASU Server from the Cluster F–6
F.6.1.1 Relocating the ASU Service F–6
F.6.1.2 Restricting a System from Running the ASU Service . F–7
F.6.1.3 Deinstall the ASU Server F–7
F.6.2 Removing ASU from All Systems in a TruCluster Version 1.x Cluster F–8
F.6.2.1 Relocating the ASU Service F–8
F.6.2.2 Restrict the ASU Server to Run on a Single System .. F–9
F.6.2.3 Removing the ASU Server from the Alternate System F–9
F.6.2.4 Removing the ASU Server from the Active System F–9
F.6.2.5 Removing the ASU Disk Service F–10

Index

Examples

6–1 Sample Multi Mode asusetup Output 6–3
6–2 Sample Multi Mode lanman.ini File 6–10
6–3 Sample Multi Mode transports.ini File 6–11
6–4 Sample Single Mode asusetup Output 6–13
6–5 Sample Single Mode lanman.ini File 6–20
6–6 Sample Single Mode transports.ini File 6–21
6–7 Sample None Mode asusetup Output 6–22
6–8 Sample None Mode lanman.ini File 6–28
6–9 Sample None Mode transports.ini File 6–28

Figures

2–1 Registry Path 2–2

2–2 HKEY_LOCAL_MACHINE Keys and SubKeys 2–3
2–3 HKEY_USERS Keys and SubKeys 2–4

Tables

1–1 ASU Mandatory Subsets 1–6
1–2 ASU Optional Subsets 1–6
1–3 ASU Server-Based Commands 1–13
2–1 Registry Data Types and Values 2–5
3–1 Mandatory Domain User Account Attributes 3–2
3–2 Mandatory Domain User Account Attributes 3–2
3–3 Optional Domain User Account Attributes 3–3
3–4 User Account Value Entries 3–5
3–5 User Directory Value Entries 3–6
3–6 User Account NIS Value Entries 3–8
3–7 Setting User Account Attributes 3–13
4–1 NFS-Related Disk Share Value Entries 4–4
4–2 ASU Special Disk Shares 4–4
4–3 Mandatory Disk Share Attributes 4–5
4–4 Optional Disk Share Attributes 4–6
4–5 Setting Disk Share Attributes 4–8
4–6 NTFS Standard Permissions 4–14
4–7 NTFS Custom Permissions 4–14
4–8 ACL Value Entries 4–16
4–9 ASU ACL Commands 4–17
4–10 Disk Share Permission Value Entries 4–20
5–1 Mandatory Print Share Attributes 5–2
5–2 Optional Print Share Attributes 5–2
5–3 Print Job Value Entries 5–2
5–4 Setting Printer Share Attributes 5–3
6–1 The net Commands that Work Differently in a Cluster 6–12
8–1 ASU Statistics 8–1
D–1 Description of the net Commands D–1
D–2 The net Command Syntax Conventions D–4

About This Guide

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

Audience

This guide is intended for anyone who is responsible for installing, configuring, and administering the ASU software.

New Features

The following list describes new features for this release:

- How the ASU server synchronizes disk shares with NFS export entries has changed. See *Section 4.1.1.2* for more information.
- On a per share basis, you can use the `lmshare` command to set default Tru64 UNIX file and directory permissions for newly created files and directories in a share or configure whether or not the ASU server ignores Tru64 UNIX permissions checking for a share. See *Section 4.4.1* for more information.
- You can restore ASU ACLs from a backup copy of an ACL store. See *Section 4.5.2.2* for more information.
- The following new registry entries have been added:

Entry	**Description**
`CreatePersonalShare`	Specifies whether or not the ASU server will automatically create a personal disk share when you create a Tru64 UNIX user account or map a domain user account to a Tru64 UNIX user account, delete a personal disk share when you delete its associated domain user account, and rename a personal disk share when you rename its associated domain user account. See *Section 4.6* and *Section B.1.9* for more information.
`CreateUnixHomeDirectory`	Specifies whether or not the ASU server creates a user's Tru64 UNIX home directory when it creates a Tru64 UNIX user account. See *Section B.1.9* for more information.

Entry	Description
`HideClusterMember`	Specifies whether or not TruCluster members will be displayed in the Network Neighborhood and other browse functions. See *Section B.1.4* for more information.
`MaxPrintJobs`	Specifies the maximum number of print jobs allowed in any class queue created by the ASU server. See *Section 5.3* and *Section B.1.4* for more information.
`MaxPrintJobName`	Specifies the maximum number of characters for a print job name. See *Section 5.3* and *Section B.1.4* for more information.
`PreserveNumericUserName`	Specifies whether or not a Tru64 UNIX user account name is created with a pre-pended letter `a` when creating a domain user account whose first character is numeric. See *Section B.1.9* for more information.
`UseClusterLicensing`	Specifies whether or not the ASU server uses cluster-wide licensing when configured in a TruCluster Server multi-instance cluster. See *Section 6.2* and *Section B.1.4* for more information.

Organization

The guide is organized as follows:

Chapter 1	Describes how to install the ASU software.
Chapter 2	Describes how to configure the ASU software.
Chapter 3	Describes ASU-related user accounts and how to create them.
Chapter 4	Describes how to use the ASU software to share UNIX file systems.
Chapter 5	Describes how to use the ASU software to share UNIX based printers.
Chapter 6	Describes how to configure the ASU software in a TruCluster Version 5.x or higher cluster.
Chapter 7	Describes how to tune the ASU software.
Chapter 8	Describes how to troubleshoot the ASU software.
Appendix A	Shows a sample ASU installation and configuration procedure.

Appendix B	Describes the ASU registry entries.
Appendix C	Describes the `lanman.ini` file.
Appendix D	Describes the net commands.
Appendix E	Describes the ASU commands.
Appendix F	Describes how to configure the ASU software in a TruCluster Version 1.x cluster.

Related Documentation

The following documents provide more information about the ASU software:

- *Concepts and Planning Guide* - Describes the concepts related to planning and administering the ASU software and environment.
- *Release Notes* - Describes the latest information about the ASU software that might not be documented elsewhere.

Reader's Comments

HP welcomes any comments and suggestions you have on this and other Tru64 UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-884-0120 Attn: UBPG Publications, ZKO3-3/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`

Please include the following information along with your comments:

- The full title of the manual and the order number. (The order number appears on the title page of printed and PDF versions of a manual.)
- The section numbers and page numbers of the information on which you are commenting.
- The version of Tru64 UNIX that you are using.
- If known, the type of processor that is running the Tru64 UNIX software.

The Tru64 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 HP technical support office. Information provided with the software media explains how to send problem reports to HP.

Conventions

The following 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 superuser prompt.
`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).

1

Installing the ASU Software

The Advanced Server for UNIX (ASU) software is a Tru64 UNIX layered application that integrates Tru64 UNIX and Windows environments. The ASU software implements Windows NT Server Version 4.0 services, security, and functionality on a system running the Tru64 UNIX operating system software. The Tru64 UNIX system on which the ASU software is running appears as a Windows NT Server to other Windows systems and to users of Windows systems, and can participate in a Windows NT and Windows 2000 domain.

You can use native Windows commands and utilities to manage the ASU software and to make UNIX based file systems and printers available to Windows users as shares. Windows users connect to shares without modification to their software. Once connected, the Tru64 UNIX directory or printer associated with a share appears as a transparent extension to a Windows user's local computing environment.

This chapter describes how to install or upgrade the ASU software and describes the ASU environment.

1.1 Preinstallation Tasks

Before installing the ASU software, you must:

- Review the ASU documentation
- Ensure that the Tru64 UNIX system on which you will install the ASU software meets the ASU software requirements
- Decide how to authenticate user account information
- Decide which interface you will to use to administer the ASU software

1.1.1 Reviewing the ASU Documentation

You can find the ASU documentation on the Tru64 UNIX Associated Products Volume 2 CD-ROM in Hypertext Markup Language (HTML) format and Portable Document Format (PDF). To access ASU documentation on the CD-ROM, open the ASU documentation library file, `/Advanced_Server/doc/html/LIBRARY.HTM`, in a Web browser.

In addition to this document, the ASU documentation includes:

- The *Release Notes* that contains the latest ASU information that may not be documented elsewhere.
- The *Concepts and Planning Guide* guide that contains information to help you plan, implement, and administer the ASU software.

1.1.2 ASU Software and Hardware Requirements

The system on which you will install the ASU software must be running the Tru64 UNIX operating system Version 5.1A or higher.

If you plan to configure the ASU software for international support, ensure that the system is running with Unicode support installed. See Section 1.10 for more information on configuring the ASU software for international support.

See the *Installation Guide* if you need to upgrade your version of the Tru64 UNIX operating system software.

There should be at least 7 MB of free disk space in the file system containing the `/usr/net` directory.

1.1.3 Determining a Method for User Account Authentication

By default, the ASU server and Tru64 UNIX operating system software must authenticate a user’s name and password before a user can access an ASU share. Therefore, a Windows user must have a domain user account that the ASU server uses for user authentication and a Tru64 UNIX user account that the Tru64 UNIX operating system uses for user authentication.

By default, when you create a domain user account, the ASU server automatically creates a Tru64 UNIX user account in the local `/etc/passwd` file if an account with the same name does not exit. The Tru64 UNIX operating system software uses the local user account information for authentication. However, you can configure the Tru64 UNIX operating system software to direct authentication requests to a Windows 2000 Server or to a Windows NT Server Version 4.0. The Windows 2000 Server or Windows NT Server Version 4.0 uses its user account information to authenticate users on behalf of the Tru64 UNIX system. This is useful if you have user account information stored on a Windows 2000 Server or on a Windows NT Server Version 4.0 and you do not want to create a user account database on the Tru64 UNIX system.

1.1.3.1 Windows 2000 Server Authentication

To configure the Tru64 UNIX operating system software to use a Windows 2000 Server to authenticate users, you must install the Windows 2000 Single Sign On (SSO) Version 2.0 or higher software on the Windows 2000 Server and on the Tru64 UNIX system on which the ASU server is running. On the Tru64 UNIX system on which the ASU server is running, you must enable the `UseActiveDirectory` registry entry before you start the ASU server.

See *Security Administration* for more information about the SSO software.

See Chapter 2 for more information about registry entries and Section B.1.9 for more information about the `UseActiveDirectory` registry entry.

1.1.3.2 Windows NT Server Version 4.0 Authentication

To configure the Tru64 UNIX operating system software to use a Windows NT Version 4.0 Server to authenticate users, you must install and configure the ASU SIA software on the system running the Tru64 UNIX operating system software. The ASU SIA software is provided in a subset with the ASU software and requires that the ASU server and transports also be installed. This option is available only on systems running the Tru64 UNIX Version 5.0 or higher operating system software and not using enhanced security.

See Table 1–2 for information about the ASU SIA software. See Section 3.6 for information about using Windows NT Server Version 4.0 authentication.

1.1.4 Overview of ASU Administrative Interfaces

To administer the ASU software you can use:

- ASU commands
- `net` commands
- Tru64 UNIX commands and graphical user interfaces (GUIs)
- Windows GUIs

Note

If you plan to configure the ASU Server in a Windows 2000 domain, then you must administer the ASU server by using Windows 2000 interfaces, except for file replication which must be administered form a Windows NT system.

The ASU commands, `net` commands, and ASU options for Tru64 UNIX commands and GUIs are only available on Tru64 UNIX systems on which the ASU server is installed.

1.1.4.1 The ASU Commands

The ASU commands are Tru64 UNIX style commands that you can use to display information about, administer, and troubleshoot the ASU server and domain. You enter ASU commands in lowercase at the Tru64 UNIX command prompt on a system running the ASU software. See Appendix E for more information on ASU commands.

1.1.4.2 The net Commands

The `net` commands are Windows style commands that you can use to create shares, domain user accounts, and groups and to display information about and administer the ASU server, domain, shares, domain user accounts, and groups.

A `net` command begins with the word `net` followed by a keyword and options. You enter `net` commands in lowercase at the Tru64 UNIX command prompt on a system running the ASU software in the following form:

```
# net keyword [/option]
```

See Appendix D for more information on `net` commands.

1.1.4.3 The Tru64 UNIX Commands and GUIs

The Tru64 UNIX user and file system commands and GUIs provide additional ASU-related options that you can use to create and administer shares and domain user accounts. See *System Administration* for information on administering the ASU server using Tru64 UNIX commands and GUIs.

1.1.4.4 The Windows GUIs

You can use the following Windows based GUIs to administer the ASU server and domain:

- The Server Manager creates, displays information about, and administers shares.
- The User Manager for Domains creates, displays information about, and administers domain user accounts and groups.
- The Policy Editor displays information about and administers the ASU registry.
- The Event Viewer displays ASU-related application, security, and system events.

You can administer the ASU server by using the version of these Windows GUIs that are provided with a Windows NT Server Version 4.0 or a Windows 2000 Server. For a system running another type of Windows operating system software, you must install the version of these Windows GUIs that are provided in the `ASUADM`*`nnn`* subset as described in Section 1.3, then install the GUIs as described in Section 1.8.

1.2 Upgrading the ASU Software

You use the Tru64 UNIX `setld` command to deinstall the ASU subsets, then reinstall new ASU subsets.

Note

Upgrading an earlier version of the ASU software to ASU Version 5.1 or higher converts the SAM database, the ACL database, and ASU share file to a new format that is not compatible with previous versions of the ASU software. If you deinstall the ASU Version 5.1 or higher software and reinstall an earlier version of the ASU software, you must recreate the shares or restore a back up copy of the SAM database, the ACL database, and ASU share file and reapply any changes that you made since the back up. The ASU files to restore are:

```
/usr/net/servers/lanman/domains/*
/usr/net/servers/lanman/datafiles/*
/usr/net/servers/lanman/sharefile
```

Follow these steps to upgrade the ASU software:

1. As root, display the installed ASU subsets, for example:

   ```
   # /usr/sbin/setld -i |grep ASU |grep -v not |grep
   installed
   ```

2. Enter the `/usr/sbin/setld -d` command followed by the name of each subset to deinstall, for example:

   ```
   # /usr/sbin/setld -d ASUBASE501 ASUTRAN501 ASUMANPAGE501
   ```

   While ASU subsets are deinstalled, you are prompted to save ASU configuration files and the user account and share databases. Save these files and databases if you want to reuse the previous ASU configuration.

   If you do not save these files and databases on a PDC:

   - ASU shares created on that system are removed.
   - Domain user accounts that were created by the ASU software are removed.

   If you do not save these files and databases on a BDC:

   - ASU shares created on that system are removed.
   - The copy of the domain user account database is removed.

   Although ASU shares are removed from a system, their associated Tru64 UNIX directories are uneffected.

3. Use the `setld` command to install the new ASU subsets. See Section 1.3 for more information.

1.3 Installing the ASU Software

To install the ASU software you use the Tru64 UNIX `setld` command to install the ASU subsets.

ASU subsets are categorized as either mandatory or optional. The ASU server will not operate properly if you do not install the mandatory subsets. The optional subsets provide information and tools that you use to manage the ASU server.

Table 1–1 describes the ASU mandatory subsets. Table 1–2 describes the ASU optional subsets. The *nnn* variable in the subset name represents the ASU version number. See the ASU *Release Notes* for the current version number.

Table 1–1: ASU Mandatory Subsets

Subset Name	Provides
`ASUBASE`*nnn*	ASU server functions.
`ASUTRAN`*nnn*	The NetBEUI and NetBIOS over TCP/IP transports that the ASU server uses for network communications.

Table 1–2: ASU Optional Subsets

Subset Name	Provides
`ASUADM`*nnn*	English language version of the Nexus tools, which are interfaces based on Microsoft Windows that you use to administer the ASU server.
`ASUADMJP`*nnn*	Japanese language version of the Nexus tools, which are interfaces based on Microsoft Windows that you use to administer the ASU server.
`ASUMANPAGE`*nnn*	English language version of the reference pages that describe ASU commands.

Table 1–2: ASU Optional Subsets (cont.)

Subset Name	Provides
ASUMANJP*nnn*	Japanese language version of the reference pages that describe ASU commands.
ASUSIA*nnn*	A Tru64 UNIX security mechanism that enables Tru64 UNIX to use a Windows NT Server Version 4.0 for authentication. This subset is available only on systems running the Tru64 UNIX Version 5.0 or higher operating system software and not using enhanced security.

Follow these steps to install the ASU subsets:

1. As the root user, insert and mount, in read-only mode, the Tru64 UNIX Associated Products Volume 2 CD-ROM. For example, on a system running Tru64 UNIX Version 5.0 or higher, enter:

   ```
   # mount -r /dev/disk/device_name /mnt
   ```

   On a system running Tru64 UNIX Version 4.*X*, enter:

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

   Where *device_name* is the name of the CD-ROM drive.

2. Enter the following `setld` command and follow the instructions on the screen, for example:

   ```
   # setld -l /mnt/Advanced_Server/kit .
   ```

   Informational messages display while the ASU subsets are installed.

3. When the installation is complete, unmount the Tru64 UNIX Associated Products Volume 2 CD-ROM.

See Appendix A for a sample ASU subset installation procedure.

1.4 Postinstallation Tasks

After you install the ASU subsets, you must run the `asusetup` utility. The `asusetup` utility:

- Prompts you for information that is required to start the ASU server.

  Default values are provided from a previous ASU installation if you saved the configuration files or otherwise from the Tru64 UNIX system information.

Note

Default values are used if you reboot the Tru64 UNIX system after using the `setld` utility to install the ASU subsets and before running the `asusetup` utility.

- Runs the ASU Installation Verification Procedure (IVP) to verify that the ASU subsets were correctly installed.
- Starts the ASU server.

You run the `asusetup` utility by entering:

```
# /usr/sbin/asusetup
```

If you exit the `asusetup` utility by pressing `Ctrl/C`, the ASU configuration is incomplete and you must rerun the `asusetup` utility.

The following sections describe the `asusetup` procedure in detail.

See Appendix A for sample output generated by the `asusetup` utility.

See Chapter 6 if you are configuring the ASU software in a TruCluster cluster.

1.4.1 Configuring ASU Network Information

The `asusetup` utility displays information similar to the following that shows the default network controllers that the ASU server will use and the methods that the ASU server uses to resolve a NetBIOS name to a TCP/IP address in a wide area network (WAN):

```
Controllers: TCP/IP  = tu0
             NetBEUI = tu0

Use DNS:      yes
Sub Domains:  asu.company.com
Use lmhosts:  yes
lmhosts file: /usr/net/servers/lanman/datafiles/lmhosts
Use NBNS:     no
Primary NBNS address:
Secondary NBNS address:

Would you like to use this network information?[y/n]?
```

To use the default values, enter `y`. If you enter `n`, you must provide a value for each item as follows:

- Controllers

The ASU server provides and can use either or both of the following networking transport software on any Ethernet, FDDI, and Token Ring controllers supported by the Tru64 UNIX operating system software:

  - NetBEUI transport, which is used exclusively for local area networking
  - NetBIOS over TCP/IP, which is used over the system's installed TCP/IP transport software for local and wide area networking

- The remaining items define the method of NetBIOS name resolution that the ASU server uses to communicate with systems in different TCP/IP subnets in a WAN. You can use any or all of the following methods:
  - A domain name server (DNS). The value for the `Sub Domains` item are the DNS subdomains that the ASU server will use to try to resolve the NetBIOS name as a TCP/IP node name. See *Network Administration* for more information on DNS.
  - An `lmhosts` file.

    If you choose to use an `lmhosts` file, the `asusetup` utility creates it by default in the `/usr/net/servers/lanman/datafiles` directory. You must edit the `lmhosts` file to add:

    ☐ An entry that includes the TCP/IP name and address of each system that is located on a different TCP/IP subnet with which the ASU server must communicate.

    ☐ A special entry for the primary domain controller (PDC).

    The following is a sample `lmhosts` file where the PDC is named Summer in a domain called summer.dom and BDCs are named Fall, Winter, and Spring:

```
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"  # PDC entry
```

    Note that the domain name entry must be padded with extra spaces to fill 15 characters, which is the maximum length for a domain name. In the previous example, `summer.dom` is 10 characters, followed by 5 spaces, followed by `\0x1b`, all within double quotes. Also note that each node does not require an entry for itself.

  - A NetBIOS Name Service (NBNS), which is also called Windows Internet Name Service (WINS). You can configure a primary and secondary NBNS. The ASU server uses the primary NBNS for name resolution. If primary NBNS is not available, the ASU server uses the secondary NBNS.

The value for the NBNS address item must be the TCP/IP address of the server running the NBNS.

See your Windows documentation for more information on NBNS.

1.4.2 Configuring ASU Server Information

The `asusetup` utility displays output similar to the following that shows the default values for ASU server information:

```
Server Name:

Domain Name:

Domain Role: Primary

Name of Domain’s Primary:

Enter Password for Administrator:

Would you like to use this general server information [y/n]?
```

To use the default values, enter `y`. If you enter `n`, you must provide a value for each item as follows:

- Server Name

  The name of the ASU server. This is the name that users and other ASU servers and Windows servers use to communicate with this ASU server. If you enter a server name, the name can contain up to 15 alphanumeric English language characters and the following symbols: ~ ! # $ % ^ _ ( ) . -

- Domain Name

  The name of the domain that the ASU server will create or join. The default is the server name followed by a `.dom` extension, for example *`servername`*`.dom`. If you enter a domain name, it must be different from the ASU server or system name and can contain up to 15 alphanumeric English language characters and the following symbols: ~ ! # $ % ^ _ ( ) . -

- Domain Role

  The role of the ASU server in the domain. The ASU server can be a:

  – Primary domain controller (PDC). There is only one PDC per domain. A PDC stores and maintains the user account database. A PDC authenticates domain user logon requests. The default is a PDC.

    You cannot configure the ASU server as a PDC in a Windows 2000 domain.

  - Backup domain controller (BDC). The PDC must running before you configure a BDC. There can be many BDCs in a domain. A BDC receives a copy of the user account database to authenticate domain user logon requests.

    You can configure the ASU server as a BDC in a Windows 2000 Server domain only if the Windows 2000 Server is configured for mixed mode.

  - Member server. There can be many member servers in a domain. A member server participates in a domain; however, it does not receive a copy of the user account database and therefore does not authenticate domain user logon requests.

    You can configure the ASU server as a member server in a Windows 2000 Server domain whether the Windows 2000 Server is configured for mixed or native mode.

- Name of Domain's Primary

  The name of the domain's PDC if the ASU server is not the PDC.

- Password for Administrator

  For a PDC, you must supply an administrative password. For a BDC, you must supply the name and password of an Administrator account on the PDC. Passwords can be up to 14 alphanumeric English language characters and are case sensitive.

1.4.3 Configuring Listen Names

The `asusetup` utility displays output similar to the following that shows the default listen names for the ASU server:

```
The ASU server currently listens for, and responds to,
messages sent to these network names:
 listenname      : server1
 ExtraListenNames:
                   (none)

You can define Extra Listen Names for the server to listen for
via the Registry parameter ExtraListenNames.

Do you want to modify the ExtraListenNames entry [y/n]?
```

A listen name is a unique name assigned to the ASU server to which it responds on the network. Users can use any of the assigned listen names when connecting to the ASU server. For example, if an ASU server is assigned a listen name of `server1` and the extra listen names of `server2` or `server3`, users can specify `\\server1`, `\\server2`, or `\\server3` when connecting to its shares.

To use the default values, enter `n`. If you enter `y`, you are prompted to enter another listen name for the ASU server or to delete a listen name assigned to the ASU server.

You can also configure extra listen names by directly modifying the `ExtraListenNames` registry entry. See Section B.1.4 for more information.

1.4.4 Starting the ASU Server

The `asusetup` utility prompts you to start the ASU server.

Do not start the ASU server if you plan to configure the ASU server to:

- Communicate in a language other then English. See Section 1.10 for more information.
- Change the default behavior that automatically creates Tru64 UNIX user accounts. See Chapter 3 for more information.
- Create Tru64 UNIX user accounts using NIS. See Chapter 3 for more information.
- Create Tru64 UNIX user account home directories under a single-letter subdirectory of `/usr/users`. See Chapter 3 for more information.
- Change the default behavior that automatically creates shares for NFS exported file systems. See Chapter 4 for more information.
- Change the default behavior to automatically create personal shares. See Chapter 4 for more information.

To start the ASU server, enter `yes` at the prompt. If you enter `no`, the `asusetup` utility exits.

To start the ASU server at a later time, enter:

```
# net start server
```

1.4.5 Verifying the ASU Software Installation

If you start the ASU server, the `asusetup` utility prompts you to run the ASU installation verification procedure (IVP) to test that the ASU software was correctly installed.

Status messages display on the screen while the IVP runs.

If the ASU IVP reports a failure, reinstall the ASU software as described in Section 1.2.

If the ASU IVP continues to report a failure, see Chapter 8 or contact your support representative.

You can run the ASU IVP at any time by entering:

```
# asuivp
```

See `asuivp`(8) for more information on the `asuivp` command.

1.4.6 Reconfiguring the ASU Software

To reconfigure ASU network and general values, reenter the `asusetup` command or use the ASU commands in Table 1–3.

Caution

> If you reconfigure a PDC as a member server, the domain user account database is removed. If you reconfigure a member server as a BDC or PDC, the local user account database is removed.

Table 1–3: ASU Server-Based Commands

ASU Setting	ASU Command
Server name	# **`/usr/sbin/setservername`** Do not directly edit the `ComputerName` entry in the ASU registry or the `listenname` parameter in the `lanman.ini` file. The `setservername` command will correctly update the SAM database, the ASU registry, and the `lanman.ini` file.
Domain	# **`/usr/sbin/joindomain`**
Domain name	# **`/usr/sbin/setdomainname`**
Administrative password	# **`net password`**
ASU server role	# **`/usr/sbin/promote`**
Transport controllers	# **`/usr/sbin/ctlrsetup`** You must restart the transports to effect any changes.

See Appendix E or the associated command reference page for more information on these commands.

1.5 ASU Directories

The ASU installation creates the `/usr/net/servers/lanman` directory. Beneath this directory are subdirectories that contain ASU-related files and subdirectories.

1.6 ASU Services

The following services automatically start when the ASU server starts:

- The `Alerter` service notifies selected clients about administrator-defined ASU alerts that occur on a particular system. The `Alerter` service requires that the `Messenger` service be started on the selected client.
- The `Browser` service maintains an up-to-date list of computers on the network and provides the list to applications upon request.
- The `Eventlog` service records system, security, and application events in ASU event logs.
- The `Netlogon` service performs authentication of user account logons.
- The `Replicator` service replicates files (such as profiles and login scripts).
- The `Server` service provides remote procedure call (RPC) support, and file, print, and named pipe sharing.

To see which ASU services are running, enter:

```
# net start
```

Information similar to the following is displayed showing which ASU services are running:

```
These Advanced Server for UNIX Systems services are
started:
BROWSER       EVENTLOG       NETLOGON
ALERTER        SERVER
The command completed successfully.
```

1.7 ASU Processes

The following list describes ASU processes:

- The `lmx.ctrl` process is the master control process and must be running. The `lmx.ctrl` process:
  - Accepts requests from new clients and passes them to the `lmx.srv` process.
  - Creates new `lmx.srv` processes as necessary.
  - Reminds the `lmx.srv` process to check for autodisconnect timeouts.
  - Polls for events on the network or from other processes.
  - Tracks the time of day.
  - Receives instructions from the operating system.
  - Handles administrative actions that are not associated with a single client.
  - Listens for and routes nonguaranteed datagram broadcasts.

  - Announces the presence of the ASU server to the domain and retains announcements from other servers.
  - Schedules printer start and stop activity.
  - Coordinates transactions between client and server applications.

- At least one `lmx.srv` process must be running. Each `lmx.srv` process services the needs of a set of clients. The `lmx.srv` process polls for incoming server message block (SMB) requests from clients and the `lmx.ctrl` process.

  The ASU server starts additional `lmx.srv` processes based on the number of supported clients, or based on the maximum number of specified server processes. As more client sessions are established, more `lmx.srv` processes might start.
- The `lmx.dmn` process must be running. The `lmx.dmn` process handles client logon requests and account replication.
- The `lmx.repl` process provides import file replication services. This process runs only if the `Replicator` service is started.
- The `lmx.alerter` process starts if the `Alerter` service starts.
- The `lmx.browser` process handles browse requests if the `Browser` service starts.

ASU-related processes start when the ASU server starts. To see which ASU processes are running, enter:

```
# ps -ef | grep lmx
```

Information similar to the following is displayed showing which ASU processes 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
```

1.8 Installing the Windows Based Interfaces

A Windows NT Server Version 4.0 and a Windows 2000 Server provides the administrative interfaces that you can use to administer the ASU server. To administer the ASU server from a system that is running any other type of Windows operating system software, you must install the ASU supplied Windows based interfaces on that system.

1.8.1 Installing or Running Administrative Interfaces on Windows NT

Follow these steps to install or run the Windows based administrative interfaces on a system running the Windows NT operating system software:

1. On the Tru64 UNIX system, ensure that the Client-based Advanced Server Administration Tools subset is installed, for example:

   ```
   # setld -i |grep ASUADM |grep -v not |grep installed
   ```

   If `ASUADM`*nnn* is displayed, the subset is installed. Otherwise, you must install the `ASUADM`*nnn* subset. See Section 1.3 for information on installing ASU subsets.
2. Connect a network drive to the `astools` disk share.
3. Select the folder that corresponds with the version of the Windows NT operating system. For example, select the `winnt.40` folder for Windows NT 4.0.
4. You can:
   - Start the interface you want by double-clicking on the appropriate file:
     - The `srvmgr.exe` file starts the Server Manager.
     - The `usrmgr.exe` file starts the User Manager for Domains.
     - The `poledit.exe` file starts the Policy editor.
   - Install the interfaces by running the `setup.bat` program. The executable files for the interfaces are installed in the `C:\WINNT\SYSTEM32` directory. Start an interface by double-clicking on an executable as described above.

1.8.2 Installing Administrative Interfaces on a Windows 95 or Windows 98 System

Follow these steps to install the Windows based administrative interfaces on a system running the Windows 95 or Windows 98 operating system software:

1. On the Tru64 UNIX system, ensure that the Client-based Advanced Server Administration Tools subset is installed, for example:

   ```
   # setld -i |grep ASUADM |grep -v not |grep installed
   ```

   If `ASUADM`*nnn* is displayed, the subset is installed. Otherwise, you must install the `ASUADM`*nnn* subset. See Section 1.3 for information on installing ASU subsets.
2. Connect a network drive to the `astools` disk share.
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 then on the Install button in the Have Disk window.
9. Click on the OK button after the files are copied.
10. If you plan to run the Server Manager interface, edit the `autoexec.bat` file to include `srvtools` to the path and reboot the system. For example, if you boot from drive `C`, either append `srvtools` to the `PATH` statement or, if there is no `PATH` statement, enter:

    ```
    SET PATH=%PATH%;C:\srvtools
    ```

Installing the administrative interfaces:

- Copies the Windows NT Server Tools files to the `srvtools` directory on the boot drive
- 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 ASU, Windows NT Server, or Windows NT Workstation software

Note the following restrictions when administering ASU from a Windows 95 system:

- Some administrative tasks require that you log on or enter your password for verification before you can perform an action.
- 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 system running Windows 95:
  - Administering 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 ASU printer queue.

- Using 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.
- Using 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.

1.9 ASU Licenses

ASU licenses are supplied in the form of a product authorization key (PAK) called `ASDU-CONNECT`. You load the `ASDU-CONNECT` PAK into the Tru64 UNIX License Management Facility (LMF).

One `ASDU-CONNECT` license is used when the user of a Windows system browses or first connects to an ASU share. The license allows the user to browse and connect to shares for which they have permission. The Windows system retains the license until the user stops browsing and terminates all connections to shares, at which time the license can be reassigned. A Windows system uses one `ASDU-CONNECT` license from each ASU server to which the user browses or connects.

`ASDU-CONNECT` PAKs are available in license units of 10, 25, 50, 100, 250, 500, and 1,000. You purchase `ASDU-CONNECT` PAKs based on the number of users. For example, if you expect 275 domain users to access shares, then you should purchase one PAK for 25 licenses and one PAK for 250 licenses.

The ASU software provides two free built-in licenses. You do not need to load these licenses into LMF, nor will you see them in LMF.

To list the number of available `ASDU-CONNECT` licenses, enter:

```
# asustat -L
```

To list the client names that have a license, enter:

```
# asustat -c
```

To view the system event log to show if a client was issued or denied a license, enter:

```
# elfread -d system | more
```

See `asustat`(8) and `elfread`(8)for more information on these commands.

1.10 Configuring International Support

You can configure the ASU server to communicate in a language other than English. To do so, follow these steps:

1. Install and configure the ASU software as described in Section 1.3. Do not start the ASU server when prompted by the `asusetup` utility.
2. Use a text editor to set the `lang` parameter in the [`lmxserver`] section of the `lanman.ini` file. Add the `lang` parameter if it is not there.

   The `lang` parameter sets the character set and locale that the ASU server uses to communicate. For example, if the Windows systems are running the French edition of Windows, set the `lang` parameter to `fr_FR.ISO8859-1`, which is the Tru64 UNIX French locale. For example:

   ```
   [ lmxserver ]
   lang=fr_FR.ISO8859-1
   ```

   The ASU server supports the Tru64 UNIX locales listed in the `l10n_intro` reference page except for Japanese SJIS and Traditional Chinese. See `l10n_intro`(5) for more information on the supported locales.
3. Install the Unicode support for the locale.

   The Unicode support includes codeset converters that the ASU server uses to convert names between the Windows system and Tru64 UNIX character sets. The Unicode support is in the Tru64 UNIX Worldwide subsets. For information on installing codeset subsets, see the WLS installation procedure in the *Installation Guide — Advanced Topics*.
4. Start the ASU server, for example:

   ```
   # net start server
   ```

2

Configuring the ASU Software

The manner in which the ASU server interoperates with the Tru64 UNIX operating system software depends on the values assigned to value entries stored in a central database called the ASU registry.

The ASU registry largely replaces the `lanman.ini` file, which was previously used to configure the ASU software. Review the `/usr/net/servers/lanman/regfiles/reg.ini` file to see which `lanman.ini` parameters were moved to the ASU registry.

Not all parameters in the `lanman.ini` file moved to the registry, and the `lanman.ini` file is still used for some configuration parameters.

See Appendix C for information about the `lanman.ini` file.

This chapter describes how to view and change the value of value entries in the ASU registry.

2.1 ASU Registry Overview

The ASU registry is a hierarchical database of subtrees, keys, subkeys, and value entries that define how the ASU server interoperates with the Tru64 UNIX operating system software.

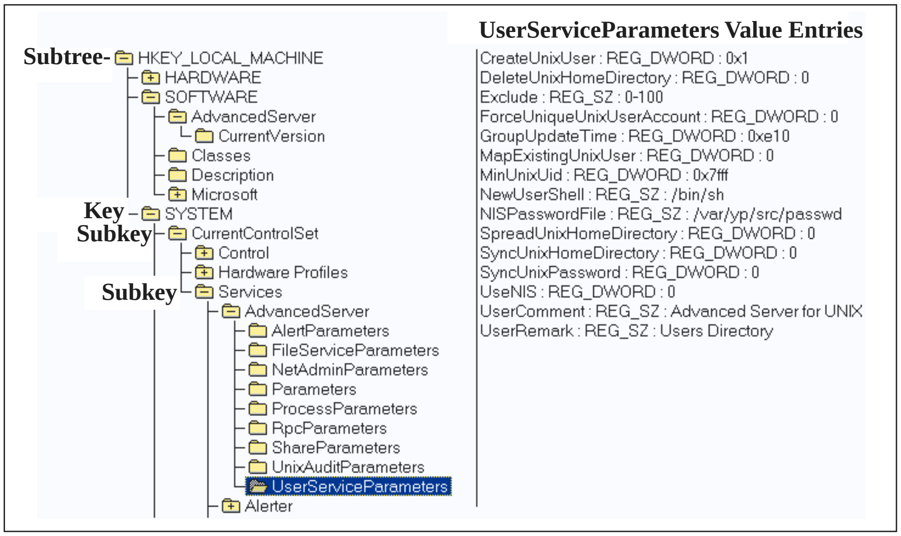
You change the default behavior of the ASU server by changing a value assigned to a value entry. To locate a value entry you follow a registry path that begins with a subtree. The ASU registry has the following subtrees:

- `HKEY_LOCAL_MACHINE`, which contains information about the local system.
- `HKEY_USERS`, which contains user profile information. Users on remote systems use the profiles that are loaded into the registry on their own computers.

From a subtree you choose a key and perhaps several subkeys to locate a value entry. For example, Figure 2–1 shows that the registry path to value entries for the `UserServiceParameters` subkey is in the `HKEY_LOCAL_MACHINE` subtree, `SYSTEM` key, `CurrentControlSet` subkey, then `Services` subkey. This registry path is displayed as:

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/
UserServiceParameters
```

Figure 2–1: Registry Path

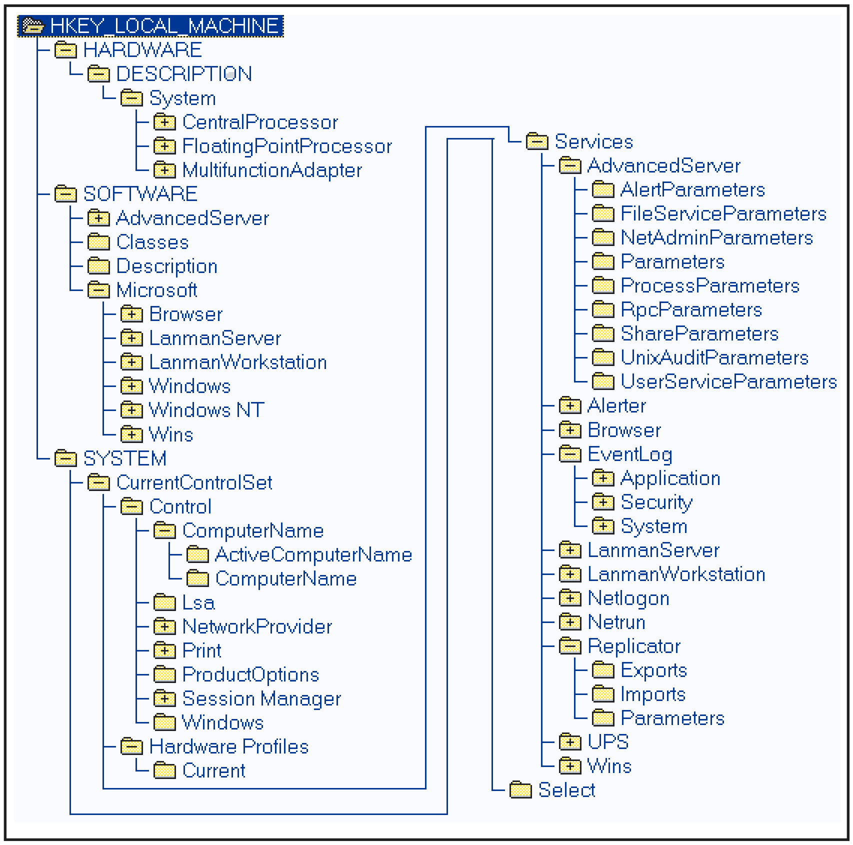


```
CreateUnixUser : REG_DWORD : 0x1
DeleteUnixHomeDirectory : REG_DWORD : 0
Exclude : REG_SZ : 0-100
ForceUniqueUnixUserAccount : REG_DWORD : 0
GroupUpdateTime : REG_DWORD : 0xe10
MapExistingUnixUser : REG_DWORD : 0
MinUnixUid : REG_DWORD : 0x7fff
NewUserShell : REG_SZ : /bin/sh
NISPasswordFile : REG_SZ : /var/yp/src/passwd
SpreadUnixHomeDirectory : REG_DWORD : 0
SyncUnixHomeDirectory : REG_DWORD : 0
SyncUnixPassword : REG_DWORD : 0
UseNIS : REG_DWORD : 0
UserComment : REG_SZ : Advanced Server for UNIX
UserRemark : REG_SZ : Users Directory
```

ZK-1657U-AI

Figure 2–2 shows some of the keys and subkeys for the `HKEY_LOCAL_MACHINE` subtree.

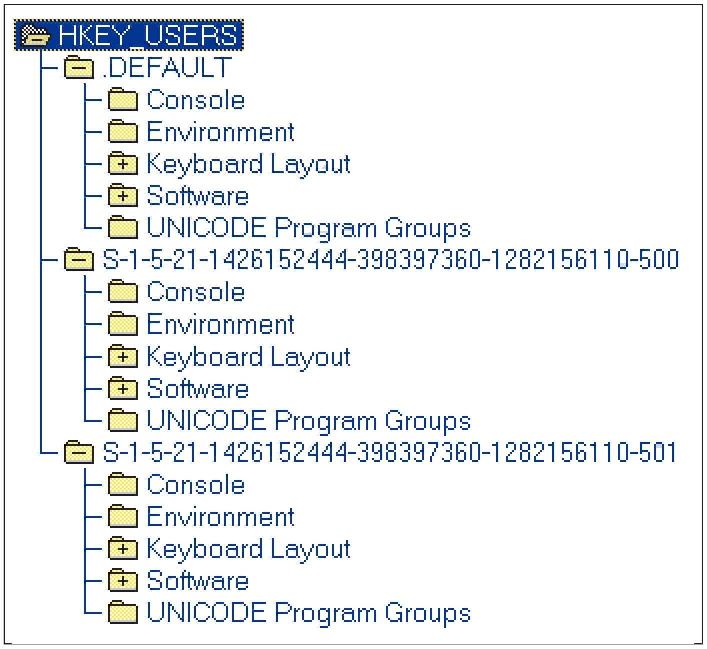
Figure 2–2: HKEY_LOCAL_MACHINE Keys and SubKeys



ZK-1658U-AI

Figure 2–3 shows some of the keys and subkeys for the `HKEY_USERS` subtree.

Figure 2–3: HKEY_USERS Keys and SubKeys

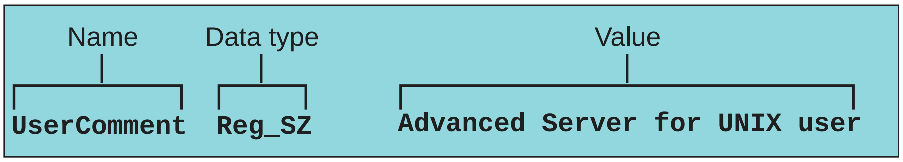


2.1.1 Value Entries

A subkey usually has several value entries. Each value entry defines how the ASU server and the Tru64 UNIX operating system software interoperate for a specific task.

See Appendix B for a complete description of registry value entries.

The following is an example of a value entry:



The three parts of a value entry are:

- Name - The value entry name.
- Data type - The value entry class or type.

- Value - The value assigned to the value entry. The type of value depends on the data type, as described in Table 2–1.

Table 2–1: Registry Data Types and Values

Data Type	Type of Value

REG_SZ	A sequence of characters representing readable text. The following example shows that the `UserComment` is `ASU`:
	`UserComment:REG_SZ:ASU`
	Enclose multiple words in quotes. The following example shows that the `UserComment` is `ASU user`:
	`UserComment:REG_SZ:"ASU user"`

REG_DWORD	A 4-byte number. Value entries of this type display in binary, hexadecimal, or decimal format. The following example shows the value entry that enables the mixed-case support: `MixedCaseSupport:REG_DWORD:1`
REG_EXPAND_SZ	An expandable data string, which is text that contains a variable that is replaced when called by an application. The following example shows the value entry that replaces the string `%SystemRoot%` with the location of the directory containing the ASU system files: `File:REG_EXPAND_SZ:%SystemRoot%\file.exe`
REG_MULTI_SZ	A multiple string in readable text, such as a list or multiple values. Entries are separated by NULL characters. The following example shows Administrator and peter are users who receive alert messages: `AlertNames:REG_MULTI_SZ:Administrator peter`

2.2 Viewing and Changing Registry Value Entries

Default values are assigned to value entries. You can change the default values; however, providing an incorrect value can cause unexpected results, including failure of the ASU software.

Use the following interfaces to view and change registry value entries:

- The `regconfig` command, a Tru64 UNIX command-line interface
- The Registry Editor, a Windows based interface
- The ASU Administrator, a Windows based interface
- The System Policy Editor, a Windows based interface

Note

You must stop and restart the ASU server to effect most changes in the ASU registry.

2.2.1 The regconfig Command

The `regconfig` command is a command that you enter at the Tru64 UNIX command prompt on a system that is running the ASU software.

To display information about common keys, subkeys, and value entries, enter:

```
# regconfig -l
```

To display specific information about a key, subkeys, and value entries, you must provide the full registry path. For example, to display information about the value entries for the `UserServiceParameters` subkey, enter the following command. The backslash (`\`) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

```
# regconfig System/CurrentControlSet/Services/\
AdvancedServer/UserServiceParameters
```

Output similar to the following is displayed that shows the name, data type, and value for each value entry for the `UserServiceParameters` subkey:

```
CreatePersonalShare:REG_DWORD:1
CreateUnixHomeDirectory:REG_DWORD:0
CreateUnixUser:REG_DWORD:1
DeleteUnixHomeDirectory:REG_DWORD:0
Exclude:REG_SZ:0-100
ForceUniqueUnixUserAccount:REG_DWORD:0
GroupUpdateTime:REG_DWORD:3600
MapExistingUnixUser:REG_DWORD:1
MinUnixUid:REG_DWORD:32767
NewUserShell:REG_SZ:/bin/sh
NISPasswordFile:REG_SZ:/var/yp/src/passwd
PreserveCase:REG_DWORD:0
PreserveNumericUserName:REG_DWORD:0
SpreadUnixHomeDirectory:REG_DWORD:0
SyncUnixHomeDirectory:REG_DWORD:0
SyncUnixPassword:REG_DWORD:0
UseActiveDirectory:REG_DWORD:0
UseNIS:REG_DWORD:0
UserComment:REG_SZ:Advanced Server for UNIX user
UserRemark:REG_SZ:Users Director
```

To change values for value entries, you must provide:

- The full registry path to the value entry

- The name of the value entry
- The type of the value entry
- The new value for the value entry

For example, to change the value of the `UserComment` to `ASU user`, enter the following command. The backslash (`\`) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

```
# regconfig System/CurrentControlSet/Services/\
AdvancedServer/UserServiceParameters UserComment \
REG_SZ "ASU user"
```

See `regconfig`(8) for more information on the `regconfig` command.

2.2.2 Registry Editor

The Registry Editor is a Windows based interface that you use on a system that is running the Windows NT operating system software.

Note

You cannot use the Windows 95 Registry Editor to remotely edit the ASU Registry.

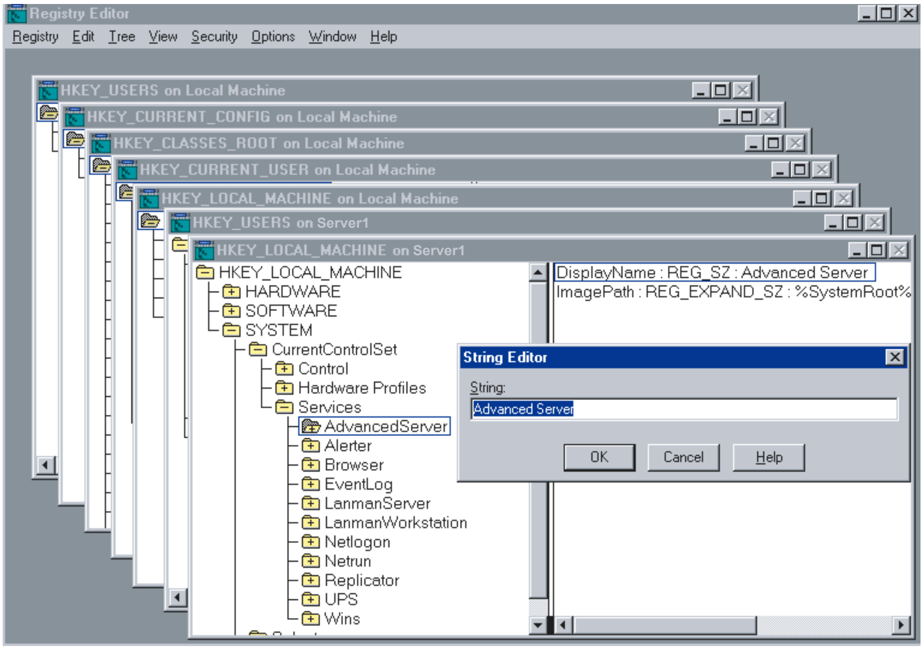
Follow these steps to start the Registry Editor on a Windows NT system:

1. Log in to the Windows NT system using the ASU administrator account.
2. Run the `regedt32.exe` application, which is in the `%SystemRoot%\system32` folder.

   When the Registry Editor starts, a window is displayed for each subtree for the local computer's registry.
3. Choose the Select Computer item on the Registry menu.
4. Enter the name of the ASU server in the Computer: field.
5. Click on the OK button.

When you connect to an ASU registry, the `HKEY_USERS` and `HKEY_LOCAL_MACHINE` subtrees are displayed.

The Registry Editor displays registry information in two frames. Keys and subkeys are displayed in the left frame and their value entries are displayed in the right frame as shown in the following figure:


Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_USERS on Local Machine
HKEY_CURRENT_CONFIG on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_CURRENT_USER on Local Machine
HKEY_LOCAL_MACHINE on Local Machine
HKEY_USERS on Server1
HKEY_LOCAL_MACHINE on Server1
HKEY_LOCAL_MACHINE
HARDWARE
SOFTWARE
SYSTEM
CurrentControlSet
Control
Hardware Profiles
Services
AdvancedServer
Alerter
Browser
EventLog
LanmanServer
LanmanWorkstation
Netlogon
Netrun
Replicator
UPS
Wins
String Editor
OK
Cancel
Help

DisplayName : REG_SZ : Advanced Server
ImagePath : REG_EXPAND_SZ : %SystemRoot%

String: Advanced Server

ZK-1661U-AI

Follow these steps to change a value:

1. Double-click on a value entry.

   The String Editor dialog box is displayed, as shown in the previous figure.
2. Type the new value in the string field.
3. Click on the OK button.

2.2.3 System Policy Editor

The System Policy Editor is a Windows based interface that you can use to view and manage policies that define the environment for specific Windows computers, users, or groups when logged in to a system running the ASU server.

Using the System Policy Editor you can set:

- A user-specific policy that applies to each domain 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 on a Windows system and does not change according to user since it does not follow users as

they move between different systems. Machine-specific policies are always merged into the `HKEY_LOCAL_MACHINE` key of the registry.

The System Policy Editor saves settings in a single policy (`.POL`) file. When a user logs in, a program called the policy downloader starts. The policy downloader is installed on every Windows 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 System Policy Editor is in the Client-based Advanced Server Administration Tools subset. See Section 1.8 for information on installing the Policy Administrator.

When the System Policy Editor starts, it displays icons for the users and computers with entries in the policy file.

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

2.2.4 ASU Administrator

The ASU Administrator is a Windows NT based interface. Unlike the other registry editors, the ASU Administrator only permits you to select or enter allowable values to modify value entries, which prevents you from entering an incorrect value in the registry.

2.2.4.1 Installing the ASU Administrator Interface

Follow these steps to install the ASU Administrator interface:

1. On the Tru64 UNIX system, ensure that the Client-based Advanced Server Administration Tools subset is installed, for example:

   ```
   # setld -i |grep ASUADM |grep -v not |grep installed
   ```

   If `ASUADM`*nnn* is displayed, the subset is installed. Otherwise, you must install the `ASUADM`*nnn* subset. See Section 1.3 for information on installing ASU subsets.
2. Log in to the system that is running the Windows NT operating system using the ASU administrator account that was created during the `asusetup` procedure.
3. Map a network drive to the `astools` disk share.

4. Expand the `asuadm` folder.
5. Run the `setup.bat` program.
6. After you install the ASU Administrator interface, disconnect the network drive to the astools disk share and create an icon for the ASU Administrator interface (`c:\winnt\system32\asuadm.exe`).

2.2.4.2 Using the ASU Administrator Interface

Follow these steps to use the ASU Administrator interface:

1. Log in to the Windows NT system using the ASU administrator account that was created during the `asusetup` procedure.
2. Run the `asuadm.exe` application, which is in the `%SystemRoot%\system32` folder on Windows NT systems.

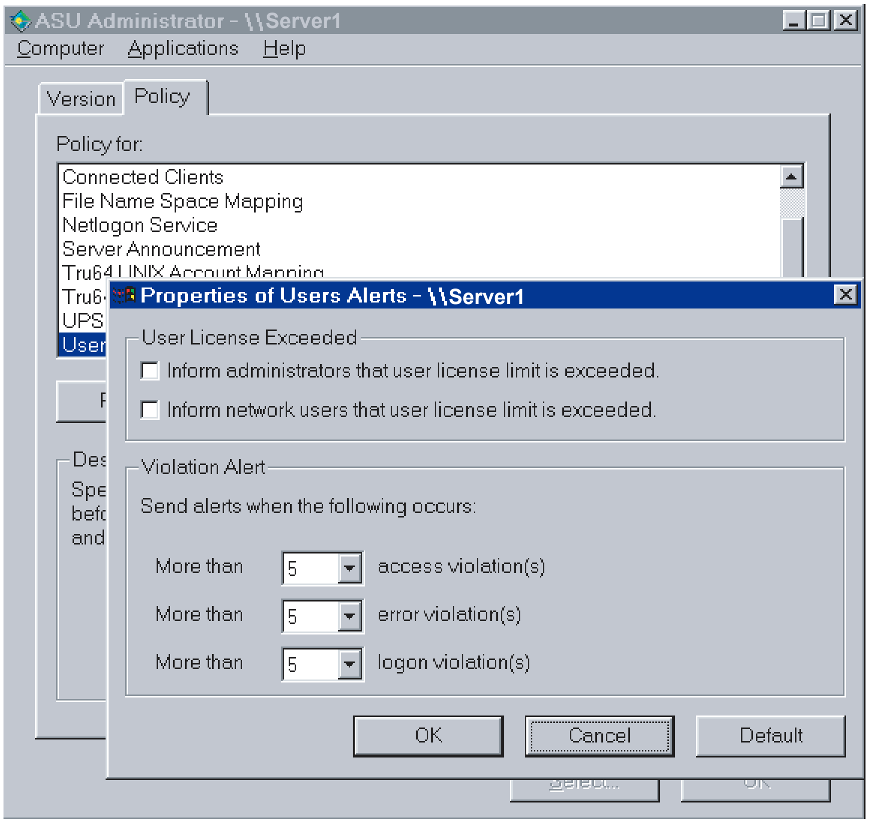
   The ASU Administrator interface starts and displays a Select Computer dialog box.
3. For the system for which you want to view or change registry values, either:
   - Enter the system name in the Computer field.
   - Click on system name in the Select Computer window.
4. Click on the OK button.
5. Click on the Policy tab. A policy is similar to a registry key or subkey.
6. In the Policy for: window, click on the policy for which you want to view or change value entries.
7. Click on the Properties button.

   A Properties window is displayed for the policy. The Properties window displays descriptions. A description is similar to a value entry. Next to each description is its value.

Depending on the value type, you change values by either:

- Clicking in a box to enable or disable a value entry. A check mark in a box indicates that the value entry is enabled.
- Choosing a value from a list of items.

The following figure shows an ASU Administrator Properties dialog box:



User License Exceeded

☐ Inform administrators that user license limit is exceeded.

☐ Inform network users that user license limit is exceeded.

Violation Alert

Send alerts when the following occurs:

More than 5 access violation(s)

More than 5 error violation(s)

More than 5 logon violation(s)

ZK-1662U-AI

The following list shows ASU Administrator policies and their related registry value entries:

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
SrvAnnounce
```

Tru64 UNIX Account Mapping

`SYSTEM\CurrentControlSet\Services\AdvancedServer\FileServiceParameters`

```
CreateUnixUser
```

Tru64 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
```

3

Creating User Accounts

By default, the ASU server and Tru64 UNIX operating system software must authenticate a user’s name and password before a user can access an ASU share. Therefore, a Windows user must have a domain user account that the ASU server uses for user authentication and a Tru64 UNIX user account that the Tru64 UNIX operating system uses for user authentication.

By default, when you create a domain user account, the ASU server automatically creates a Tru64 UNIX user account in the local `/etc/passwd` file if an account with the same name does not exit. The Tru64 UNIX operating system software uses the local user account information for authentication if you did not configure it to direct authentication requests to a Windows 2000 Server or to a Windows NT Server Version 4.0 as described in Section 1.1.3.

This chapter describes how to change the default ASU server behavior and how to create and manage domain user accounts and Tru64 UNIX user accounts created by the ASU server.

3.1 Domain User Account Attributes

A domain user account is the same whether you create it on an ASU server or a Windows NT server.

A domain user account is made up of three categories of attributes:

- Mandatory attributes for which you must provide values
- Mandatory attributes that are assigned default values that you can change
- Optional attributes for which you can provide values

Table 3–1 describes the mandatory domain user account attributes for which you must provide values when you create a domain user account.

Table 3–1: Mandatory Domain User Account Attributes

Attribute	Specifies	Restrictions/Default
User name	The name of the user account	A user name must be unique. Can contain up to 20 alphanumeric characters. However, 8 or fewer is recommended because by default, this user name maps to a Tru64 UNIX user name that is limited to 8 alphanumeric characters.
Password	The password assigned to the user account	Can contain up to 14 alphanumeric characters.

Table 3–2 describes the mandatory attributes that are assigned default values. You can change the default value when you create an domain account.

Table 3–2: Mandatory Domain User Account Attributes

Attribute	Specifies	Possible/Default Values
Account type	If the user account is global (for regular user accounts in this domain) or local (for user accounts on a member server that are not in the domain)	Global or local Default: Global
Active	If the user account is activated or deactivated	Yes or no Default: Yes (activated)
Country code	The language files for a user's help and error messages	A numeric value that the operating system uses for a country code Default: 0 (same as the operating system)
Expires	The date that the user account expires	A date or never Default: Never
Must change password	If the user must change password at next logon	Yes or no Default: When using the `net user` command the default is no (do not force a password change). When using the User Manager for Domains GUI the default is yes (force a password change).
Password change	If the user can change the password	Yes or no Default: Yes (allow change)

Table 3–2: Mandatory Domain User Account Attributes (cont.)

Attribute	Specifies	Possible/Default Values
Password expires	If the password expires based on the maximum password age	Yes or no Default: Yes (password expires)
Password must change	If the user must change the password at next logon	Yes or no Default: No (do not have to change password)
Password required	If a user account requires a password	Yes or no Default: Yes (requires a password)
Primary group	The primary group for the user	Any global group to which the user belongs Default: Domain Users
Times	The times when the user is allowed to use the ASU server	A specified time or All Default: All
Workstations	Up to eight computer names from which a user can log on to the network	A comma-separated list or an asterisk (*) or no list to allow log on from any client Default: * (all)

Table 3–3 describes the optional attributes for which you can provide values when you create a domain user account.

Table 3–3: Optional Domain User Account Attributes

Attribute	Specifies	Possible Values
Comment	A comment about the user's account	Can contain up to 48 alphanumeric characters enclosed in quotation marks
Full name	A user's full name (rather than user name)	Can contain up to 256 alphanumeric characters enclosed in quotation marks
Home directory	The pathname for the user's home directory	A path name Default: none
Home directory drive	A network drive letter; for example z:, to connect the user's remote home directory as a local drive.	An alpha character followed by a colon. Default: none
Profile path	A path for the user's logon profile	A path name Default: none

Table 3–3: Optional Domain User Account Attributes (cont.)

Attribute	Specifies	Possible Values
Script path	The path to the user's login script	A path name Default: none
User comment	An administrative comment	Can contain up to 48 alphanumeric characters enclosed in quotation marks

3.2 Tru64 UNIX User Accounts Created by ASU

By default, when you create a domain user account, the ASU server automatically creates a Tru64 UNIX user account (using lowercase letters) in the local `/etc/passwd` file if an account with the same name does not exist.

You control if and how the ASU server creates Tru64 UNIX user accounts by assigning values to registry value entries located in the following registry path:

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/
AdvancedServer/UserServiceParameters
```

If the `CreateUnixUser` value entry is enabled, which it is by default, then how and where the ASU server creates Tru64 UNIX user accounts depends on the values assigned to other entries in the `UserServiceParameters` registry subkey. For example, entries that define:

- Whether or not the ASU server creates a Tru64 UNIX user account using the same case that you entered to create a domain user account
- The default user account and login attributes that are assigned to all Tru64 UNIX user accounts created by the ASU server
- How the ASU server creates Tru64 UNIX user account home directories
- If the ASU server creates Tru64 UNIX user accounts in the local `/etc/passwd` file or in a Network Information Service (NIS) database
- If a user's Tru64 UNIX user account password is automatically synchronized to their domain user account password when the user changes their domain user account password

The following sections describe some of the registry value entries that effect the setup and behavior of Tru64 UNIX user accounts that are created by the ASU server. See Section B.1.9 for a complete list of registry value entries that effect how the ASU server creates Tru64 UNIX user account.

3.2.1 ASU and Tru64 UNIX User Account Attributes

By default, the ASU server creates a Tru64 UNIX user account using the same name in lowercase letters as the domain user account. However, domain user account names can contain up to 20 characters; the maximum number of characters for a Tru64 UNIX user account is 8. If a domain user account name exceeds 8 characters, then the ASU server creates a Tru64 UNIX user account using the first 6 characters and substitutes random characters for the last 2 characters. For example, if a domain user account name is `longusername`, then the corresponding Tru64 UNIX user account that the ASU server creates might be named `longush3`.

If you are using Tru64 UNIX for user account authentication, then you must set Tru64 UNIX passwords for users before they can log in to the Tru64 UNIX system.

Table 3–4 describes the registry value entries that effect how the ASU server creates Tru64 UNIX user accounts.

Table 3–4: User Account Value Entries

Entry	Specifies/Default
`Exclude`	A range of Tru64 UNIX user IDs that the ASU server cannot assign. If the ASU server attempts to create a Tru64 UNIX account with a name that matches a user ID in the exclude list, then the ASU server generates a new Tru64 UNIX user account. Default: 0 - 100
`ForceUniqueUnixUserAccount`	Whether to automatically assign an existing Tru64 UNIX user account if one exists when the ASU server creates a Tru64 UNIX user account, or to create a unique Tru64 UNIX user account. Default: 0 (Assign existing accounts)
`NewUserShell`	The login shell for new Tru64 UNIX user accounts. Set this key to `/bin/false` to prevent users from logging in to the Tru64 UNIX system. Default: `/bin/sh`

Table 3–4: User Account Value Entries (cont.)

Entry	Specifies/Default
`PreserveCase`	Whether or not the ASU server creates Tru64 UNIX user accounts using the same case that you enter to create domain user accounts. Default: 0 (do not preseve the case; create Tru64 UNIX user accounts using lowercase letters)
`UserRemark`	Specifies the comment associated with the USERS shared directory. Default: Users Directory

You use a registry editor to change the values of these entries. For example, follow these steps to use the `regconfig` editor to change the `UserRemark` entry to display `ASU user home directories`. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Change the text associated with the `UserRemark` entry to `ASU user home directories` by entering the following command:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
AdvancedServer/UserServiceParameters \
UserRemark  REG_SZ 'ASU user home directories'
```

2. Restart the ASU server by entering the following commands:

```
# net stop server
```

```
# net start server
```

3.2.2 ASU and Tru64 UNIX User Account Home Directories

Table 3–5 describes the registry value entries that define how the ASU server effects Tru64 UNIX user directories:

Table 3–5: User Directory Value Entries

Entry	Specifies/Default
`CreateUnixHomeDirectory`	Whether or not the ASU server creates a user's Tru64 UNIX home directory when it creates a Tru64 UNIX user account. Default: 1 (create Tru64 UNIX home directory)

Table 3–5: User Directory Value Entries (cont.)

Entry	Specifies/Default
`DeleteUnixHomeDirectory`	Whether or not the ASU server deletes a user's Tru64 UNIX home directory when it deletes the Tru64 UNIX user account. Note: The ASU server only deletes Tru64 UNIX user accounts that it created. Default: 0 (do not delete home directories)
`SpreadUnixHomeDirectory`	Whether or not the ASU server creates Tru64 UNIX user home directories in a one-letter subdirectory that corresponds to the first letter of the user name. For example, whether or not the Tru64 UNIX home directory for a user named peter is created as `/usr/users/p/peter`. Enabling this entry allows you to create more than 32,768 user home directories under the `/usr/users` directory path. Default: 0 (do not use one-letter subdirectories)
`SyncUnixHomeDirectory`	Whether or not the ASU server changes the Tru64 UNIX home directory of a user account if the home directory of the associated domain user account changes. Default: 0 (do not synchronize home directories)

You use a registry editor to change the values of these keys. For example, follow these steps to use the `regconfig` registry editor to delete a user's Tru64 UNIX home directory when you delete their domain user account. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Enable the `DeleteUnixHomeDirectory` entry by entering the following command:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/UserServiceParameters \
   DeleteUnixHomeDirectory REG_DWORD 1
   ```

2. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

3.2.3 Local or NIS Tru64 UNIX User Accounts

By default, the ASU server creates Tru64 UNIX user accounts in the local `/etc/passwd` file. If the Tru64 UNIX system is configured as the ASU PDC and the network information service (NIS) master, you can configure the ASU server to use NIS when creating Tru64 UNIX user accounts.

Table 3–6 describes the registry value entries that specify if the ASU server creates Tru64 UNIX user accounts with NIS.

Table 3–6: User Account NIS Value Entries

Registry Value Entry	Specifies/Default
`UseNIS`	Whether or not the ASU server uses NIS to create Tru64 UNIX user account. Enable this value entry only on a Tru64 UNIX system that is configured as an ASU PDC and as a NIS master. Default: 0 (not enabled)
`NISPasswordFile`	The directory path to the NIS password file. Default: `/var/yp/src/passwd`

Use a registry editor to change the values of these entries. For example, follow these steps to use the `regconfig` registry editor to enable the ASU server to use NIS when creating Tru64 UNIX user accounts. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Ensure that the ASU server is configured as the PDC. To display the role of the ASU server, enter:

   ```
   # net computer
   ```

   See Chapter 1 if you need to reconfigure the role of the ASU server.

2. On the PDC, ensure that the system is the NIS master. To display and change a system's NIS configuration, enter:

   ```
   # nissetup
   ```

3. On the PDC, enable the `UseNIS` entry by entering the following command:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/UserServiceParameters UseNIS REG_DWORD 1
   ```

4. On the PDC, display the value of the `NISPasswordFile` entry and, if necessary, change the value. To display the value of the `NISPasswordFile` entry, enter:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/UserServiceParameters NISPasswordFile
   ```

5. On BDCs, ensure that the `CreateUnixUser` entry is disabled so that it does not create Tru64 UNIX user accounts. To display the value of the `CreateUnixUser` entry, enter:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/UserServiceParameters CreateUnixUser
   ```

   To disable the `CreateUnixUser` entry, enter:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/UserServiceParameters \
   CreateUnixUser REG_DWORD 0
   ```

6. On each system for which you changed a registry value, restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

3.2.4 Tru64 UNIX and Domain Password Synchronization

The ASU software associates the domain and Tru64 UNIX user accounts; however, the accounts are independently stored and managed and users can set different passwords for each account. To coordinate user passwords, the ASU software provides the following options:

- The `SyncUnixPassword` registry entry

  The `SyncUnixPassword` registry entry specifies whether or not Tru64 UNIX user passwords are synchronized to their domain user account password when their domain password is changed.

- The Change Password utility

  The Change Password utility is a Windows-based interface that you install on a Windows system to allow users to set their domain user account and Tru64 UNIX user account or NIS passwords at the same time.

3.2.4.1 Enabling the `SyncUnixPassword` Entry

To configure the ASU server to synchronize passwords, you must enable the `SyncUnixPassword` entry.

If the `UseNIS` entry is enabled, the ASU server synchronizes Tru64 UNIX passwords in the file defined by the `NISPasswordFile` entry. Otherwise, the ASU server synchronizes passwords in the local `/etc/passwd` file.

See Section 3.2.3 for more information on NIS.

The Tru64 UNIX user account must have a valid password. For example, the ASU server will not synchronize a Tru64 UNIX password of `NoLogin` or asterisk (*). You must use Tru64 UNIX commands or utilities to change the password to a valid Tru64 UNIX password.

Follow these steps to use the `regconfig` registry editor to configure the ASU server to synchronize Tru64 UNIX passwords to domain user account passwords. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. On the PDC, enable the `SyncUnixPassword` registry entry. To enable the `SyncUnixPassword` registry entry, enter:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/UserServiceParameters \
   SyncUnixPassword REG_DWORD 1
   ```

2. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

3.2.4.2 Installing the Change Password Utility

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

Follow these steps to install the Change Password utility on a system running the Windows operating system software:

1. On the Tru64 UNIX system, ensure that the Client-based Advanced Server Administration Tools subset is installed. To display installed ASU subsets, enter:

   ```
   # setld -i |grep ASU |grep -v not |grep installed
   ```

   Look for the `ASUADM`*nnn* (*nnn* reflects the current ASU version) subset in the output.

   If `ASUADM`*nnn* is displayed, the subset is installed. Otherwise, you must install the `ASUADM`*nnn* subset. See Section 1.3 for information on installing ASU subsets.

2. Connect a network drive to the `astools` disk share.
3. Select the `asdupass` folder.
4. Change to the `i386` directory.
5. Run the `setup.exe` program and follow the instructions on the screen.

3.2.4.2.1 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:

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

   The Password Properties dialog box is displayed
2. Click on the Change Other Passwords... button.

   The Select Password dialog box is displayed
3. Select either the ASDU UNIX or NIS password option to change your Tru64 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.

See the Password Management utility online help for more information about the Password Management utility.

3.2.4.2.2 Using the Password Management Utility on a Windows NT System

Follow these steps to start the Password Management utility on a system running the Windows NT operating system software:

1. Expand the Programs option from the Start button.
2. Select the ASDU Password option to start the Password Management utility.

Enter your old and new passwords in the password fields, then choose the account to which you want to apply the change and click on:

- The Setup... button next to the Windows section to change the domain user account password.
- The Setup... button next to the UNIX section to change the Tru64 UNIX or NIS password.

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

See the Password Management utility online help for more information about the Password Management utility.

3.3 Disabling ASU from Creating Tru64 UNIX User Accounts

You can configure the ASU server to not create Tru64 UNIX user accounts when you create domain user accounts. This is recommended if you are running NIS and the ASU server is configured as a BDC.

Follow these steps to use the `regconfig` registry editor to configure the ASU server to not create Tru64 UNIX user accounts. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Disable the `CreateUnixUser` entry by entering the following command:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
AdvancedServer/UserServiceParameters \
CreateUnixUser REG_DWORD 0
```

2. Restart the ASU server by entering the following commands:

```
# net stop server
```

```
# net start server
```

If you disable the `CreateUnixUser` entry, you can follow these steps to use the `regconfig` registry editor to enable the `MapExistingUnixUser` entry to map a newly created domain user account to an existing Tru64 UNIX user account with the same name in lowercase letters. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Enable the `MapExistingUnixUser` entry by entering the following command:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
AdvancedServer/UserServiceParameters \
MapExistingUnixUser REG_DWORD 1
```

2. Restart the ASU server by entering the following commands:

```
# net stop server
```

```
# net start server
```

3.4 Creating a Domain User Account

You can use either of the following interfaces to create a domain user account:

- The `net user` command with the `/add` option
- The User Manager for Domains GUI

You can also use the following Tru64 UNIX interfaces to create a domain user account when you create a Tru64 UNIX user account:

- Account Manager (`dxaccounts`)

- The `useradd`, `usermod`, and `userdel` commands

See *System Administration* for more information on creating domain user accounts using Tru64 UNIX interfaces.

Caution

On a Tru64 UNIX Version 5.0 or higher system, a lock file called `/etc/.AM_is_running` prevents you from using two different interfaces (or two instances of the same interface) at the same time. This might happen in large environments in which many administrators are managing user accounts. If the lock file exists, only one process can access the system files that relate to user and group data. If you attempt to invoke a second instance of any Tru64 UNIX account management interface, an error message informs you that the data file is locked.

If the lock file exists, neither the `net` command nor the User Manager for Domain GUI inform you about the presence of the lock file and creates only the domain user account. The associated Tru64 UNIX user account is not created. A message indicating that the associated Tru64 UNIX user account was not created or a lock file error message is displayed. When using the `net` command or the User Manager Manager for Domain GUI, you must check the `/etc/passwd` file to verify that the associated Tru64 UNIX user account was created.

3.4.1 Using the net user Command

You enter a `net` command in lowercase at the Tru64 UNIX command prompt on a system running the ASU server. Press the Enter key at the end of the entire command.

Table 3–7 shows the user account attributes and the `net user` command option that you use to set the attribute. See Section 3.1 for more information on these attributes.

Table 3–7: Setting User Account Attributes

Attribute	net user Option
User name	Enter the user name after the `net user` command
Password	Enter the password or an asterisk (*) to be prompted for the password
Account type	`/accounttype:{global | local}`

Table 3–7: Setting User Account Attributes (cont.)

Attribute	net user Option
Active	`/active:{yes | no}`
Comment	`/comment:"value"`
Country code	`/countrycode:value`
Expires	`/expires:{date | never}`
Full name	`/fullname:"value"`
Home directory	`/homedir:pathname`
Home directory drive	`/homedirdrive:letter`
Must change password	`/passwordmustchg:{yes | no}`
Password required	`/passwordreq:{yes | no}`
Password change	`/passwordchg:{yes | no}`
Password expires	`/passwordexp:{yes | no}`
Primary group	`/primarygroup:[groupname]`
Profile path	`/profilepath:[pathname]`
Script path	`/scriptpath:[pathname]`
Times	`/times:{times | all}`
User name	`/username:"new_name"`
User comment	`/usercomment:"text"`
Workstation	`/workstations:{computername[,...]  | *}`

To create a domain user account named peter and a password of temporary, enter:

```
# net user peter temporary /add
```

To create a domain user account named peter and be prompted for the password, enter:

```
# net user peter \* /add
```

Enter the following command to create a domain user account named peter with a password of temporary, a comment of Office 3C, and force the user to change the password when first connecting to an ASU share. The backslash (\) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

```
# net user peter temporary /comment:"Office 3C"\
/passwordmustchg:yes /add
```

3.4.2 Using the User Manager for Domains

Follow these steps to create a domain user account using the User Manager for Domains GUI:

1. Start the User Manager for Domains GUI (`usrmgr.exe`).

   You must install the User Manager for Domains GUI on the Windows system from which you will administer the ASU server. See Section 1.8 for information on installing the User Manager for Domains GUI.

   The main User Manager for Domains windows is displayed.

2. From the User menu, choose Select Domain.

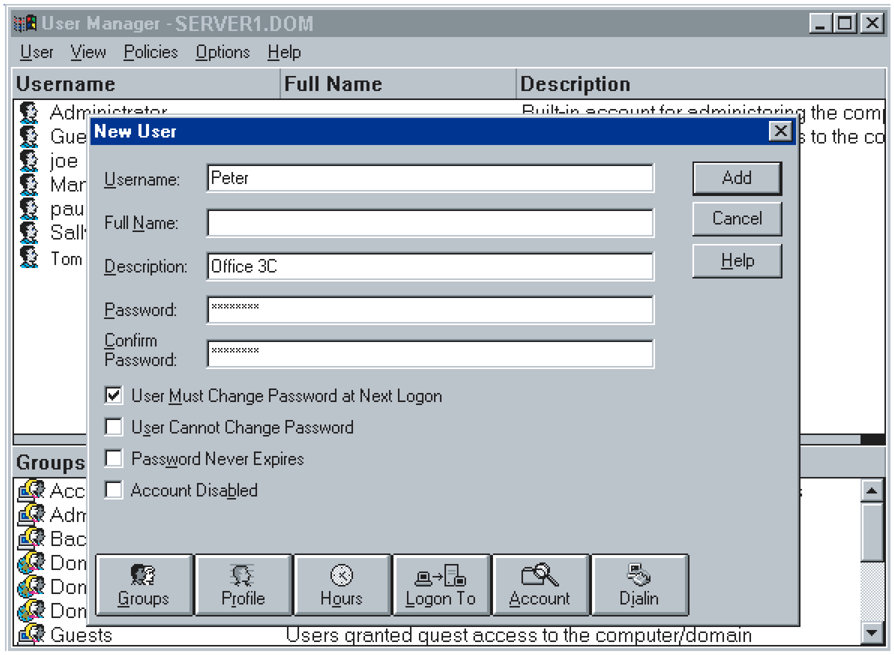
   The Select Domain dialog box is displayed.

3. Choose the name of the domain in which you want to create the account by either entering the name in the Domain: field or by browsing and clicking on the domain name in the Select Domain: window.

   A dialog box is displayed that shows user account names in the domain.

4. Choose New User from the Users menu.

   A New Users dialog box displays where you enter user information as shown in the following figure:



Username: Peter

Full Name:

Description: Office 3C

Password: ********

Confirm Password: ********

☑ User Must Change Password at Next Logon

☐ User Cannot Change Password

☐ Password Never Expires

☐ Account Disabled

Built-in account for administering the comp

Users granted guest access to the computer/domain

ZK-1663U-AI

Enter the user name, password, and other user account attributes in the appropriate fields. Click on the Groups, Profiles, Hours, Logon To, Account, or Dialin button to provide information for those related attributes.

5. Click on the Add button to create the user account.

3.5 Domain and Tru64 UNIX User Account Mapping

The ASU server stores the mapping of a user's domain user account to their corresponding Tru64 UNIX user account. By default, one domain user account is mapped to one Tru64 UNIX user account. You can map one or many domain user accounts to a Tru64 UNIX user account. You cannot map a domain user account to multiple Tru64 UNIX user accounts.

The following are special mappings of domain user accounts to Tru64 UNIX user accounts:

- The domain administrator's user account is mapped to the Tru64 UNIX `lmxadmin` user account and is assigned the user ID of 200.
- The domain guest user account is mapped to the `lmxguest` Tru64 UNIX user account and is assigned the user ID of 201.
- A domain user account that is not mapped to a specific Tru64 UNIX user account or an account from a trusted domain that is not mapped to a local Tru64 UNIX user account, is mapped to the `lmworld` Tru64 UNIX user account and is assigned the user ID of 202.

The ASU server assigns the `lmxadmin`, `lmxguest`, and `lmworld` Tru64 UNIX user accounts the next available user ID if 200, 201, or 202 are assigned to other accounts.

You use the `mapuname` command to view and change the mapping between a user's domain user account and their corresponding Tru64 UNIX user account.

To display domain user account to Tru64 UNIX account mappings, enter:

```
# mapuname
```

Information similar to the following is displayed that shows the mappings for the built-in accounts and the user accounts in a domain. In the following example, the domain is called asudoc.dom.

```
Builtin:Account Operators       lmxadmin
asudoc.dom:john john
asudoc.dom:evan evan
asudoc.dom:Administrator        lmxadmin
Builtin:Server Operators        lmxadmin
:SYSTEM root
```

```
asudoc.dom:sam  sam
asudoc.dom:stan stan
asudoc.dom:peter        peter
asudoc.dom:Domain Admins        lmxadmin
Builtin:Print Operators lmxadmin
Builtin:Guests  lmxguest
asudoc.dom:Domain Guests        lmxguest
asudoc.dom:Guest        lmxguest
Builtin:Administrators  lmxadmin
Builtin:Backup Operators        lmxadmin
```

Follow these steps to change the mapping between a domain user account and a Tru64 UNIX user account:

1. Delete the current mapping. To delete the current mapping for a user named peter, enter:

   ```
   # mapuname -d peter
   ```

2. Add the new mapping. To map peter's account to the lmxadmin Tru64 UNIX account in a domain called asudoc.dom, enter:

   ```
   # mapuname -a asudoc.dom:peter lmxadmin
   ```

3. Instruct the user to disconnect and reconnect to shares to effect the change. To verify that the user is disconnected, enter:

   ```
   # net session \\pc_name
   ```

   In this example, **\\*pc_name*** is the name of the user's system. A user is disconnected if a message indicates that there are no sessions for the computer.

See `mapuname`(8) for more information on the `mapuname` command.

3.6 Using Windows NT Server Version 4.0 Authentication

This section describes how users can log in to a Tru64 UNIX application and can change their passwords if you installed the ASU SIA software to configure the Tru64 UNIX operating system software use a Windows NT Version 4.0 Server for authentication, as described in Section 1.1.3.2.

3.6.1 Logging In To a Tru64 UNIX Application

Users can log in to a Tru64 UNIX application using their domain user account information by including the name of the domain that contains their user account information and their domain user name, for example:

\\*domain_name*\*user_name*

The double backslashes (\\) are optional. Users can omit the **\\*domain_name*** if they are logged in to the domain that contains their domain user account. To specify a default domain, edit the `lanman.ini` file and add the following entry under the [`workstation`] section:

```
[ workstation ]
defaultdomain=domain_name
```

Replace ***domain_name*** with the name of the default domain.

The ASU SIA module checks user name and password requests. If the ASU SIA module cannot authenticate the request, the request is passed to the local Tru64 UNIX security module.

If ASU SIA authenticates the request, the ***domain_name*** is stored in the `NTUSERDOMAIN` environment variable and the ***user_name*** is stored in the `NTUSERNAME` environment variable.

A user can use either their domain or Tru64 UNIX user account name and password with the Tru64 UNIX `su` command using the following format:

```
su [-f] | [-] \\domain_name\user_name
```

The double backslashes (\\) are optional. Users can omit the **\\*domain_name*** if they are logged in to the default ASU domain. If the user omits the ***user_name***, the default is root.

3.6.2 Specifying Only Tru64 UNIX Authentication

Users can specify only Tru64 UNIX authentication when logging in to a Tru64 UNIX application by entering a colon (:) before their user name, for example:

```
:user_name
```

You can specify only Tru64 UNIX authentication for a user by entering the account name in the `/etc/asusiausers` file. The `/etc/asusiausers` file is a text file that you edit to enter one user account name per line. User account names must exactly match the user account name in the `/etc/passwd` file. In the `/etc/asusiausers` file white space is prohibited and a pound sign (#) must precede a comment line.

By default, the `/etc/asusiausers` file contains the root account. A user whose Tru64 UNIX user account name is in the `/etc/asusiausers` file must log in to a UNIX application using the following format:

```
\\domain_name\user_name
```

3.6.3 Changing Passwords

Users change their domain or Tru64 UNIX password by entering the Tru64 UNIX `passwd` command with the name of the domain that contains their user account information and their user name, for example:

```
passwd '\\domain_name\user_name'
```

The single quotes surrounding the domain and user names are necessary to prevent a shell from interpreting the backslash as an escape character. The double backslashes (\\) are optional. Users can omit the **`\\domain_name`** if they are logged in to their ASU domain. If the user omits the **`user_name`**, the default name is the value in the `NTUSERNAME` environment variable. If the `NTUSERNAME` is not set, the default name is the associated Tru64 UNIX user account name.

The user is either prompted for password information or a menu is displayed from which users choose a password to change. The menu is displayed if the user's name is recognized by more than one security module. Users choose ASU to change a domain password or BSD to change a Tru64 UNIX password.

3.7 Deleting a Domain User Account

To delete a domain user account you can use either:

- The `net user` command with the `/delete` option. For example, to delete a domain user account named peter, enter:

  ```
  # net user peter /delete
  ```

- The User Manager for Domains GUI.

  Follow these steps to delete a user account:

  1. Start the User Manager for Domains GUI (`usrmgr.exe`).

     You must install the User Manager for Domains GUI on the Windows system from which you will administer the ASU server. See Section 1.8 for information on installing the User Manager for Domains GUI.

     The main User Manager for Domains window is displayed.

  2. From the User menu, choose Select Domain.

     The Select Domain dialog box is displayed.

  3. Choose the name of the domain in which you want to delete the account by either entering the name in the Domain: field or by browsing and clicking on the domain name in the Select Domain: window.

A dialog box is displayed that shows the user account names in the domain.

4. Click on a user account name.
5. Choose Delete from the User menu.

3.8 Grouping Domain User Accounts

To ease administration, you can group domain user accounts and administer the group as one unit. Users added to a group become members of the group and immediately acquire the rights and permissions granted to the group. Changes made to the group effect each member.

Like user accounts, ASU and the Tru64 UNIX operating system software maintain separate repositories for group information. However, there is no mapping between ASU groups and Tru64 UNIX groups.

By default, a domain user account is a member of the Windows `Everyone` group and the `Domain Users` group. You cannot administer, that is, add users to or remove users from, the `Everyone` group. You can administer the `Domain Users` group or any other group that you create. Tru64 UNIX user accounts created by the ASU server are members of the Tru64 UNIX `users` group.

Certain ASU files are assigned DOS attributes. The ASU server uses the Tru64 UNIX group field and group numbers 91 through 99 to store DOS attributes. If, during the ASU installation, group numbers 91 to 99 groups are available, then the ASU server creates the following entries in the `/etc/group` file:

```
DOS----::99:
DOS-a--::98:
DOS--s-::97:
DOS---h::96:
DOS-as-::95:
DOS-a-h::94:
DOS--sh::93:
DOS-ash::92:
Other::91:
```

If, during the ASU installation, the group numbers 91 to 99 are not available, then the ASU server selects the next available range of group numbers and assigns them to the DOS attributes entries.

3.8.1 Creating and Administering a Domain Group

To create a domain group you must create the group, then add domain user accounts to the group. To create a domain group, you can use either:

- The `net group` command with the `/add` option
- The User Manager for Domains GUI

3.8.1.1 Using the net Command

Enter a `net` command in lowercase at the Tru64 UNIX command prompt on a system running the ASU server. Press the Enter key at the end of the entire command.

To create a group called project1, enter:

```
# net group project1 /add
```

To add the peter, jen, mike, and sue domain user accounts as members to the project1 group, enter:

```
# net group project1 peter jen mike sue /add
```

To view project1 group information, enter:

```
# net group project1
```

3.8.1.2 Using the User Manager for Domains

Follow these steps to use the User Manager for Domains:

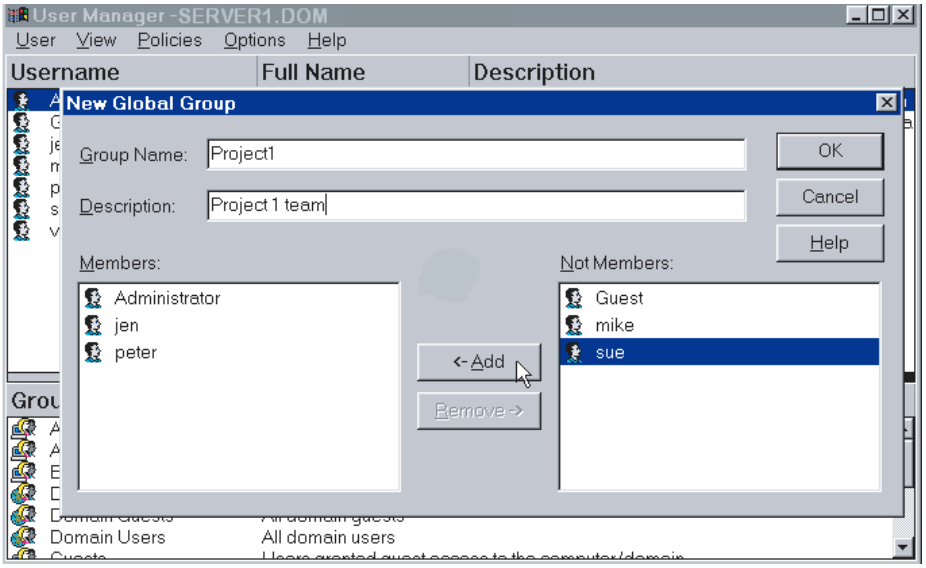
1. Start the User Manager for Domains GUI (`usrmgr.exe`).

   You must install the User Manager for Domains GUI on the Windows system from which you will administer the ASU server. See Section 1.8 for information on installing the User Manager for Domains GUI.

   The main User Manager for Domains window is displayed.
2. Choose Select Domain... from the User menu.

   The Select Domain dialog box is displayed.
3. In the Domain: field, enter the name of the domain in which you want to create the group and click on the OK button.

   The User Manager main window is displayed. The top half of the window displays user names, the bottom half displays group names.
4. Choose New Global Group from the User menu. The New Global Group box is displayed.
5. Enter the name of the group and an optional group description. To add members to the group, click on a name in the Not Members window then click on the Add button, as shown in the following figure:



Group Name: Project1

Description: Project 1 team

ZK-1664U-AI

3.8.2 Deleting a Domain Group

To delete a domain group, you can use either:

- The `net group` command with the `/delete` option
- The User Manager for Domains GUI

3.8.2.1 Using the net Command

Enter a `net` command in lowercase at the Tru64 UNIX command prompt on a system running the ASU server. Press the Enter key at the end of the entire command.

To delete the project1 group, enter:

```
# net group project1 /delete
```

3.8.2.2 Using the User Manager for Domains

Follow these steps to use the User Manager for Domains:

1. Start the User Manager for Domains GUI (`usrmgr.exe`).

   Install the User Manager for Domains GUI on the Windows NT system from which you will administer the ASU server. See Section 1.8 for information on installing the User Manager for Domains GUI.

The User Manager for Domains window is displayed.

2. Choose Select Domain... from the User menu.

   The Select Domain dialog box is displayed.

3. In the Domain: field, enter the name of the domain in which you want to delete the group and click on the OK button.

   The User Manager main window is displayed. The top half of the window displays user names, the bottom half displays group names.

4. Click on the name of the group that you want to delete.

5. Choose Delete from the User Menu.

4

Creating ASU Disk Shares

You can share the following types of file systems as disk shares with domain users:

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

This chapter describes how to share file systems with domain users.

4.1 Default Disk Share Attributes

You control how the ASU server creates disk shares by assigning values to registry value entries located in the following registry path:

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/
AdvancedServer/FileServiceParameters
```

Entries in this path define:

- Whether or not the ASU server automatically creates a disk share for file systems exported through network file system (NFS)
- Whether or not Tru64 UNIX permissions are checked before a user can access files and directories in disk share
- Whether or not the ASU server uses Tru64 UNIX groups or DOS groups
- How the ASU server applies NTFS ACLs

See Section B.1.2 for a complete list of registry entries that effect disk shares.

4.1.1 Disk Shares Created By ASU for NFS Exported File Systems

By default, the ASU server automatically creates a disk share for NFS exported file systems. The ASU server creates the disk share using:

- The name of the exported file system as the disk share name.
- The path in the `/etc/exports` file, which is converted to DOS format and preceded with `c:` as the path to the disk share. For example, if the

`/etc/exports` entry is `/home/nfs/usr/src`, then the ASU server uses `c:\home\nfs\usr\src` as the path to the disk share.

If a disk share exists with the same name as the exported resource but with a different path, 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 the ASU server creates a disk share called `src_0` with a path of `c:\home\nfs\usr\src`. The ASU server does not create a new disk share if a disk share exists with the same name and path as the exported resource.

- The number of users that can access the share is set to no limit.

4.1.1.1 Converting NFS Permissions

The following table describes how the ASU server converts NFS permissions to disk share permissions:

NFS Permission	Disk Share Permission
`Read` (`r`) and `Write` (`w`)	Full Access
`Not specified`	Full Access
`Read Only` (`ro`)	Read and Execute (for the specified list of clients).
`None`	No Access

The following table provides examples of how the ASU server converts NFS permissions to disk share permissions:

NFS Permission	Disk Share Permission
`/usr/local`	Full Access for all clients
`/usr/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=client1:10.0.0.10`	Full Access for `client1` from `10.0.0.10` and No Access for all other clients

The ASU server does not create a share for NFS mount points with the following NFS permissions:

- `/usr/local -root=0 client1`

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

4.1.1.2 Managing NFS Related Disk Shares Created by ASU

By default, when the ASU server starts, it synchronizes the ASU disk shares with NFS export entries. If an exports entry does not have a corresponding disk share, the ASU server creates the disk share. If an exports entry no longer exists or is not supported (root=0), the ASU server deletes the corresponding disk share. If the NFS permissions for an NFS export entry changed, the ASU server updates the permissions on the corresponding disk share.

You use the `nfsshare` command to:

- Delete one or all shares related to an NFS exported file system. If a share name is supplied on the command line, only that share is deleted. For example, to delete all shares relating to NFS exported file systems, enter:

  ```
  # nfsshare -d
  ```

- List one or all shares related to an NFS exported file system. If a share name is supplied on the command line, only that share is listed. For example, to list all shares relating to NFS exported file systems, enter:

  ```
  # nfsshare -l
  ```

- Synchronize NFS exported file systems with ASU disk shares, which creates a disk share for new NFS exported file system and removes disk shares for NFS exported file systems that no longer exist. For example, to synchronize all shares relating to NFS exported file systems, enter:

  ```
  # nfsshare -s
  ```

See `nfsshare`(8) for more information on the `nfsshare` command.

4.1.1.3 Controlling the ASU Creation of NFS-Related Disk Shares

If the `ShareNFSExports` entry is enabled, which is the default, then the creation of ASU disk shares for NFS exported file systems depends on the values assigned to the NFS-related entries in the `FileServiceParameters` registry subkey. Table 4–1 describes the NFS-related registry value entries.

Table 4–1: NFS-Related Disk Share Value Entries

Entry	Description and Default Value
`NFSExportFile`	Specifies the name of the NFS export file. Default: `/etc/exports`
`SyncNFSExports`	Determines whether or not NFS exports are synchronized with disk shares when the ASU server starts. If this entry is disabled, disk shares that were created from the NFS exports are deleted. Default: 1 (synchronize at ASU server startup)

4.1.1.4 Configuring ASU to Not Create NFS-Related Disk Shares

You can configure the ASU server to not create disk shares for NFS exported file systems.

Follow these steps to use the `regconfig` registry editor to configure the ASU server to not create disk shares for NFS exported file systems. The backslash (\ ) at the end a line indicates continuation. Enter the entire command, then press the Enter key.

1. Disable the `ShareNFSExports` entry by entering the following command:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
AdvancedServer/FileServiceParameters \
ShareNFSExports REG_DWORD 0
```

2. Restart the ASU server by entering the following commands:

```
# net stop server
# net start server
```

4.2 Special Disk Shares

The ASU server automatically creates the special disk shares listed in Table 4–2. The list might differ depending on the installed ASU subsets. Do not remove or modify these shares.

Table 4–2: ASU Special 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$`	Directories and files located on the `root` (`/`) file system.

Table 4–2: ASU Special Disk Shares (cont.)

Name of Disk Share	Contains
`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 ASU server from a Microsoft client.
`DOSUTIL`	MS-DOS `clipcach` and `clispool`administrative commands.
`NETLOGON`	Logon scripts.
`PRINTLOG`	LP printer messages.
`USERS`	Users home directories. The default is the `/usr/users` directory.

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

\\*servername*\sharename$

4.3 Disk Share Attributes

A disk share is made up of mandatory and optional attributes.

Table 4–3 describes the mandatory disk share attributes for which you must provide values when you create a disk share.

Table 4–3: Mandatory Disk Share Attributes

Attribute	Description
Share name	A unique name of up to 80 alphanumeric characters that users use to connect to the share. A share name cannot be: COMM, PRINT, DEV, PIPE, QUEUES, SEM, MAILSLOT, SHAREMEM Append a dollar sign ($) to a share name to make it hidden when users browse the ASU server.
Path	The absolute path of a directory to be shared (including the drive, which is always `c:`). For example, the path to a directory called `project1`, which is a subdirectory of `market`, is `c:/market/project1`

Table 4–4 describes the optional attributes for which you can provide values when you create a disk share.

Table 4–4: Optional Disk Share Attributes

Attribute	Description
Users	The maximum number of users who can simultaneously access the share.
Remark	A comment about the share. Comments must be enclosed in quotation marks.

4.4 Creating a Disk Share

To create a disk share you can use:

- The `lmshare` command. Only the `lmshare` command allows you to configure on a per share basis the default Tru64 UNIX permissions for newly created files and directories in a share or whether or not the ASU server ignores Tru64 UNIX permission checking on a share. See Section 4.4.1 for more information.
- The `net share` command. See Section 4.4.2 for more information.
- The Server Manager. See Section 4.4.3 for more information.

4.4.1 Using the lmshare Command

The `lmshare` command prompts you for information about a share, including:

- The default Tru64 UNIX permissions in octal format for newly created files and directories in the share.
- Whether or not the ASU server ignores Tru64 UNIX permissions checking on the share.

See Section 4.5.3 for more information about Tru64 UNIX file and directory permissions.

To configure the ASU server to ignore Tru64 UNIX permission checking on a per share basis, the `IgnoreUnixPermissions` registry entry must be disabled, which it is by default.

If you enable the `IgnoreUnixPermissions` registry entry, the ASU server ignores Tru64 UNIX permission checking on all disk shares, regardless of the per share ignore Unix permissions setting on a share.

If you enable Tru64 UNIX quota checking, the Tru64 UNIX permissions are enforced regardless of the `IgnoreUnixPermission` registry entry settting, or the per share ignore Unix permissions settings.

Follow these steps to use the `regconfig` registry editor to disable the `IgnoreUnixPermissions` registry entry. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Disable the `IgnoreUnixPermissions` registry entry if it was enabled:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/FileServiceParameters \
   IgnoreUnixPermissions REG_DWORD 0
   ```

2. If you disabled the `IgnoreUnixPermissions` registry entry, restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

To create a share using the `lmshare` command, enter:

```
# lmshare -a
```

The `lmshare` command prompts you for the following information about the share. Press Enter for those fields that you do not want to change the value of.

```
Sharename? test1
Type (d|p|c|i)? [d] d
Local path? /home/test1
Remark? test1
Permissions(rwcxdaps)? [rwcxda]
Per share Unix file permissions? [0] 664
Per share Unix directory permissions? [0] 777
Per share ignore Unix permissions? [0]
Maximum users? [unlimited]
Password?
```

Existing shares and shares not created by the `lmshare` command will have a default value of zero (0) for the per share Unix file and directory permissions and will have Tru64 UNIX permissions checking enabled by default.

Newly created files in shares with a zero value for the per share Unix file permissions will get the Tru64 UNIX file permissions as defined by the value of the `UnixFilePerms` registry entry.

Newly created directories in shares with a zero value for the per share Unix directory permissions will get the TTru64 UNIX directory permissions as defined by the value of the `UnixDirectoryPerms` registry entry.

To display the current per share Unix file and directory permissions for a share, enter:

```
# lmshare -L share_name
```

To set the default Tru64 UNIX file permissions for newly created files in a share, enter:

```
# lmshare -F share_name file_permissions
```

where *share_name* is the name of the share, and *file_permissions* are the Tru64 UNIX file permissions in octal format.

To set the default Tru64 UNIX directory permissions for newly created directories in a share, enter:

```
# lmshare -D share_name directory_permissions
```

where *share_name* is the name of the share, and *directory_permissions* are the Tru64 UNIX directory permissions in octal format.

To disable Tru64 UNIX permissions checking on a share, enter the following command. Connected users must reconnect to the share for the new setting to take effect.

```
# lmshare -I share_name 1
```

To enable Tru64 UNIX permissions checking on a share, enter the following command. Connected users must reconnect to the share for the new setting to take effect.

```
# lmshare -I share_name 0
```

See `lmshare`(8) for more information.

4.4.2 Using the net share Command

You enter a `net` command in lowercase at the Tru64 UNIX command prompt on a system running the ASU server. Press the Enter key at the end of the entire command.

Table 4–5 shows the disk share attributes and the `net share` command option that you use to set the attribute.

Table 4–5: Setting Disk Share Attributes

Attribute	net share Option
Share name	Enter the name after the `net share` command
Path	Enter an equal sign (=) followed by the path after the share name
Users	`/users:#` or `/unlimited`
Remark	`/remark:"text"`

To create a disk share called project that corresponds to the `/usr/net/servers/lanman/project` directory, enter:

```
# net share project=c:/usr/net/servers/lanman/shares/project
```

To create a hidden disk share, append a dollar sign ($) to the share name. For example, to create a hidden share called project1 that corresponds to the `/usr/net/servers/lanman/project1` directory, enter:

```
# net share project1$=c:/usr/net/servers/lanman/shares/project1
```

Hidden shares do not display when users browse the ASU server.

Note to csh Shell Users

The dollar sign ($) is a special character when using the csh shell and therefore, you must precede the $ with a backslash escape character (\ ), for example:

```
# net share project1\$=c:/usr/net/servers/lanman/shares/project1
```

To view information about all shares, including hidden shares, enter:

```
# net share
```

To view information about a specific share, enter:

```
# net share share_name
```

4.4.3 Using the Server Manager

Follow these steps to create a disk share using the Server Manager:

1. Start the Server Manager (`srvmgr.exe`).

   Install the Server Manager GUI on the Windows system from which you will administer the ASU server. See Section 1.8 for information on installing the Server Manager GUI.

2. Choose Select Domain... from the Computer menu.

   The Select Domain dialog box is displayed.

3. In the Domain: field, enter the name of the domain in which you want to create the disk share and click on the OK button.

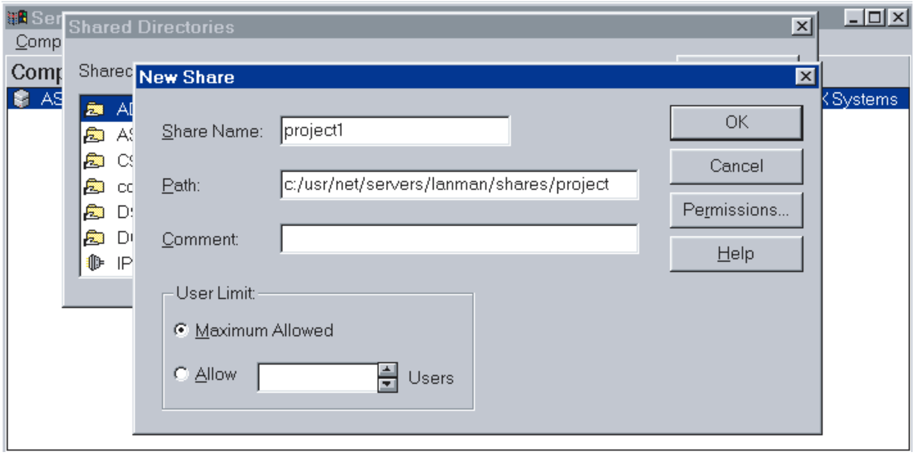
4. Choose Shared Directories... from the Computer menu.

   The Shared Directories dialog box is displayed.

5. Click on the New Share... button.

   The New Share dialog box is displayed.

6. Enter the disk share information as shown in the following figure:



Share Name: project1

Path: c:/usr/net/servers/lanman/shares/project

Comment:

● Maximum Allowed

○ Allow

ZK-1665U-AI

4.5 Disk Share Permissions

By default, a user must pass the following levels of security before they can access a file or directory in a disk share:

- Windows NT share level security
- Windows NT File System (NTFS) security
- Standard UNIX file and directory security

The following steps describe how permissions are checked when a user maps a drive to a disk share and requests access to a file in the disk share:

1. From a system running the Windows operating system software, a user connects to a disk share. By default, all users have permission to connect to a share. Access to directories and files in the share is normally controlled through NTFS permissions.

   The user's Windows system provides the ASU server with authentication information about the user, including the user's name, password, and security ID.

2. The ASU server checks the user's name and password in the user account database.

   If the ASU server authenticates the user's information, a unique ID is assigned to the user's Windows system. The Windows system must present this ID when the user makes subsequent requests to shares.

3. The user attempts to open a file in the share.

The ASU `lmx.srv` process services the user's request. Normally, the `lmx.srv` process runs as root, the highest Tru64 UNIX privilege level.

4. The `lmx.srv` process determines if the user has the correct Windows NT share permissions to access the share.

   If the permissions are not correct, the `lmx.srv` returns an access denied error to the Windows system.

5. The `lmx.srv` process determines if the user has the correct NTFS permissions to access the file in the share.

   If the permissions are not correct, the `lmx.srv` process returns an access denied error to the Windows system.

6. The `lmx.srv` process determines Tru64 UNIX access based on the mapping of the domain user account to a Tru64 UNIX user account.
7. The `lmx.srv` process changes its effective user ID from root to the ID of the corresponding Tru64 UNIX account and tries to open the file.
8. The Tru64 UNIX operating system determines if the user has the correct Tru64 UNIX permissions.

   If the permissions are correct, the file is opened. If the permissions are not correct, the `lmx.srv` process returns an access denied error to the Windows system.

4.5.1 Windows NT Permissions

The Windows NT permissions that you can set for disk share are:

- No Access, which prevents a user from accessing the disk share
- Read, which allows users to:
  - View file and subdirectory names
  - Move to subdirectories
  - View data in files
  - Run application files
- Change, which allows users to do everything Read allows, plus:
  - Add files and subdirectories
  - Change data in files
  - Delete subdirectories and files
- Full control, which allows users to do everything Read and Change allows, plus:
  - Change Windows NT and NTFS permissions

  - Set Windows NT and NTFS permission to take ownership of files and subdirectories

When a directory is shared, the default is to grant the Everyone domain user group Full Control permissions.

4.5.1.1 Setting Windows NT Permissions

To view and set Windows NT share permission you can use the:

- The `net perms` command
- Server Manager

4.5.1.1.1 Using the net perms Command

The syntax of the `net perms` command is:

```
# net perms \\sharename [/GRANT name:permissions | /CHANGE
name:permissions | /REVOKE name | /TAKE]
```

To display the Windows NT permissions for a disk share called project1, enter:

```
# net perms \\project1
```

To set the project1 Windows NT disk share permission to read for a user named peter, enter:

```
# net perms \\project1 /grant peter:read
```

4.5.1.1.2 Using the Server Manager Utility

Follow these steps to use the Server Manager utility to set Windows NT disk share permissions:

1. Start the Server Manager (`srvmgr.exe`).

   Install the Server Manager GUI on the Windows system from which you will administer the ASU server. See Section 1.8 for information on installing the Server Manager GUI.

2. In the Server Manager window, select a computer from the list and click Shared Directories on the Computer menu.

   The Shared Directories dialog box is displayed.

3. In the Shared Directories dialog box, select a share name and click Properties.

   The Shared Properties dialog box is displayed.

4. Click Permissions.

To change a permission, select a group or user account in the Name window, and then select a permission from the Type of Access list.

To add a group or user account to the list of those granted permissions for this shared directory, click Add, and then complete the Add Users and Groups dialog box that appears.

To remove a group or user account on the list of those granted permissions for this shared directory, select a group or user account in the Name window, and then click Remove.

4.5.2 Windows NTFS Permissions

When you create a disk share, an entry that associates a disk share with its corresponding Tru64 UNIX directory is created in the ASU share database. The Tru64 UNIX directory is created if it does not exist.

When a domain user requests access to the directory or a file in the directory, ASU checks its access control list (ACL) file to determine if the user has NTFS permission to access the file.

A file or directory in a disk share may or may not have its own ACL. For example, if you set explicit NTFS permissions on a file, an entry is added to the ACL listing that the file has its own ACL.

If you do not set explicit permissions for a file or directory, then the file or directory inherits the ACL entry from its parent directory. If the parent directory does not have an entry in the ACL, the ASU server checks higher-level directories until it finds one that does. For example, suppose you create a disk share called `projects` in the `/usr/net/servers/lanman/shares` directory. By default, the `projects` directory does not have its own ACL; it inherits the ACL from its parent directory (`/usr/net/servers/lanman/shares`). If the parent directory ACL grants the Everyone group Read permission to subdirectories and files, then the same ACL applies to the `projects` subdirectory.

If you set NTFS permission on the `projects` subdirectory to Change for the Everyone group, then an ACL is created for the `projects` directory and the Everyone group has the following permissions:

- Read permission for the `/usr/net/servers/lanman/shares` directory
- Change permission for the `/usr/net/servers/lanman/shares/projects` directory

The exception to the inherited ACL policy is the default home directory for users. By default, when you create a domain user account, a subdirectory with the same name is created in the `/usr/users` directory with an ACL that identifies the new user as the owner of the subdirectory and grants them all the NTFS permissions to the subdirectory and its contents. For example, if you create a domain user account named peter, a subdirectory named `peter` is created in the `/usr/users` directory (`/usr/users/peter`) and the peter user account is granted all NTFS permissions to the directory. The creation of an ACL for a user's home directory is a feature that makes sharing a user's directory easier.

There is a standard set of NTFS permissions that you can set or you can customize NTFS permissions to meet you needs. Table 4–6 describes the standard Windows NTFS permissions that you can set. Table 4–7 describes the custom Windows NTFS permissions that you can set.

Table 4–6: NTFS Standard Permissions

Permission	For File	For Directory
Add	Cannot read the contents of current files, change them, or list the files	Can add files to the directory
AddRead	Can read and execute files but cannot change files	Can read, write, and execute files in the directory
Change	Can change the contents of current files	Can read and add files
Full control	Can read and change files, add new ones, change permissions for files, and take ownership of file	Change permissions for the directory and take ownership of the directory
NoAccess	Not applicable	Cannot access the directory in any way, even if the user is a member of a group that has been granted access to the directory
List	Cannot access files	List the files and subdirectories in this directory and change to a subdirectory of this directory
Read	Can read the contents of files and run applications	Allows viewing the names of files and subdirectories

Table 4–7: NTFS Custom Permissions

Permission	For File	For Directory
Change Permissions (P)	Allows changing the file's permissions	Allows changing the directory's permissions
Delete (D)	Allows deleting the file	Allows deleting the directory

Table 4–7: NTFS Custom Permissions (cont.)

Permission	For File	For Directory
Execute (X)	Allows running the file if it is a program	Allows changing to subdirectories
Read (R)	Allows viewing the file's data	Allows viewing the names of files and subdirectories
Take Ownership (O)	Allows taking ownership of the file	Allows taking ownership of the directory
Write (W)	Allows changing the file's data	Allows adding files and subdirectories

When you set NTFS permissions, two sets of individual permissions are displayed: the permissions set on the directory and the permissions set on files in the directory. For example, the following output would display if you set AddRead permission on a share for a user name peter. The (RWX), signifying Read, Write, and Execute permissions on the share, and (RX), signifying Read and Execute permission on its files.

```
Resource:    c:\usr\net\servers\lanman\shares\share1
Owner:       server1.dom\Administrators
Name:                              Permissions:
-------------------------------------------------------------------------------
*Administrators                    FullControl(All)(All)
*Everyone                          Read(RX)(RX)
peter                              AddRead(RWX)(RX)
```

When ASU server displays resource permissions, it designates groups with an asterisk (*)

NTFS Permissions on files in a directory can be set to NotSpecified. This means that by default no permissions will be set for that user or group to the files that are present in the directory or that are created after setting this permission. A group or user cannot use files in the directory unless access is granted by another method such as setting permissions that grant access on individual files.

When you are setting permissions on a directory, you can use the CREATOR OWNER special group to allow users to control only the subdirectories and files that they create within the directory. Permissions set on CREATOR OWNER are transferred to the user who creates a directory or file within the directory. To change permissions on the directory, you must be the owner of the directory or have been granted permission to do so by the owner.

Note

By default, Windows NTFS permissions grant read and execute permission to the Everyone group, of which every domain user account is a member. You must grant Windows NTFS write permission to the domain user or group account that will write files to the disk share.

4.5.2.1 Controlling ASU and ACLs

How the ASU server creates and uses ACLs depends on the values assigned to the ACL-related entries in the `FileServiceParameters` registry subkey. Table 4–8 describes ACL-related registry value entries.

Table 4–8: ACL Value Entries

Entry	Description and Default Value
`AclCacheSize`	Specifies the number of entries in ACL cache, which tracks the results of recent access checks performed on ASU resources. Default: 6
`ForceDirectoryAcl`	Determines whether or not the ASU server creates an access control list for a newly created directory if the client computer does not provide an explicit ACL. If an ACL is not created, one is inherited from its parent directory. Default: 1 (create new ACL)
`ForceFileAcl`	Determines whether or not the ASU server creates an access control list for a new file if the client computer did not provide an explicit access control list. If an access control list is not created, one is inherited from its parent directory. Default: 0 (will not create new ACL)
`HomeDirectoryAccess`	Specifies whether or not to add a full access (`RWXDPO`) control entry for the user on the user's Tru64 UNIX home directory when you create a domain user account. Default: 1 (add access control entry for user)
`SyncAclFileOnWrite`	Determines whether or not changes to the ACL are forced to disk using an `fsync`(2) system call when the ACL is updated. Default: 0 (ACL changes are not forced)
`UnixAclSupport`	Allows the ASU server to use Tru64 ACLs in addition to NTFS user and group permissions. This entry is supported only on systems running the Tru64 UNIX Version 5.0A and higher software. Default: 0 (do not use Tru64 UNIX ACLs)

Table 4–9 describes ASU ACL related commands.

Table 4–9: ASU ACL Commands

Command	Purpose
`/usr/sbin/acladm`	Create, check, manage, move, remove, and trim the ACL database.
`/usr/sbin/acldump`	Dump the ACL database to an ASCII file.
`/usr/sbin/chacl`	Change ACL information on objects.
`/usr/sbin/aclload`	Load the ACL database from an ASCII file.
`/usr/sbin/lsacl`	Display ACLs placed on objects (files and directories).
`/usr/sbin/rmacl`	Removes ACLs on objects.

See `acladm`(8) for more information on the `acladm` command.

4.5.2.2 Restoring ASU ACLs

You can restore ASU ACLs from a backup copy of an ACL store. You do not need to stop the ASU server to restore ASU ACLs from backup. Follow these steps to restore a file and its corresponding ASU ACLs:

1. Restore the file from backup.
2. Restore the ACL store file (`/usr/net/servers/lanman/datafiles/acl`) from the same date as the backed up file to a different filename, for example `may10.acl`.
3. Enter the following command to restore the ASU ACLs:

   ```
   # acladm -M -i ACL_store_file -v /path/filename
   ```

   For example, to restore the ASU ACLs in the `may10.acl` file for the `/usr/temp` file, enter:

   ```
   # acladm -M -i may10.acl -v /usr/temp
   ```

4.5.2.3 Setting Windows NTFS Permissions

You set Windows NTFS permissions by using either:

- The `net perms` command
- The Windows Explorer GUI

4.5.2.3.1 Using the net perms Command

The syntax of the `net perms` command to set Windows NTFS permissions is as follows.

```
# net perms c:/path [/GRANT name:permissions | /CHANGE
name:permissions | /REVOKE name | /TAKE]
```

To display the Windows NTFS permissions for a file or directory called `project1`, enter:

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

To grant the group called project1 the Windows NTFS write permission to a file or directory called `project`, enter:

```
# net perms c:/usr/net/servers/lanman/shares/project
/grant project1:w
```

4.5.2.3.2 Using the Windows Explorer GUI

Follow these steps to allow the project1 group the Windows NTFS write permission:

1. Start the Server Manager (`srvmgr.exe`).

   Install the Server Manager GUI on the Windows system from which you will administer the ASU server. See Section 1.8 for information on installing the Server Manager GUI.
2. Start the Windows Explorer (`explorer.exe`).
3. Connect to the disk share (if necessary) and display its properties.

   The Properties window is displayed for the disk share.
4. Click on the Security tab, then click Permissions.

   The Directory Permissions window is displayed.

   To change a permission, select a group or user account in the Name window, and then select either the Special Directory Access or Special File Access permission from the Type of Access list. A Special Directory or File Access dialog box is displayed from which you select Windows NTFS permissions.

   To add a group or user account to the list of those granted permissions for this shared directory, click Add and complete the Add Users and Groups dialog box that appears.

   To remove a group or user account from the list of those granted permissions for this shared directory, select a group or user account in the Name window, and then click Remove.

4.5.3 Setting Tru64 UNIX Permissions

By default, subdirectories created in a disk share have the following Tru64 UNIX permissions:

- Owner has read and write permission
- Group has read permission

- Other has read permission

By default, files created in a disk share have the following Tru64 UNIX permissions:

- Owner has read and write permission
- Group has read permission
- Other has read permission

When you use the `lmshare` command to create a share, you can set the default Tru64 UNIX permissions in octal format for newly created files and directories in the share. The `lmshare` command prompts you for the per share Tru64 UNIX file and directory permissions.

You can selectively change the file and directory permissions in a share by using the following commands:

- The `lmshare` command to change the default permissions assigned to new files and directories that you create. The default permissions set by the `lmshare` command override the overall system default file and directory permissions.
- The `chmod` command to change the current permissions on an existing file or directory. For example, to allow the owner's group the write permission to a file, enter:

  ```
  # chmod g+w filename
  ```

See `lmshare`(8) and `chmod`(8) for more information on these commands.

You can permanently change the default permissions for new files and directories created in all shares by changing the value of the registry value entries described in Table 4–10. Permanently changing the default permissions overrides the overall system default file and directory permissions.

Table 4–10: Disk Share Permission Value Entries

Entry	Description and Default Value
`UnixDirectoryPerms`	Specifies the default Tru64 UNIX system permissions for newly created directories. Default: 0755 octal (493 decimal), which translates to `-rwxr-xr-x` Set the value to 0 (zero) to specify that directories created in ASU shares inherit the Tru64 UNIX permissions from the parent directory.
`UnixFilePerms`	Specifies the default Tru64 UNIX system permissions for newly created files. Default: 0644 octal (420 decimal), which translates to `-rw-r--r--` Set the value to 0 (zero) to specify that files created in ASU shares inherit the Tru64 UNIX permissions from the parent directory.

The registry editor uses decimal format to display the values of the `UnixDirectoryPerms` and `UnixFilePerms` entries. The Tru64 UNIX software uses octal format to specify directory and file permissions.

Changing the value of the `UnixFilePerms` and `UnixDirectoryPerms` registry entries will take effect when you restart the ASU server and only applies to newly created files and directories. Existing and renamed files and directories will retain their original Tru64 UNIX permissions. The `UnixDirectoryCheck` registry entry, which can be set to bypass Tru64 UNIX security checking, will not effect the inheritence of permission.

Follow these steps to use the `regconfig` registry editor to allow Tru64 UNIX permissions to be inherited from the parent directory. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Change the value of the `UnixFilePerms` entry by entering the following command:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/FileServiceParameters \
   UnixFilePerms REG_DWORD 0
   ```

2. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

4.5.3.1 Tru64 UNIX Groups or DOS Groups

By default, files created in a directory by a Tru64 UNIX user are owned by that user and the group ownership is listed as the user's default group.

Files created by domain users in a disk share are owned by the user's corresponding Tru64 UNIX account, and the Tru64 UNIX group ownership is listed as one of the ASU groups beginning with `DOS-`.

By default, the ASU server uses the `DOS-` groups to maintain DOS attributes for a file. For example, if the group ownership of a file is `DOS-ash`, the DOS attributes (archive, system, and hidden) are set. The fourth attribute, ReadOnly, is maintained by setting or clearing the Tru64 UNIX write permission.

You can configure the ASU server to use Tru64 UNIX groups instead of using the `DOS-` groups. However, users cannot set the archive, system, or hidden attributes on any file shared on the ASU server. User will only be able to set the ReadOnly attribute.

Follow these steps to use the `regconfig` registry editor to configure the ASU server to use Tru64 UNIX groups instead of DOS groups. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Enable the `UseUnixGroups` entry by entering the following command:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
AdvancedServer/FileServiceParameters \
UseUnixGroups REG_DWORD 1
```

2. Restart the ASU server by entering the following commands:

```
# net stop server
```

```
# net start server
```

4.5.3.2 Configuring the ASU Server to Not Check Tru64 UNIX Permissions

The ASU server must check Windows NT and Windows NTFS permissions; however you can configure the ASU server to not check Tru64 UNIX permissions.

Follow these steps to use the `regconfig` registry editor to configure the ASU server to not check Tru64 UNIX permissions. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Enable the `IgnoreUnixPermissions` entry by entering the following command:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
AdvancedServer/FileServiceParameters \
IgnoreUnixPermissions REG_DWORD 1
```

2. Restart the ASU server by entering the following commands:

```
# net stop server
# net start server
```

4.6 Creating Personal Disk Shares for Users

By default, when you create a domain user account, the ASU server creates a subdirectory for the user in the `/usr/users` directory using the user's Tru64 UNIX account name and grants the user all Windows NT share, Windows NTFS, and Tru64 UNIX access permissions to their subdirectory.

By default, the `/usr/users` directory is associated to the `USERS` special disk share, which means that you do not need to create individual disk shares for each user because there is automatically a subdirectory for each user in the `USERS` disk share.

Users connect to the `\\`*`server`*`\users` disk share from their Windows system and browse to their directory. Users can view other users' directories, but have permission to access only their own directory.

If you use a Tru64 UNIX directory other than `/usr/users` for the users' home directories, you should redirect the `USERS` disk share to the new location. To redirect a share you must delete the share and recreate it.

Optionally, you can configure the ASU server to automatically:

- Create a personal disk share when you create a Tru64 UNIX user account or map a Tru64 UNIX user account to a domain user account.
- Delete a personal disk share when you delete its associated domain user account.
- Rename a personal disk share when you rename it associated domain user account.

The ASU server creates a personal disk share as a hidden disk share mapped to the user's UNIX home directory. The ASU server will not create a personal disk share if the UNIX home directory does not exist or if there is an existing disk share with the same name. A hidden disk share has a name that ends with a dollar sign ($) and does not display when browsing the ASU server. For example, creating a Tru64 UNIX user account named `peter` will automatically create a personal disk share called `peter$` mapped to peter's home directory. A user can connect to a hidden disk share by appending the dollar sign to the share name.

Follow these steps to use the `regconfig` registry editor to configure the ASU server to create, delete, and rename personal disk shares. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Ensure that the `CreateUnixUser` entry is enabled, which it is by default.

   See Section 2.2 for information on displaying registry entry values.

2. Enable the `CreatePersonalShare` entry by entering the following command:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/UserServiceParameters \
   CreatePersonalShare REG_DWORD 1
   ```

3. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

4.7 Creating a Disk Share for a Remote File System

On a Tru64 UNIX system that is running the ASU server, you can create a disk share for directories that are NFS-exported by systems other than Tru64 UNIX. To do so, you must:

- Ensure that all UNIX systems are running the NFS service with the `lock` option
- Ensure that the ASU `UseNfsLocks` registry entry is enabled
- Ensure that the remote UNIX system is exporting the directory
- Mount the remote directory on the Tru64 UNIX system on which the ASU server is running
- Create the disk share with a path to the mounted remote directory
- Optionally, you can set LanManager-only security. With LanManager-only security, ASU users are not restricted from accessing files and directories because of Tru64 UNIX permissions.

4.7.1 Running the NFS Service with the Lock Option

On most UNIX systems, you can enter the following command to determine if the NFS service is running:

```
# ps -ef | grep nfs
```

Information similar to the following is displayed if the NFS service is running:

```
Root 297 1 0.0 May 01 ??  0:00.01 /usr/sbin/nfsiod 7
```

Enter the following command to determine if NFS locking is enabled on a UNIX system:

```
# ps -ef | grep lockd
```

Information similar to the following is displayed if locking is enabled:

```
Root 7417 1 0.1 08:33:57 ??  0:00.08 /usr/sbin/rpc.lockd
```

4.7.2 Enabling the UseNfsLocks Entry

The `UseNfsLocks` entry specifies whether or not the ASU server tries to set Tru64 UNIX system record locks in files as requested by clients.

When this value entry is enabled, make sure that the `rpc.lockd` and `rpc.statd` daemons are running on the NFS server or on the Tru64 UNIX system on which the ASU server is running. If these daemons are not running, the ASU server might stall or data might be lost.

By default, the `UseNfsLocks` entry is enabled.

To check the value of the `UseNfsLocks` entry, enter:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
 AdvancedServer/FileServiceParameters UseNfsLocks
```

4.7.3 Exporting File Systems

Ensure that the UNIX system is exporting the file system.

To verify whether or not a file system is exported, enter:

```
# /sbin/mount
```

A list of exported file systems is displayed. Follow these steps if the file system is not displayed:

1. Edit the `/etc/exports` file to add the entry.
2. Close the `/etc/exports` file.
3. Enter the following command:

   ```
   # exportfs
   ```

4.7.4 Mounting Remote Directories

To mount remote directories on a Tru64 UNIX system, use the following syntax to include an entry for each remote directory in the `/etc/fstab` file:

```
file-spec mnt-point fs-type mnt-options backup fsck
```

In this syntax statement:

The *`file-spec`* variable is the full pathname to the remote directory.

The *`mnt-point`* variable is the mount point for the remote directory.

The *`fs-type`* variable is the type of file system, which is `nfs` for the purpose of this service.

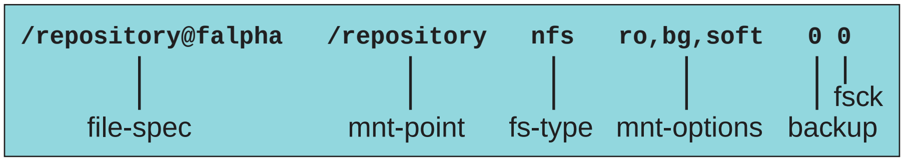
The *`mnt-options`* variable is a list of options (separated with commas) associated with the directory, such as the:

- Type of access to the resource, for example the `ro` (Read Only) or `rw` (Read-Write) options.
- Action to take if the directory fails to mount on the first attempt, for example the `bg` option, which retries the mount in the background.
- Behavior that client systems experience if the NFS server hosting the remote directory to which the client system is connected becomes unavailable. The `hard` option, which is the default, stalls a client system and displays an hourglass. The `soft` option pauses the client system and generates an error message.

The `backup` option is used by the `dump` command to determine which file systems to back up. This is not applicable to NFS. Set this option to zero (0).

The `fsck` option is used by the `fsck` command to determine the order in which to check file systems at reboot time. This is not applicable to NFS. Set this option to zero (0).

The following is a sample entry in the `/etc/fstab` file:



```
/repository@falpha   /repository   nfs   ro,bg,soft   0 0
```

ZK-1656U-AI

If necessary, create and then mount the remote directory by using the `mount` command or the `automount` utility.

The `mount` command mounts the directory in the `/etc/fstab` file that you specify. For example:

```
# mount /repository
```

The `automount` utility mounts all the entries in the `/etc/fstab` file. You start the `automount` utility from the command line or by running the `nfssetup` utility and answering yes when prompted to run the `automount` daemon.

4.7.5 Enabling LanManager Only Security for NFS Shares

The ASU server now allows for LanManager-only security for NFS shares. With LanManager-only security, ASU users are not restricted from accessing files and directories because of Tru64 UNIX permissions. Files and directories created by an ASU user appear as if they were created by a Tru64 UNIX user.

To enable LanManager-only security:

1. Export the NFS file system (usually in the `/etc/exports` file) with the following entry:

   ```
   /nfs -root=0
   ```

2. Set the value for the ASU registry entries as described in the following table:

Registry Entry	Value
`IgnoreUnixPermissions`	1
`UnixDirectoryCheck`	2
`UseUnixGroups`	1
`UseUnixLocks`	1

   For example, to use the `regconfig` registry editor to enable the `IgnoreUnixPermissions` entry, enter the following command. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/FileServiceParameters \
   IgnoreUnixPermissions REG_DWORD 1
   ```

3. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

4.8 Deleting a Disk Share

When you delete a disk share, only the association of the share name to the Tru64 UNIX directory is deleted; the associated Tru64 UNIX directory and its contents are not deleted. To delete a disk share you can use either:

- The `net share` command

- The Server Manager

4.8.1 Using the net share Command

You enter a `net` command in lowercase at the Tru64 UNIX command prompt on a system running the ASU software. Press the Enter key at the end of the entire command.

To delete a disk share, enter:

```
# net share sharename /delete
```

For example, to delete a disk share called project, enter:

```
# net share project /delete
```

4.8.2 Using the Server Manager

Follow these steps to delete a disk share using the Server Manager:

1. Start the Server Manager GUI (`srvmgr.exe`).

   Install the Server Manager GUI on the Windows system from which you will administer ASU. See Section 1.8 for information on installing the Server Manager GUI.
2. Choose Select Domain... from the Computer menu.

   The Select Domain dialog box is displayed.
3. In the Domain: field, enter the name of the domain in which you want to create the group and click on the OK button.
4. Choose Shared Directories... from the Computer menu.

   The Shared Directories dialog box is displayed.
5. Click on the name of the share that you want to delete.
6. Click on the Stop Sharing button.

5

Creating ASU Printer Shares

This chapter describes how to use the ASU server to share Tru64 UNIX printers with domain users.

5.1 Before Creating a Printer Share

Before you create a printer share:

- The printer must have an entry in the `/etc/printcap` file.

  If there is no entry for the printer in the `/etc/printcap` file, then use the `lprsetup` utility to set up the printer. The `lprsetup` utility prompts you for information about the printer, creates a spool directory, links the output filter, and adds an entry for the printer in the `/etc/printcap` file.

  Do not delete the `lmxnone` and `lmxnull` entries from the `/etc/printcap` file or the associated spool directories. These entries and directories were created if the `/etc/printcap` file did not exist and you entered the `net device` command.
- The printer for which you want to create a print share must be working.

5.2 Printer Share Attributes

A printer share is made up of mandatory and optional attributes.

Table 5–1 describes the print share attributes for which you must provide a value.

Table 5–1: Mandatory Print Share Attributes

Attribute	Description
Share name	A unique name of up to 12 alphanumeric characters that users use to connect to the printer share. A share name cannot be: COMM, PRINT, DEV, PIPE, QUEUES, SEM, MAILSLOT, SHAREMEM Append a dollar sign ($) to a share name to make it hidden when users browse the ASU server.
Device name	The name by which the Tru64 UNIX operating system software recognizes the printer.

Table 5–2 describes the print share attributes for which you can provide a value.

Table 5–2: Optional Print Share Attributes

Attribute	Description
Users	The maximum number of users who can simultaneously access the share.
Remark	A comment about the share. Comments must be enclosed in quotation marks.

5.3 Configuring Print Jobs

Table 5–3 describes the registry value entries in the `SYSTEM/CurrentControlSet/Services/AdvancedServer/Parameters` registry path that define the maximum number of print jobs and length of print job names.

Table 5–3: Print Job Value Entries

Entry	Specifies/Default
`MaxPrintJobs`	The maximum number of print jobs allowed in any class queue created by the ASU server. Default: 1000 print jobs
`MaxPrintJobName`	The maximum number of characters for a print job name. Characters that exceed the value of the `MaxPrintJobName` entry are truncated. Default: 0 characters (do not truncate print job names)

You use a registry editor to change the values of these keys. For example, follow these steps to use the `regconfig` registry editor to set the maximum number of print job names to 8 characters. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Enter the new value for the `MaxPrintJobName` entry by entering the following command:

```
# regconfig SYSTEM/CurrentControlSet/Services/\
AdvancedServer/Parameters MaxPrintJobName REG_DWORD 8
```

2. Restart the ASU server by entering the following commands:

```
# net stop server
```

```
# net start server
```

5.4 Creating Printer Shares

To create a printer share you can use either:

- The `net share` command with the `/print` option
- The Windows Printer Wizard

5.4.1 Using the net share Command

You enter a `net` command in lowercase at the Tru64 UNIX command prompt on a system running the ASU server. Press the Enter key at the end of the entire command.

Table 5–4 shows the `net share` command options that you use to set attributes for printer shares.

Table 5–4: Setting Printer Share Attributes

Attribute	net share Option
Share name	Enter the name after the `net share` command
Device name	Enter the Tru64 UNIX name of the printer after the share name
Users	`/users:#` or `/unlimited`
Remark	`/remark:"text"`

To create a printer share called `win_printer` that is associated to a Tru64 UNIX printer called `laserwriter`, enter:

```
# net share win_printer=laserwriter /print
```

To view information about the `win_printer` print share, enter:

```
# net share win_printer
```

5.4.2 Using the Windows Printer Wizard

Follow these steps to create a print share using the Windows Printer Wizard:

1. Log in to the system running the Windows software using an account with administrative privileges.
2. Browse the Network Neighborhood or use the Run or Find option from the Start button to locate and double click on the ASU server on which you want to create the printer share.

   A window is displayed listing the disk shares and a Printers folder.
3. Double click on the Printers folder.
4. Click on the Add Printer icon and follow the instructions on the screen.

5.5 Deleting Printer Shares

Do not use the Tru64 UNIX `lprsetup` command or edit the `/etc/printcap` file to delete an ASU printer share. To delete a printer share, use the `clsetup` command, or enter:

```
# net share sharename /delete
```

See `clsetup`(8) for more information on the `clsetup` command.

5.6 Installing Alternate Printer Drivers

You can install alternate print drivers for a printer share so users of various Windows based systems (Alpha, PowerPC, MIPS, or x86) can automatically download the driver that they need when adding the printer share. For example, when a Windows 95 user adds to their system a printer that points to an ASU print share, the Windows 95 Printer Wizard connects to the ASU server and searches for a x86-based driver for that printer. If a driver is found, the Printer Wizard copies the driver to the Windows 95 system. If a driver is not found, the Printer Wizard requires that user provide it.

Follow these steps to install alternate print drivers for a printer share:

1. Install the printer locally on a Windows NT system.
2. Display the Properties dialog box for the printer share.
3. Click on the Sharing tab.
4. Choose to share the printer and select the alternate drivers that you want to install.
5. Click on the OK button.

5.7 Setting Printer Share Permissions

Permissions for a print share can be No Access, Print, Manage Documents, and Full Control.

Although permissions are cumulative, the No Access permission overrides all other permissions. By default, the Full Control permission is assigned to each domain user account.

To change permissions on a print share, you must be the owner of the printer. You can change print share permissions by using either:

- The `net perms` command
- The Windows Printer Properties GUI

5.7.1 Using the net perms Command

Enter a `net` command in lowercase at the Tru64 UNIX command prompt on a system running the ASU server. Press the Enter key at the end of the entire command.

To prohibit a user named peter from using a printer share called win_printer, enter:

```
# net perms \\win_printer /grant peter:noaccess
```

To view permissions about the win_printer printer share, enter:

```
# net perms \\win_printer
```

5.7.2 Using the Windows Printer Properties GUI

Follow these steps to set printer share permissions:

1. Select the printer share by clicking on the start button, selecting the Settings option, then the Printers folder.

   A window is displayed that shows the installed printers.
2. Click on the name of the print share in the Printers window.
3. Choose Properties from the File menu.

   The Properties dialog box for the printer is displayed.
4. Click on the Security tab then click on the Permissions button.

   The Printer Permissions dialog is box displayed.
5. If the user or group name for which you want to set permissions is not displayed, then click on the Add button to add it to the list. Choose the type of access for the user or group and click on the OK button.

5.8 Viewing the Status of ASU Print Jobs

On systems running the Tru64 UNIX Version 5.0 and higher operating system software, you can use the Tru64 UNIX SysMan Event Viewer to view status information about print jobs sent to the ASU server.

The ASU server uses parts of the `lpd` daemon. As a result, ASU printing events will appear in the SysMan Event Viewer as normal Tru64 UNIX printing events.

See *System Administration* for more information on the SysMan Event Viewer.

5.9 Configuring Client Printers as ASU Printer Shares

You can create an ASU printer share for a printer attached to a PC running the MS-DOS operating system software. You cannot create a printer share for a printer attached to a PC running Windows software.

You use the `asuclient` command to create a special disk share for a printer attached to a PC. The disk share stores print jobs that are sent to the printer. The PC connects to the disk share and retrieves the files to print. To configure a printer that is attached to a PC as an ASU printer share, you must configure the ASU server and the PC as described in the following sections.

5.9.1 Configuring the ASU Server

To configure the ASU server to recognize the printer attached to a PC, you must:

1. Enter the `lprsetup` command.
2. When the `lprsetup` utility prompts you for the printer type, enter `clientps` if the printer is a PostScript printer or `clienttxt` if the printer is a text printer.
3. When the `lprsetup` utility prompts you for the spooler directory and error log file, enter a path and replace `CLIENTNAME` with the name of the PC to which the printer is attached.

   The `lprsetup` utility creates a print queue for it on the Tru64 UNIX system.
4. Use the `net share` command to create a printer share for the printer. For example, to create a printer share called `win_printer` for a printer called `laser`, enter:

   ```
   # net share win_printer=laser /print
   ```

5. Enter the `asuclient printername -a` command to create the disk share for the printer. For example, to create a disk share for a printer called `laser`, enter:

   ```
   # asuclient laser -a
   ```

5.9.2 Configuring the PC

To configure the PC you must:

1. Load the spooler agent software that is provided with the ASU software onto the PC to which the printer is attached. The spooler agent software is a terminate-and-stay-resident (TSR) program that receives print jobs from the ASU server and sends them to MS-DOS TSRs for printing.
2. Configure a persistent connection on the PC. This connection establishes a link to the ASU server and copies print jobs for the attached printer from the special file share.

These tasks are described in the next sections.

5.9.2.1 Loading Spooler Agent Software

The way you load the spooler agent software onto the PC depends on whether you are attaching a text printer or a PostScript printer, as described in the following sections:

5.9.2.1.1 Attaching a Text Printer

At the MS-DOS prompt on the PC to which the text printer is attached:

1. Edit the `autoexec.bat` file and add the following entries after the `call \directory\STARTNET.BAT` entry:

   ```
   print /d:portid:
   use driveid: \\unix_server_name\DOSUTIL
   driveid:\clispool /i /s:driveid
   ```

   The *`portid`* variable is the ID of the client's printer port. For example, LPT1 or COM1.

   The *`driveid`* variable indicates the drive where you want to install the spooler agent software.
2. Reboot the PC.

5.9.2.1.2 Attaching a PostScript Printer

At the MS-DOS prompt on the PC to which the PostScript printer is attached:

1. Edit the `autoexec.bat` file and add the following entries after the `call \transport\STARTNET.BAT` entry (*transport* is either TCP/IP or DECnet):

   ```
   c:\pcache\pcache.com
   c:\pcache\print /d:portid:
   use driveid: \\unix_server_name\DOSUTIL
   driveid:\clipcach /i /s:driveid
   ```

   The *portid* variable is the ID of the client's printer port. For example, LPT1 or COM1.

   The *driveid* variable indicates the drive where you want to install the spooler agent software.

2. Reboot the PC.

5.9.2.2 Configuring a Persistent Connection

If, on the ASU server, the `AutoDisconnect` registry value entry is disabled, which it is by default, and you followed the steps in Section 5.9.2.1, then nothing more is needed to create a persistent connection.

If, on the ASU server, the `AutoDisconnect` registry value entry is enabled, you need to disable it.

Follow these steps to use the `regconfig` registry editor to disable the `AutoDisconnect` registry value entry. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Disable the `AutoDisconnect` entry by entering the following command:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   LanmanServer/Parameters \
   AutoDisconnect REG_DWORD 0
   ```

2. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

6

Configuring ASU in a TruCluster Environment

You can configure ASU disk shares, print shares, and services to be highly available by configuring two or more ASU servers in a TruCluster environment. A TruCluster environment is a grouping of AlphaServer systems running the TruCluster software. See *Cluster Administration* for more information on the TruCluster software.

This chapter describes how to configure the ASU server in a TruCluster Server Version 5.x or higher environment.

See Appendix F for information on how to configure the ASU server in a TruCluster Version 1.x (Available Server Environment (ASE)) environment.

6.1 ASU Server Modes in a TruCluster Server Version 5.x Environment

You can configure the ASU server to operate in one of the following modes in a TruCluster Server Version 5.x environment:

- Multi

  Configuring 1 or more cluster members in multi mode provides the highest ASU server availability.

  In multi mode, the ASU server runs on each cluster member and appears to clients as a single ASU server. For example, ASU servers configured in multi mode on six cluster members can access all ASU resources and have a single role of either primary domain controller (PDC), backup domain controller (BDC), or member server.

  ASU servers configured in mutli mode use a **cluster alias**, which is a name known by each ASU server. Users should specify the cluster alias instead of an ASU server when connecting to shares. When users specify the cluster alias, one of the ASU servers responds. Client connections using TCP/IP are distributed among the ASU servers. Client connections using the NetBEUI transport protocol go to a single cluster member.

  If an ASU server configured in multi mode stops, user connections to that ASU server are disconnected. Most clients that connected using the cluster alias will automatically reconnect to an active ASU server. If users must manually reconnect, they should again specify the cluster alias, which will connect them to an active ASU server.

Multi mode is the default mode. See Section 6.1.1 for more information on configuring the ASU server in multi mode.

- Single, also called cluster application availability (CAA)

  Configuring 2 or more cluster members in single mode provides high ASU server availability.

  In single mode you configure the ASU server on 2 or more cluster members, but run the ASU server on only one cluster member.

  If the ASU server configured in single mode stops, user connections are disconnected and the TruCluster software automatically restarts the ASU server on an alternate cluster member that is configured to run the ASU server in single mode. The alternate ASU server assumes the identity and responsibility of the stopped ASU server. Most clients will automatically reconnect to the alternate ASU server. If users must manually reconnect, they should again specify the same ASU server name, which will connect them to the alternate ASU server.

  Configuring ASU servers in single mode provides similar functionality to that provided by the TruCluster Version 1.x (ASE) software.

  See Section 6.1.2 for more information on configuring the ASU server in single mode.

- None

  Configuring ASU servers in none mode does not provide high ASU server availability. You configure the ASU server in none mode if you are running the TruCluster software on a system and do not want the ASU server to use the TruCluster software.

  In none mode you configure the ASU server to run on only one cluster member. If that cluster member fails, the ASU server does not restart on another cluster member.

  See Section 6.1.3 for more information on configuring the ASU server in none mode.

6.1.1 Configuring the ASU Server in Multi Mode

You must run the `asusetup` utility on a cluster member. The `asusetup` utility prompts you for ASU server network and general information that is described in Section 1.4 and for the following TruCluster information:

- The mode (multi, single, or none) in which the ASU server will operate in the TruCluster environment
- The cluster alias

To run the `asusetup` utility, enter:

`#` **`/usr/sbin/asusetup`**

Example 6–1 displays sample `asusetup` output for an ASU server configured to operate in multi mode.

Example 6–1: Sample Multi Mode asusetup Output

```
       Advanced Server for UNIX Configuration Utility

Administrators can configure the Advanced Server software by using the
default configuration values that are detected from a previous Advanced
Server configuration.  If no previous Advanced Server configuration is
detected then the default values are determined by this utility. In
either case, administrators can choose not to use the default values and
customize the Advanced Server configuration by interactively supplying
Advanced Server configuration values.

The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’ics0’)
                NetBEUI (controller ’ics0’)
   Cluster Alias: colors
   Cluster Type:  multi
   Server Name:   red
   Domain Name:   red.dom
   Domain Role:   Primary
   WAN Support:   enabledns=yes, uselmhosts=yes

Do you want to use this default information [y/n]? n

The following network configuration is based on the previous
network configuration, with default values for new items:

   Controllers:  TCP/IP  = ics0
                 NetBEUI = ics0

   Use DNS:                yes
   Sub Domains:            company.com
   Use lmhosts:            yes
   lmhosts file:           /usr/net/servers/lanman/datafiles/lmhosts
   Use NBNS:               no
   Primary NBNS address:
   Secondary NBNS address:

Would you like to use this network information [y/n]? n

You will now be prompted to enter configuration information
for the Advanced Server for UNIX server including
which network transports and controllers to use and how
to resolve names in a wide area network.

 **********************************************************
         NetBIOS over TCP/IP Setup
 **********************************************************

 Select a controller for NetBIOS over TCP/IP.
 The "transports.ini" file will be modified accordingly.

  ics0 @ address:  10.0.0.2
  tu0 @ address:   10.0.0.3
```

Example 6–1: Sample Multi Mode asusetup Output (cont.)

```
 none

Enter the controllers separated by a comma
or type ? for help: [ ics0 ]  tu0

You have entered:
 tu0

Are you satisfied with these controllers? [yes]?

Modifying the "transports.ini" file with tu0.

**********************************************************
                  WAN Name Services
**********************************************************

By configuring Name Services, your server will be able to
become a part of domains that span IP subnets.

Do you want to (re)configure the Name Services [yes]?

To enable WAN support you must select at least one of the
following mechanisms:

- Name Resolution via lmhosts file
- Name Resolution via NetBIOS Name Service (NBNS) - e.g WINS Client
- Name Resolution via Domain Name Service (DNS)

Do you want to use lmhosts file? [no]? y

lmhosts filename: [/usr/net/servers/lanman/datafiles/lmhosts]

Do you want to edit the lmhosts file now [y/n]? n

Do you want to enable NBNS name resolution [no]? y
Enter IP address of Primary NBNS server: [no default] 10.0.0.4

Enter IP address of Secondary NBNS server or none: [none] 10.0.0.5

Do you want to enable DNS name resolution [no]? y

Enter list of DNS subdomains separated by comma: [no default]
company.com,company1.com

You’ve selected the following options for Name Services:

Use lmhosts file /usr/net/servers/lanman/datafiles/lmhosts
Use Primary NBNS server, address 10.0.0.4
Use Secondary NBNS server, address 10.0.0.5
Use DNS server, subdomains company.com,company1.com

Are you satisfied with these choices [yes]? y

Modifying the "transports.ini" file with Name Service choices.


**********************************************************
        NetBEUI-Datalink Controller Selection
**********************************************************

Select the controllers for the NetBEUI transport.
```

Example 6–1: Sample Multi Mode asusetup Output (cont.)

```
   ics0
   tu0

 Enter the controllers separated by a comma
 or type ? for help: [ ics0 ]  tu0

 You have entered:
  tu0

 Are you satisfied with these controllers? [yes]?

 Modifying the "transports.ini" file with tu0.

You will now be prompted to enter cluster configuration information
for the Advanced Server for UNIX.
The cluster environment can be configured as follows:
 none   - not using the cluster, the server runs on one node,
 single - single instance server ( controlled by CAA ),
 multi  - multi instance server, the server runs on all
    cluster members.


Enter the cluster environment type (multi, single or none) [multi]: multi

Enter the cluster alias [colors]:

Starting the transports...
Start:  Datalink service controller_01 tu0
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
          /dev/streams/netbeui         32         69
         /dev/streams/netbeuid         32         70
         /dev/streams/nbeadmin         32         71
Microsoft Datalink Driver : Starting dllink ...
Datalink driver attached to tu0 at PPA1
dllink: done - Adapter set
Start:  NetBEUI controller_01 tu0
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
          /dev/streams/netbeui         32         69
         /dev/streams/netbeuid         32         70
         /dev/streams/nbeadmin         32         71
Microsoft NetBEUI Driver : Starting nbelink ... done
Start:  TCP/IP NetBIOS controller_01 tu0
Starting the TCP/IP NetBIOS service...
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
           /dev/streams/knbtcp         32         72
           /dev/streams/knbadm         32         73
          /dev/streams/knbtcpd         32         74
TCP/IP NetBIOS: Starting knblink ...
   controller(s) configured as ’tu0’
   kernel dynamic cache will be enabled
   lmhosts file use enabled
   DNS support is enabled
   The following 2 DNS subdomains have been specified:
 company.com
```

Example 6–1: Sample Multi Mode asusetup Output (cont.)

```
 company1.com
   Cluster IP address = 10.0.0.6
   NBNS Client support enabled, primary server at 10.0.0.4
   NBNS Client support enabled, secondary server at 10.0.0.5
Successfully configured with controller(s) ’tu0’
TCP/IP NetBIOS name resolver started, pid=1080614
TCP/IP NetBIOS service started

Each ASU server must be assigned an ASU server name. ASU server names
can be up to 15 alphanumeric characters and can contain the following
symbols:

~ ! # $ % ^ & _ ( ) . -

Server names cannot include any international characters.

If this ASU server will participate in an ASE cluster environment,
then the server name that you assign here must also be the name that you
assign to the ASE cluster disk service for the ASU server.

Enter the name of the server
or press Enter to select ’red’:

Each server must be given a role in a domain.  The possible roles are:

Primary domain controller (PDC). There can be only one PDC per domain.
The PDC is where the master user account database is stored, which is
what the PDC uses to validate network logon requests.

Backup domain controller (BDC). There can be many BDCs per domain.
The BDC recieves a copy of the user account database from the PDC,
which is what it uses to validate network logon requests.
A BDC can be promoted to PDC if the PDC is not accessible.

Member server is a member of a domain.  Member servers do not store user
account information and therefore do not validate network logon requests.
These servers are dedicated to perform specific tasks such as being
file and print servers.

Enter role (primary, backup, or member): primary

Enter the name of the domain
or press Enter to select ’red.dom’: colors.dom

That domain name may already be in use.

Do you want to select a different domain name [y/n]? n

Confirm choices:
                    server name   : red
                    role          : primary
                    domain        : colors.dom
Is this correct [y/n]? y

Enter the password for Administrator:
Re-enter password:

Creating Advanced Server for UNIX accounts database.

A clean copy of the SAM database has been written.
Configuring registry...
```

Example 6–1: Sample Multi Mode asusetup Output (cont.)

```
reg.ini created successfully
reg.ini upgraded successfully
Creating new registry file...
processed 935 lines...
Registry file created successfully

loading /usr/net/servers/lanman/regfiles/perf009.regadm
loading /usr/net/servers/lanman/regfiles/users.regadm
loading /usr/net/servers/lanman/regfiles/machine.regadm
load registry initialization scripts...
registry load complete.

Upgrading SAM database to support new format

The ASU server currently listens for, and responds to,
messages sent to these network names:
 clusteralias    : colors
 ExtraListenNames:
                   (none)

You can define Extra Listen Names for the server to listen for
via the Registry parameter ExtraListenNames.

Do you want to modify the ExtraListenNames entry [y/n]? y

Enter the Extra Listen Names to add to the list.
 Press RETURN to terminate the list.

Enter an Extra Listen Name to add: red1

Enter an Extra Listen Name to add: red2

Enter an Extra Listen Name to add:

 ExtraListenNames:
                   red1
                   red2

Enter the Extra Listen Names to remove from the list.
 Press RETURN to terminate the list.

Enter an Extra Listen Name to remove:

 ExtraListenNames:
                   red1
                   red2

Are you satisfied with this list of ExtraListenNames [y/n]? y

These changes will take effect the next time
the server is started.

Cluster member blue.company.com is not configured to run Advanced Server.
You can configure it without affecting any other cluster member.

You will be asked to provide the names of controllers on blue.company.com
to be used for the Advanced Server transports.
We will provide default controller names based on the configuration
of another member of the cluster. But we cannot see what devices are
on blue.company.com, so we cannot validate these defaults. Also, we cannot
validate any device names you specify.
```

Example 6–1: Sample Multi Mode asusetup Output (cont.)

```
If you aren’t sure what controllers to specify, you should answer "no"
and re-run asusetup from blue.company.com.

Would you like to configure Advanced Server for UNIX
for cluster member blue.company.com [y/n]? y

CAUTION: The following default configuration is based on the
configuration of cluster member red.company.com.
It may not be suitable for blue.company.com,
so please respond appropriately.

The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’tu0’)
                NetBEUI (controller ’tu0’)

Would you like to use this network information [y/n]? y

The Advanced Server will be configured using this
network information.

Cluster member green.company.com is not configured to run Advanced Server.
You can configure it without affecting any other cluster member.

You will be asked to provide the names of controllers on green.company.com
to be used for the Advanced Server transports.
We will provide default controller names based on the configuration
of another member of the cluster. But we cannot see what devices are
on green.company.com, so we cannot validate these defaults. Also, we cannot
validate any device names you specify.

If you aren’t sure what controllers to specify, you should answer "no"
and re-run asusetup from green.company.com.

Would you like to configure Advanced Server for UNIX
for cluster member green.company.com [y/n]? y

CAUTION: The following default configuration is based on the
configuration of cluster member red.company.com.
It may not be suitable for green.company.com,
so please respond appropriately.

The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’tu0’)
                NetBEUI (controller ’tu0’)

Would you like to use this network information [y/n]? y

The Advanced Server will be configured using this
network information.

There are a number of registry parameters that affect how the
Advanced Server creates UNIX user accounts, such as UseNIS,
CreateUnixUser, and SpreadUnixHomeDirectory.  If you want to
change the values of these parameters, please use the regconfig
utility to change the parameters now before starting the server.
Please see the installation guide for further information.

Start the Advanced Server for UNIX [y/n]? y
```

Example 6–1: Sample Multi Mode asusetup Output (cont.)

```
The SERVER service is starting.................
The SERVER service was started successfully.

Advanced Server for UNIX has the ability to test itself.

Would you like to run this test now [y/n]? y

 (c) Compaq Computer Corp. 2001. All Rights Reserved.

Verification #1 via network netbeui

Create Share netbeui ...Succeeded
Grant user access to share ...Succeeded
Attempting connection to \\RED\netbeui ...Succeeded
List File ...Succeeded
Create File ...Succeeded
Write data to file ...Succeeded
Close data file ...Succeeded
Open file for reading ...Succeeded
Read data from file ...Succeeded
Data Verification ...Succeeded
Close data file ...Succeeded
Tree Disconnect ...Succeeded
Revoke user access to share ...Succeeded
Remove share netbeui ...Succeeded

Network netbeui complete.

Verification #1 via network knbtcp

Create Share knbtcp ...Succeeded
Grant user access to share ...Succeeded
Attempting connection to \\RED\knbtcp ...Succeeded
List File ...Succeeded
Create File ...Succeeded
Write data to file ...Succeeded
Close data file ...Succeeded
Open file for reading ...Succeeded
Read data from file ...Succeeded
Data Verification ...Succeeded
Close data file ...Succeeded
Tree Disconnect ...Succeeded
Revoke user access to share ...Succeeded
Remove share knbtcp ...Succeeded

Network knbtcp complete.
```

6.1.1.1 Configuring Additional ASU Servers in Multi Mode

If the ASU server is already running in the TruCluster cluster, and you want to configure an additional ASU server on a cluster member, then you must run the `asusetup` utility that cluster member.

The `asusetup` utility provides default values that you should use. If you must change some of the default values, do not change the default values of the cluster environment type (multi), cluster alias, and ASU role. These values are the same for all the ASU servers configured in multi mode in the TruCluster environment.

6.1.1.2 Multi lanman.ini File

ASU servers configured in multi mode determine their configuration by using a shared `lanman.ini` file that the `asusetup` utility creates.

The `[ cluster ]` section in the `lanman.ini` file contains the `cluster` attribute that specifies the ASU server mode and the `clusteralias` attribute that specifies the name of the cluster alias.

Example 6–2 is a sample `lanman.ini` file for ASU servers configured to operate in multi mode in a TruCluster environment.

Example 6–2: Sample Multi Mode lanman.ini File

```
[ cluster ]
cluster=multi
clusteralias=colors
[ workstation ]
domain=colors.dom
[ server ]
srvservices=alerter,netlogon,browser
[ lmxserver ]
LMCompatibilityLevel=0
secsources=Spooler;Security Account Manager;SC Manager;LSA;Security
syssources=workstation;UPS;Srv;Service Control Manager;server;SAM;
Rdr;Print;NetLogon;
eventlog;Browser;Alerter;System
appsources=Replicator;Perfmon;Perflib;Application
```

6.1.1.3 Multi transports.ini File

ASU servers configured in multi mode determine their network-specific configuration by using a shared `transports.ini` file that the `asusetup` utility creates.

The `[ member ]` section in the `transports.ini` file contains `member_`*`nn`*`=ASU_server_name` attributes that uniquely identify each cluster member that is running the ASU server in the TruCluster environment. This identification is necessary for the TruCluster software to rotate client connections and to redistribute client connections from a failed cluster member, and so clients can connect to ASU shares using the ASU server name instead of the cluster alias.

The [`tcpip`] section contains the `clusteraddr` attribute that specifies either the DNS name or TCP/IP address of the cluster alias.

Example 6–3 is a sample `/usr/net/servers/lanman/transports.ini` file for ASU servers configured to operate in multi mode in a TruCluster environment.

Example 6–3: Sample Multi Mode transports.ini File

```
[ tcpip ]
clusteraddr=colors
controller_01=tu0
uselmhosts=yes
lmhostsfile=/usr/net/servers/lanman/datafiles/lmhosts
enablenbns=yes
nbnsservaddr=10.0.0.4
nbnsservaddr2=10.0.0.5
enabledns=yes
dnssubdomains=company.com,company1.com
controller_02=tu0
controller_03=tu0
[ member ]
member_01=red.company.com,red
member_02=blue.company.com,blue
member_03=green.company.com,green
[ netbeui ]
controller_01=tu0
controller_02=tu0
controller_03=tu0
```

6.1.1.4 Managing ASU Servers Configured in Multi Mode

Rebooting or taking off-line a cluster member running the ASU server in multi mode does not effect the other ASU servers running in the TruCluster environment.

You use the ASU `net` commands to manage an ASU server configured in multi mode in a TruCluster environment. See Appendix D for more information about `net` commands. Table 6–1 notes how some `net` commands work differently in a TruCluster environment.

You use the commands and utilities described *Cluster Administration* to manage the cluster members and some aspects of the ASU servers, such as a load balancing policy. See *Cluster Administration* for more information.

Table 6–1: The net Commands that Work Differently in a Cluster

Command	Notes
`net file`	Displays all the open files in the TruCluster environment.
`net send`	Sends the message to users connected to the cluster member on which the command is entered.
`net session`	Displays all the client sessions in the TruCluster environment.
`net statistics server`, `net status`, and `net config`	Displays counters for the cluster member on which the command is entered.
`net start <service>`	Starts the specified service on all the ASU servers. For example, entering `net start browser` on a cluster member starts the browser service on all the ASU servers. See Section 1.6 for a list of ASU services. An exception is the `net start server` command, which starts the ASU server service only on the cluster member on which the command is entered.
`net stop <service>`	Stops the specified service on all the ASU servers. For example, entering `net stop browser` on a cluster member stops the browser service on all the ASU servers. See Section 1.6 for a list of ASU services. An exception is the `net stop server` command, which stops the ASU server service only on the cluster member on which the command is entered. You can enter the `asustop` command on any cluster member to stop the ASU server on all cluster members.
`net pause <service>`	Pauses the specified service on all the ASU servers. For example, entering `net pause browser` on a cluster member pauses the browser service on all the ASU servers. See Section 1.6 for a list of ASU services.
`net continue <service>`	Continues the specified service on all the ASU servers. For example, entering `net continue browser` on a cluster member continues the browser service on all the ASU servers. See Section 1.6 for a list of ASU services.

6.1.2 Configuring the ASU Server in Single Mode

You must run the `asusetup` utility on each cluster member on which you want to run the ASU server in single mode. The `asusetup` utility prompts you for the ASU server network and general information that is described in Section 1.4 and for the following TruCluster information:

- The mode (multi, single, or none) in which the ASU server will operate in the TruCluster environment
- The cluster alias

To run the `asusetup` utility, enter:

```
# /usr/sbin/asusetup
```

Example 6–4 displays sample `asusetup` output for an ASU server configured to operate in single mode.

Example 6–4: Sample Single Mode asusetup Output

```
       Advanced Server for UNIX Configuration Utility

Administrators can configure the Advanced Server software by using the
default configuration values that are detected from a previous Advanced
Server configuration.  If no previous Advanced Server configuration is
detected then the default values are determined by this utility. In
either case, administrators can choose not to use the default values and
customize the Advanced Server configuration by interactively supplying
Advanced Server configuration values.

The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’ics0’)
                NetBEUI (controller ’ics0’)
   Cluster Alias: cplors
   Cluster Type:  multi
   Server Name:   green
   Domain Name:   green.dom
   Domain Role:   Primary
   WAN Support:   enabledns=yes, uselmhosts=yes

Do you want to use this default information [y/n]? n

The following network configuration is based on the previous
network configuration, with default values for new items:

   Controllers:  TCP/IP  = ics0
                 NetBEUI = ics0

   Use DNS:                yes
   Sub Domains:            asu.company.com
   Use lmhosts:            yes
   lmhosts file:           /usr/net/servers/lanman/datafiles/lmhosts
   Use NBNS:               no
   Primary NBNS address:
   Secondary NBNS address:

Would you like to use this network information [y/n]? n
You will now be prompted to enter configuration information
for the Advanced Server for UNIX server including
which network transports and controllers to use and how
to resolve names in a wide area network.

Press return to continue...
```

Example 6–4: Sample Single Mode asusetup Output (cont.)

```
**********************************************************
        NetBIOS over TCP/IP Setup
**********************************************************

Select a controller for NetBIOS over TCP/IP.
The "transports.ini" file will be modified accordingly.

 ics0 @ address:  10.0.0.3
 tu0 @ address:   10.0.0.4
 none

Enter the controllers separated by a comma
or type ? for help: [ ics0 ]  tu0

You have entered:
 tu0

Are you satisfied with these controllers? [yes]?

Modifying the "transports.ini" file with tu0.

**********************************************************
                  WAN Name Services
**********************************************************

By configuring Name Services, your server will be able to
become a part of domains that span IP subnets.

Do you want to (re)configure the Name Services [yes]?

To enable WAN support you must select at least one of the
following mechanisms:

- Name Resolution via lmhosts file
- Name Resolution via NetBIOS Name Service (NBNS) - e.g WINS Client
- Name Resolution via Domain Name Service (DNS)

Do you want to use lmhosts file? [no]? y

lmhosts filename: [/usr/net/servers/lanman/datafiles/lmhosts]

Do you want to edit the lmhosts file now [y/n]? n

Do you want to enable NBNS name resolution [no]? y

Enter IP address of Primary NBNS server: [no default] 10.0.0.4

Enter IP address of Secondary NBNS server or none: [none] 10.0.0.5

Do you want to enable DNS name resolution [no]? y

Enter list of DNS subdomains separated by comma: [no default]
  company.com,company1.com

You’ve selected the following options for Name Services:

Use lmhosts file /usr/net/servers/lanman/datafiles/lmhosts
Use Primary NBNS server, address 10.0.0.4
Use Secondary NBNS server, address 10.0.0.5
Use DNS server, subdomains company.com,company1.com
```

Example 6–4: Sample Single Mode asusetup Output (cont.)

```
 Are you satisfied with these choices [yes]? y

 Modifying the "transports.ini" file with Name Service choices.

 **********************************************************
         NetBEUI-Datalink Controller Selection
 **********************************************************

 Select the controllers for the NetBEUI transport.

   ics0
   tu0
   none

 Enter the controllers separated by a comma
 or type ? for help: [ ics0 ]  tu0

 You have entered:
  tu0

 Are you satisfied with these controllers? [yes]?

 Modifying the "transports.ini" file with tu0.

You will now be prompted to enter cluster configuration information
for the Advanced Server for UNIX.
The cluster environment can be configured as follows:
 none   - not using the cluster, the server runs on one node,
 single - single instance server ( controlled by CAA ),
 multi  - multi instance server, the server runs on all
    cluster members.

Enter the cluster environment type (multi, single or none) [multi]: single

Enter the cluster alias [colors]:

Starting the transports...
Start:  Datalink service controller_01 tu0
Microsoft Datalink Driver : Starting dllink ...
Datalink driver attached to tu0 at PPA1
dllink: done - Adapter set
Start:  NetBEUI controller_01 tu0
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
          /dev/streams/netbeui         32         72
         /dev/streams/netbeuid         32         73
         /dev/streams/nbeadmin         32         74
Microsoft NetBEUI Driver : Starting nbelink ... done
Start:  TCP/IP NetBIOS controller_01 tu0
Starting the TCP/IP NetBIOS service...
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
           /dev/streams/knbtcp         32         69
           /dev/streams/knbadm         32         70
          /dev/streams/knbtcpd         32         71
TCP/IP NetBIOS: Starting knblink ...
   controller(s) configured as ’tu0’
   kernel dynamic cache will be enabled
```

Example 6–4: Sample Single Mode asusetup Output (cont.)

```
   lmhosts file use enabled
   DNS support is enabled
   The following 2 DNS subdomains have been specified:
 company.com
 company1.com
   Cluster IP address = 10.0.0.6
   NBNS Client support enabled, primary server at 10.0.0.4
   NBNS Client support enabled, secondary server at 10.0.0.5
Using alias as IP address on interface tu0
Successfully configured with controller(s) ’tu0’
TCP/IP NetBIOS name resolver started, pid=1624682
TCP/IP NetBIOS service started

Each ASU server must be assigned an ASU server name. ASU server names
can be up to 15 alphanumeric characters and can contain the following
symbols:

~ ! # $ % ^ & _ ( ) . -

Server names cannot include any international characters.

If this ASU server will participate in an ASE cluster environment,
then the server name that you assign here must also be the name that you
assign to the ASE cluster disk service for the ASU server.


Enter the name of the server
or press Enter to select ’green’:

Each server must be given a role in a domain.  The possible roles are:

Primary domain controller (PDC). There can be only one PDC per domain.
The PDC is where the master user account database is stored, which is
what the PDC uses to validate network logon requests.

Backup domain controller (BDC). There can be many BDCs per domain.
The BDC recieves a copy of the user account database from the PDC,
which is what it uses to validate network logon requests.
A BDC can be promoted to PDC if the PDC is not accessible.

Member server is a member of a domain.  Member servers do not store user
account information and therefore do not validate network logon requests.
These servers are dedicated to perform specific tasks such as being
file and print servers.

Enter role (primary, backup, or member): primary

Enter the name of the domain
or press Enter to select ’green.dom’: colors.dom

That domain name may already be in use.

Do you want to select a different domain name [y/n]? n

Confirm choices:
                    server name   : green
                    role          : primary
                    domain        : colors.dom
Is this correct [y/n]? y

Enter the password for Administrator:
```

Example 6–4: Sample Single Mode asusetup Output (cont.)

```
Re-enter password:

Creating Advanced Server for UNIX accounts database.

A clean copy of the SAM database has been written.
Configuring registry...
reg.ini created successfully
Upgrading ...
reg.ini upgraded successfully
Creating new registry file...
processed 935 lines...
Registry file created successfully

loading /usr/net/servers/lanman/regfiles/perf009.regadm
loading /usr/net/servers/lanman/regfiles/users.regadm
loading /usr/net/servers/lanman/regfiles/machine.regadm
load registry initialization scripts...
registry load complete.

Upgrading SAM database to support new format

The ASU server currently listens for, and responds to,
messages sent to these network names:
 listenname      : green
 ExtraListenNames:
                  (none)

You can define Extra Listen Names for the server to listen for
via the Registry parameter ExtraListenNames.

Do you want to modify the ExtraListenNames entry [y/n]? y
Enter the Extra Listen Names to add to the list.
 Press RETURN to terminate the list.

Enter an Extra Listen Name to add: green1

Enter an Extra Listen Name to add: green2

Enter an Extra Listen Name to add:

 ExtraListenNames:
                  green1
                  green2

Enter the Extra Listen Names to remove from the list.
 Press RETURN to terminate the list.

Enter an Extra Listen Name to remove:

 ExtraListenNames:
                  green1
                  green2

Are you satisfied with this list of ExtraListenNames [y/n]? y

These changes will take effect the next time
the server is started.

Cluster member blue.company.com is not configured to run Advanced Server.
You can configure it without affecting any other cluster member.
```

Example 6–4: Sample Single Mode asusetup Output (cont.)

```
You will be asked to provide the names of controllers on blue.company.com
to be used for the Advanced Server transports.
We will provide default controller names based on the configuration
of another member of the cluster. But we cannot see what devices are
on blue.company.com, so we cannot validate these defaults. Also, we cannot
validate any device names you specify.

If you aren’t sure what controllers to specify, you should answer "no"
and re-run asusetup from blue.company.com.

Would you like to configure Advanced Server for UNIX
for cluster member blue.company.com [y/n]? y

CAUTION: The following default configuration is based on the
configuration of cluster member green.company.com.
It may not be suitable for blue.company.com,
so please respond appropriately.


The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’tu0’)
                NetBEUI (controller ’tu0’)

Would you like to use this network information [y/n]? y

The Advanced Server will be configured using this
network information.

Cluster member red.company.com is not configured to run Advanced Server.
You can configure it without affecting any other cluster member.

You will be asked to provide the names of controllers on red.company.com
to be used for the Advanced Server transports.
We will provide default controller names based on the configuration
of another member of the cluster. But we cannot see what devices are
on red.company.com, so we cannot validate these defaults. Also, we cannot
validate any device names you specify.

If you aren’t sure what controllers to specify, you should answer "no"
and re-run asusetup from red.company.com.

Would you like to configure Advanced Server for UNIX
for cluster member red.company.com [y/n]? y


CAUTION: The following default configuration is based on the
configuration of cluster member green.company.com.
It may not be suitable for red.company.com,
so please respond appropriately.


The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’tu0’)
                NetBEUI (controller ’tu0’)

Would you like to use this network information [y/n]? y

The Advanced Server will be configured using this
network information.
```

Example 6–4: Sample Single Mode asusetup Output (cont.)

```
There are a number of registry parameters that affect how the
Advanced Server creates UNIX user accounts, such as UseNIS,
CreateUnixUser, and SpreadUnixHomeDirectory.  If you want to
change the values of these parameters, please use the regconfig
utility to change the parameters now before starting the server.
Please see the installation guide for further information.

Start the Advanced Server for UNIX [y/n]? y
The SERVER service is starting..................
The SERVER service was started successfully.

Advanced Server for UNIX has the ability to test itself.

Would you like to run this test now [y/n]? y

 (c) Compaq Computer Corp. 2001. All Rights Reserved.

Verification #1 via network netbeui

Create Share netbeui ...Succeeded
Grant user access to share ...Succeeded
Attempting connection to \\GREEN\netbeui ...Succeeded
List File ...Succeeded
Create File ...Succeeded
Write data to file ...Succeeded
Close data file ...Succeeded
Open file for reading ...Succeeded
Read data from file ...Succeeded
Data Verification ...Succeeded
Close data file ...Succeeded
Tree Disconnect ...Succeeded
Revoke user access to share ...Succeeded
Remove share netbeui ...Succeeded

Network netbeui complete.

Verification #1 via network knbtcp

Create Share knbtcp ...Succeeded
Grant user access to share ...Succeeded
Attempting connection to \\GREEN\knbtcp ...Succeeded
List File ...Succeeded
Create File ...Succeeded
Write data to file ...Succeeded
Close data file ...Succeeded
Open file for reading ...Succeeded
Read data from file ...Succeeded
Data Verification ...Succeeded
Close data file ...Succeeded
Tree Disconnect ...Succeeded
Revoke user access to share ...Succeeded
Remove share knbtcp ...Succeeded

Network knbtcp complete.
```

6.1.2.1 Configuring Additional ASU Servers in Single Mode

If the ASU server is already running in the TruCluster cluster, and you want to configure an additional ASU server on a cluster member, then you must run the `asusetup` utility that cluster member.

The `asusetup` utility provides default values that you should use. If you must change some of the default values, do not change the default values of the cluster environment type (single), cluster alias, and ASU role. These values are the same for all the ASU servers configured in single mode in the TruCluster environment.

6.1.2.2 Single lanman.ini File

ASU servers configured in single mode determine their configuration by using a shared `lanman.ini` file that the `asusetup` utility creates.

The `[ cluster ]` section in the `lanman.ini` file contains the `cluster` attribute that specifies the ASU server mode and the `clusteralias` attribute that specifies the name of the cluster alias.

Example 6–5 is a sample `lanman.ini` file for ASU servers configured to operate in single mode in a TruCluster environment.

Example 6–5: Sample Single Mode lanman.ini File

```
[ cluster ]
cluster=single
clusteralias=colors
[ workstation ]
domain=colors.dom
[ server ]
listenname=green
srvservices=alerter,netlogon,browser
[ lmxserver ]
LMCompatibilityLevel=0
secsources=Spooler;Security Account Manager;SC Manager;LSA;Security
syssources=workstation;UPS;Srv;Service Control Manager;server;SAM;Rdr;
Print;NetLogon;eventlog;Browser;Alerter;System
appsources=Replicator;Perfmon;Perflib;Application
```

6.1.2.3 Single transports.ini File

ASU servers configured in single mode determine their network-specific configuration by using a shared `transports.ini` file that the `asusetup` utility creates.

The `[ member ]` section in the `transports.ini` file contains `member_`*`nn`*`=ASU_server_name` attributes that uniquely identify each member server that is running the ASU server in the TruCluster environment. This identification is necessary for the TruCluster software to identify an alternate cluster member on which to start the ASU server if necessary.

The [`tcpip`] section contains the `clusteraddr` attribute that specifies either the DNS name or TCP/IP address of the cluster alias.

Example 6–6 is a sample `/usr/net/servers/lanman/transports.ini` file for ASU servers configured to operate in single mode in a TruCluster environment.

Example 6–6: Sample Single Mode transports.ini File

```
[ tcpip ]
clusteraddr=colors
controller_01=tu0
uselmhosts=yes
lmhostsfile=/usr/net/servers/lanman/datafiles/lmhosts
enablenbns=yes
nbnsservaddr=10.0.0.4
nbnsservaddr2=10.0.0.5
enabledns=yes
dnssubdomains=company.com,company1.com
controller_02=tu0
controller_03=tu0
[ member ]
member_01=green.company.com,green
member_02=blue.company.com,blue
member_03=red.company.com,red
[ netbeui ]
controller_01=tu0
controller_02=tu0
controller_03=tu0
```

6.1.2.4 Managing ASU Servers Configured in Single Mode

You use the ASU `net` commands to manage an ASU server configured in single mode in a TruCluster environment. The `net` commands will only work on the system on which the ASU server is running. See Appendix D for more information about `net` commands.

You use the commands and utilities described *Cluster Administration* to manage the cluster member and some aspects of the ASU server, such as specifying the alternate ASU server. See *Cluster Administration* for more information.

Note

If you configure ASU to run in single mode (CAA), then the ASU server is started by using the `caa_start asu` command and stopped by using the `caa_stop asu` command.

If the ASU server is not running at the time of a system shutdown, it will not start during the boot process. You must issue the `caa_start asu` command to start the ASU server.

See *Cluster Administration* for more information.

6.1.3 Configuring the ASU Server in None Mode

You must run the `asusetup` utility on the cluster member on which you want to run the ASU server in none mode. The `asusetup` utility prompts you for the ASU server network and general information that is described in Section 1.4 and for the following TruCluster information:

- The mode (multi, single, or none) in which the ASU server will operate in the TruCluster environment
- The cluster alias

  The cluster alias has no effect on an ASU server configured in none mode.

To run the `asusetup` utility, enter:

```
# /usr/sbin/asusetup
```

Example 6–7 displays sample `asusetup` output for an ASU server configured to operate in none mode.

Example 6–7: Sample None Mode asusetup Output

```
       Advanced Server for UNIX Configuration Utility

Administrators can configure the Advanced Server software by using the
default configuration values that are detected from a previous Advanced
Server configuration.  If no previous Advanced Server configuration is
detected then the default values are determined by this utility. In
either case, administrators can choose not to use the default values and
customize the Advanced Server configuration by interactively supplying
Advanced Server configuration values.

The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’ics0’)
                NetBEUI (controller ’ics0’)
   Cluster Alias: colors
   Cluster Type:  multi
```

Example 6–7: Sample None Mode asusetup Output (cont.)

```
Server Name:   blue
Domain Name:   blue.dom
Domain Role:   Primary
WAN Support:   enabledns=yes, uselmhosts=yes

     **********************************************************
             NetBIOS over TCP/IP Setup
     **********************************************************

     Select a controller for NetBIOS over TCP/IP.
     The "transports.ini" file will be modified accordingly.


             ics0 @ address:  10.0.0.3
             tu0 @ address:  16.20.20.96


     Enter the controllers separated by a comma
     or type ? for help: [ ics0 ]  tu0

     You have entered:
             tu0

     Are you satisfied with these controllers? [yes]?

     Modifying the "transports.ini" file with tu0.

     **********************************************************
                       WAN Name Services
     **********************************************************

     By configuring Name Services, your server will be able to
     become a part of domains that span IP subnets.

     Do you want to (re)configure the Name Services [yes]?

     To enable WAN support you must select at least one of the
     following mechanisms:

     - Name Resolution via lmhosts file
     - Name Resolution via NetBIOS Name Service (NBNS) - e.g WINS Client
     - Name Resolution via Domain Name Service (DNS)


     Do you want to use lmhosts file? [no]? y

     lmhosts filename: [/usr/net/servers/lanman/datafiles/lmhosts]

     Do you want to edit the lmhosts file now [y/n]? n

     Do you want to enable NBNS name resolution [no]? y

     Enter IP address of Primary NBNS server: [no default] 10.0.0.4
     Enter IP address of Secondary NBNS server or none: [none] 10.0.0.5

    Do you want to enable DNS name resolution [no]? y

     Enter list of DNS subdomains separated by comma: [no default] company.co
     m,company1.com

     You’ve selected the following options for Name Services:
```

Example 6–7: Sample None Mode asusetup Output (cont.)

```
        Use lmhosts file /usr/net/servers/lanman/datafiles/lmhosts
        Use Primary NBNS server, address 10.0.0.4
        Use Secondary NBNS server, address 10.0.0.5
        Use DNS server, subdomains company.com,company1.com

        Are you satisfied with these choices [yes]?

        Modifying the "transports.ini" file with Name Service choices.

        **********************************************************
                NetBEUI-Datalink Controller Selection
        **********************************************************

        Select the controllers for the NetBEUI transport.

                 ics0
                 tu0

        Enter the controllers separated by a comma
        or type ? for help: [ ics0 ]  tu0

        You have entered:
                tu0
 Are you satisfied with these controllers? [yes]?

        Modifying the "transports.ini" file with tu0.

You will now be prompted to enter cluster configuration information
for the Advanced Server for UNIX.
The cluster environment can be configured as follows:
        none   - not using the cluster, the server runs on one node,
        single - single instance server ( controlled by CAA ),
        multi  - multi instance server, the server runs on all
                         cluster members.

Enter the cluster environment type (multi, single or none) [multi]: none

Starting the transports...
Start:  Datalink service controller_01 tu0
        The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
           /dev/streams/knbtcp         32         69
           /dev/streams/knbadm         32         70
          /dev/streams/knbtcpd         32         71
          /dev/streams/netbeui         32         72
         /dev/streams/netbeuid         32         73
         /dev/streams/nbeadmin         32         74
Microsoft Datalink Driver : Starting dllink ...
Datalink driver attached to tu0 at PPA1
dllink: done - Adapter set
Start:  NetBEUI controller_01 tu0
        The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
          /dev/streams/netbeui         32         72
         /dev/streams/netbeuid         32         73
         /dev/streams/nbeadmin         32         74
Microsoft NetBEUI Driver : Starting nbelink ... done
Start:  TCP/IP NetBIOS controller_01 tu0
```

Example 6–7: Sample None Mode asusetup Output (cont.)

```
Starting the TCP/IP NetBIOS service...
TCP/IP NetBIOS: Starting knblink ...
   controller(s) configured as ’tu0’
   kernel dynamic cache will be enabled
   lmhosts file use enabled
   DNS support is enabled
   The following 2 DNS subdomains have been specified:
        company.com
        company1.com
   Cluster IP address = 10.0.0.6
   NBNS Client support enabled, primary server at 10.0.0.4
   NBNS Client support enabled, secondary server at 10.0.0.5
Using alias as IP address on interface tu0
Successfully configured with controller(s) ’tu0’
TCP/IP NetBIOS name resolver started, pid=1649549
TCP/IP NetBIOS service started

Each ASU server must be assigned an ASU server name. ASU server names
can be up to 15 alphanumeric characters and can contain the following
symbols:
~ ! # $ % ^ & _ ( ) . -

Server names cannot include any international characters.

If this ASU server will participate in an ASE cluster environment,
then the server name that you assign here must also be the name that you
assign to the ASE cluster disk service for the ASU server.


Enter the name of the server
or press Enter to select ’blue’:

Each server must be given a role in a domain.  The possible roles are:

Primary domain controller (PDC). There can be only one PDC per domain.
The PDC is where the master user account database is stored, which is
what the PDC uses to validate network logon requests.

Backup domain controller (BDC). There can be many BDCs per domain.
The BDC recieves a copy of the user account database from the PDC,
which is what it uses to validate network logon requests.
A BDC can be promoted to PDC if the PDC is not accessible.

Member server is a member of a domain.  Member servers do not store user
account information and therefore do not validate network logon requests.
These servers are dedicated to perform specific tasks such as being
file and print servers.

Enter role (primary, backup, or member): primary

Enter the name of the domain
or press Enter to select ’blue.dom’: colors.dom

That domain name may already be in use.

Do you want to select a different domain name [y/n]? n

Confirm choices:
                    server name   : blue
                    role          : primary
                    domain        : colors.dom
```

Example 6–7: Sample None Mode asusetup Output (cont.)

```
Is this correct [y/n]? y

Enter the password for Administrator:
Re-enter password:

Creating Advanced Server for UNIX accounts database.

A clean copy of the SAM database has been written.
Configuring registry...
reg.ini created successfully
Upgrading ...
reg.ini upgraded successfully
Creating new registry file...
processed 935 lines...
Registry file created successfully

loading /usr/net/servers/lanman/regfiles/perf009.regadm
loading /usr/net/servers/lanman/regfiles/users.regadm
loading /usr/net/servers/lanman/regfiles/machine.regadm
load registry initialization scripts...
registry load complete.

Upgrading SAM database to support new format

The ASU server currently listens for, and responds to,
messages sent to these network names:
        listenname      : blue
        ExtraListenNames:
                          (none)

You can define Extra Listen Names for the server to listen for
via the Registry parameter ExtraListenNames.

Do you want to modify the ExtraListenNames entry [y/n]? y

Enter the Extra Listen Names to add to the list.
        Press RETURN to terminate the list.

Enter an Extra Listen Name to add: blue1

Enter an Extra Listen Name to add: blue2
Are you satisfied with this list of ExtraListenNames [y/n]? y

These changes will take effect the next time
the server is started.


There are a number of registry parameters that affect how the
Advanced Server creates UNIX user accounts, such as UseNIS,
CreateUnixUser, and SpreadUnixHomeDirectory.  If you want to
change the values of these parameters, please use the regconfig
utility to change the parameters now before starting the server.
Please see the installation guide for further information.

Start the Advanced Server for UNIX [y/n]? y
The SERVER service is starting..................
The SERVER service was started successfully.

Advanced Server for UNIX has the ability to test itself.

Would you like to run this test now [y/n]? y
```

Example 6–7: Sample None Mode asusetup Output (cont.)

```
        (c) Compaq Computer Corp. 2001. All Rights Reserved.

Verification #1 via network netbeui

Create Share netbeui ...Succeeded
Grant user access to share ...Succeeded
Attempting connection to \\BLUE\netbeui ...Succeeded
List File ...Succeeded
Create File ...Succeeded
Write data to file ...Succeeded
Close data file ...Succeeded
Open file for reading ...Succeeded
Read data from file ...Succeeded
Data Verification ...Succeeded
Close data file ...Succeeded
Tree Disconnect ...Succeeded
Revoke user access to share ...Succeeded
Remove share netbeui ...Succeeded

Network netbeui complete.

Verification #1 via network knbtcp

Create Share knbtcp ...Succeeded
Grant user access to share ...Succeeded
Attempting connection to \\BLUE\knbtcp ...Succeeded
List File ...Succeeded
Create File ...Succeeded
Write data to file ...Succeeded
Close data file ...Succeeded
Open file for reading ...Succeeded
Read data from file ...Succeeded
Data Verification ...Succeeded
Close data file ...Succeeded
Tree Disconnect ...Succeeded
Revoke user access to share ...Succeeded
Remove share knbtcp ...Succeeded

Network knbtcp complete.
```

6.1.3.1 None lanman.ini File

ASU servers configured in none mode determine their configuration by using a shared `lanman.ini` file that the `asusetup` utility creates.

The `[ cluster ]` section in the `lanman.ini` file contains the `cluster` attribute that specifies the ASU server mode and the `clusteralias` attribute that specifies the name of the cluster alias.

Example 6–8 is a sample `lanman.ini` file for ASU servers configured to operate in none mode in a TruCluster environment.

Example 6–8: Sample None Mode lanman.ini File

```
[ cluster ]
cluster=none
[ server ]
listenname=blue
srvservices=alerter,netlogon,browser
[ workstation ]
domain=colors.dom
[ lmxserver ]
LMCompatibilityLevel=0
secsources=Spooler;Security Account Manager;SC Manager;LSA;Security
syssources=workstation;UPS;Srv;Service Control Manager;server;SAM;Rdr;
Print;NetLogon;eventlog;Browser;Alerter;System
appsources=Replicator;Perfmon;Perflib;Application
```

6.1.3.2 None transports.ini File

ASU servers configured in none mode determine their network-specific configuration by using a shared `transports.ini` file that the `asusetup` utility creates.

The `[ member ]` section in the `transports.ini` file contains `member_`*`nn`*`=ASU_server_name` attributes that uniquely identify each ASU server in the TruCluster environment. This identification is necessary if clients connect to ASU shares using the ASU server name instead of the cluster alias.

Example 6–9 is a sample `/usr/net/servers/lanman/transports.ini` file for ASU servers configured to operate in none mode in a TruCluster environment.

Example 6–9: Sample None Mode transports.ini File

```
[ tcpip ]
clusteraddr=sam
controller_01=tu0
uselmhosts=yes
lmhostsfile=/usr/net/servers/lanman/datafiles/lmhosts
enablenbns=yes
nbnsservaddr=10.0.0.4
nbnsservaddr2=10.0.0.5
enabledns=yes
dnssubdomains=company.com,company1.com
[ member ]
member_01=blue.company.com,blue
[ netbeui ]
```

Example 6–9: Sample None Mode transports.ini File (cont.)

```
controller_01=tu0
```

6.1.3.3 Managing ASU Servers Configured in None Mode

You use the ASU `net` commands to manage an ASU server configured in none mode in a TruCluster environment. See Appendix D for more information about `net` commands.

6.2 ASU Licensing in a TruCluster Environment

You configure ASU licensing in a TruCluster environment as follows:

- If the ASU server is configured in none mode, you must have a separate ASU license PAK installed on each cluster member that is running the ASU server.
- If the ASU server is configured in single mode (CAA), you can install the same ASU license PAK on all cluster members to which the ASU server can failover because the ASU server will be running only on one cluster member at a time.
- If the ASU server is configured in multi mode, you can configure the ASU server to use cluster-wide licensing. When using cluster-wide licensing, you install the ASU license PAKs on each cluster member; the ASU server will issue the licenses and keep track of the connections to the cluster. For example, if you purchase a 100 user client PAK and you have a three member cluster, install the PAK on all three members. The ASU server will ensure that only 100 clients (plus two free) can connect to the cluster.

  Follow these steps to use cluster-wide licensing:

  1. On a cluster member, enter the `asustop` command to stop all instances of the ASU server in the cluster. The `asustop` command stops the ASU server on all cluster members.
  2. On a cluster member, enter the following command to enable the `UseClusterLicensing` registry entry. The backslash (\ ) at the end a line indicates continuation. Enter the entire command, then press the Enter key.

     ```
     # regconfig SYSTEM/CurrentControlSet/Services/\
     AdvancedServer/Parameters UseClusterLicensing REG_DWORD 1
     ```

  3. On each cluster member on which the ASU server is installed, enter the following command to restart the ASU server:

```
# net start server
```

4. Install the ASU license PAKs on each cluster member running the ASU server.

7

Tuning ASU

This chapter describes how to specify the number of clients, transport sessions, server processes, and open files for the ASU server. You might need to specify these if you want to:

- Limit the number of clients that access the ASU software
- Configure the ASU server to support an unusually large number of clients and connections
- Support Hierarchical Storage Manager (HSM)

7.1 Specifying the Number of Clients

By default, the ASU server is configured to service 200 clients. You can increase this number, however the ASU server will service only as many clients as there are ASU licenses.

To change the number of clients that the ASU server services, change the value of the `maxclients` parameter in the [`server`] section of the `lanman.ini` file. If you increase the number of clients, you might need to increase the number of transport sessions that the ASU server can support as described in Section 7.2.

See Appendix C for information on modifying parameters in the `lanman.ini` file.

7.2 Specifying the Number of Transport Sessions

If you increase the number of clients that the ASU server services, then you might need to increase the number of transport sessions that the ASU server can open. Each Windows 95 and Windows 98 client uses one session. Each Windows NT client uses two sessions. The following table shows the default session limits for the ASU transports.

Transport	Default Session Limit
NetBEUI	256
TCP/IP	Unlimited

Follow these steps to change the number of NetBEUI sessions:

1. Stop the ASU server by entering the following command:

   ```
   # net stop server
   ```

2. Stop the NetBEUI transport by entering the following command:

   ```
   # /sbin/init.d/asunbelink stop
   ```

3. Create a `stanza` format attributes file. For example, to create a `stanza` format attributes file to increase the NetBEUI sessions to 1024, enter:

   ```
   # cat > netbeui.stanza
   netbeui:
   nb_sessions = 1024
   ^D
   ```

4. Merge the attributes into the `/etc/sysconfigtab` file by entering the following command:

   ```
   # sysconfigdb -a -f netbeui.stanza netbeui
   ```

   If there is an existing entry in the `sysconfigtab` file for `knbtcp` or `netbeui`, use the `-u` flag to update the entry instead of the `-a` option to add an entry.

5. Restart the NetBEUI transport by entering the following command:

   ```
   # /sbin/init.d/asunbelink start
   ```

6. Restart the ASU server by entering the following command:

   ```
   # net start server
   ```

7. Enter the following command to show the new number of NetBEUI sessions:

   ```
   # nbemon -i1
   ```

7.3 Specifying the Number of Server Processes

By default, each client acquires its own `lmx.srv` process until a maximum is reached. Then, the existing `lmx.srv` processes are assigned to additional clients in a rotating fashion.

By default, the maximum number of `lmx.srv` processes that the ASU server creates to service client requests is computed from the `VCDistribution` registry value entry and from the `maxclients` parameter in the `lanman.ini` file.

To change the default value, you assign a value to the `maxserverprocs` parameter in the [`server`] section of the `lanman.ini` file. Assigning a value to the `maxserverprocs` parameter overrides the value of the `MinVCPerProc`, `MaxVCPerProc`, and `VCDistribution` registry entries.

If you set the `maxserverprocs` parameter, choose the largest number possible before memory swapping occurs. For example, a 2 GB system can support 350 server processes before memory swapping occurs, if no other applications are run on that system.

If you set the `maxserverprocs` parameter above 100, you must also change the maximum number of NetBIOS names. See Section 7.4 for information on changing the number of NetBIOS names.

See Appendix C for information on modifying parameters in the `lanman.ini` file.

7.4 Specifying the Number of NetBIOS Names

Each `lmx.srv` process needs a NetBIOS name to send datagrams. These names are *`lmxname#pid`*, where *`lmxname`* is the listen name of the ASU server and *`pid`* is the PID of the server process. The default number of NetBIOS names is 128 for TCP/IP and NetBEUI.

Follow these steps to set the number NetBIOS names for TCP/IP and NetBEUI to 200:

1. Stop the ASU server by entering the following command:

   ```
   # net stop server
   ```

2. Stop the ASU transports by entering the following command:

   ```
   # /sbin/init.d/asutcp stop
   ```

   To stop the NetBEUI transport, enter:

   ```
   # /sbin/init.d/asunbelink stop
   ```

3. Create a `stanza` format attributes file. For example, to create a `stanza` format attributes file to increase the TCP/IP names to 200, enter:

   ```
   # cat > knbtcp.stanza
   knbtcp:
   knbnames = 200
   ^D
   ```

   To create a `stanza` format attributes file to increase the NetBEUI names to 200, enter:

   ```
   # cat > netbeui.stanza
   netbeui:
   nb_names = 200
   ^D
   ```

4. Merge the attributes in to the `/etc/sysconfigtab` file. To merge the TCP/IP changes, enter:

   ```
   # sysconfigdb -a -f knbtcp.stanza knbtcp
   ```

To merge the NetBEUI changes, enter:

```
# sysconfigdb -a -f netbeui.stanza netbeui
```

If there is an existing entry in the `sysconfigtab` file for `knbtcp` or `netbeui`, use the `-u` flag to update the entry instead of the `-a` option to add an entry.

5. Restart the ASU transports. To start the TCP/IP transport, enter:

   ```
   # /sbin/init.d/asutcp start
   ```

   To start the NetBEUI transport, enter:

   ```
   # /sbin/init.d/asunbelink start
   ```

6. Restart the ASU server by entering the following command:

   ```
   # net start server
   ```

7.5 Support for HSM

The Hierarchical Storage Manager (HSM) migrates infrequently used files to tape, and recalls them automatically when the file is referenced. The process that opens the file is blocked until the file is retrieved from tape. This can cause denial-of-service problems if the process is the ASU `lmx.srv` process that is serving more than one client.

To avoid this problem, ensure that each client gets its own `lmx.srv` process by setting the `maxserverprocs` parameter in the [`server`] section of the `lanman.ini` file to the same value as `maxclients` parameter in the [`server`] section of the `lanman.ini` file. Each client then gets its own `lmx.srv` process and no client blocks another client by opening a file that was migrated to tape. See Appendix C for information on modifying parameters in the `lanman.ini` file.

If you set the `maxserverprocs` parameter above 100, you must change the number of NetBIOS names. See Section 7.4 for information on changing the number of NetBIOS names.

7.6 Specifying the Number of Open Files and Record Locks

The ASU server can run out of structures in shared memory if:

- There are a large number of connections
- Each client opens several files
- Each client holds several file locks, as in a database environment

If the ASU server runs out of structures, users receive error messages when they try to open files, and a message is logged in the system event log. The log can be viewed either by running the Event Viewer application on a

Windows NT system and connecting to the ASU server, or by running the `elfread` utility on the Tru64 UNIX command line.

You can allocate additional structures to the ASU server by changing the value of the `NumUStructs` value entry in the ASU registry, which by default is 1000. Three structures are used for each open file and one structure is used for each byte range lock. You can estimate the number of open files and locks that each user might use and multiply by the number of users to determine the number of structures. If you increase the `NumUStructs` value entry, you might also need to increase the parameters that specify the amount of Tru64 UNIX shared memory. See *System Tuning* for more information on shared memory.

You use a registry editor to change the value of the `NumUStructs` value entry. For example, follow these steps to use the `regconfig` registry editor to increase the `NumUStructs` value entry to 5000. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Change the `NumUStructs` entry by entering the following command:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/ProcessParameters \
   NumUStructs REG_DWORD 5000
   ```

2. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   ```

   ```
   # net start server
   ```

8

Troubleshooting the ASU Software

This chapter describes how to troubleshoot some common ASU problems, describes tools that you can use to learn about problems, and offers possible solutions.

8.1 Preventing Problems

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

8.1.1 Reviewing Statistics

You can use the `net statistics` command to display detailed statistics about the current usage and cumulative usage of ASU over a period of time. If you review ASU statistics on a regular basis, you will find it easier to recognize and address ASU changes. Table 8–1 describes the statistics that the ASU server maintains.

Table 8–1: ASU Statistics

Statistic	Shows
Statistics since	The start date for reading this set of statistics (either at the last ASU startup or the last time the statistics were cleared).
Sessions accepted	The number of times users connected to the ASU 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 ASU server transmitted.
Kilobytes received	The number of kilobytes of data the ASU server received.

Table 8–1: ASU Statistics (cont.)

Statistic	Shows
Mean response time (msec)	The average response time for processing remote server requests. This always will be zero (0) for Tru64 UNIX system servers.
System errors	This statistic does not apply to Tru64 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.
Communication devices accessed	This statistic is not supported on the ASU server.
Print jobs spooled	The number of print jobs that were spooled to printer queues.
Times buffers exhausted	The number of shortages of big request buffers. Always set to zero (0) for Tru64 UNIX system servers.

8.1.2 Gathering Transaction Statistics

By default, transaction statistics are gathered by the `countbeans` parameter in the `lanman.ini` file.

To disable the countbeans parameter, edit the `lanman.ini` file and change the `countbeans` value to `no`. Add the `countbeans` parameter to the `lanman.ini` file under the `lmxserver` section if it does not already exist. For example, to disable the `countbeans` parameter, enter:

```
[ lmxserver ]
countbeans=no
```

To enable the `countbeans` parameter, set the value to `yes`.

Use the `asustat -n` command to view transaction statistics. The following message is displayed if the `countbeans` parameter is disabled:

```
The gathering of transaction statistics has been disabled.
```

8.1.3 Using Scripts

You can use the scripting features provided by the Tru64 UNIX operating system in combination with ASU data-gathering tools to create a powerful tool that can assess the condition of the ASU server at any time.

For example, using the Tru64 UNIX system job scheduling feature (`cron`), ASU data gathering tools, and standard Tru64 UNIX commands for checking file system integrity and free space, you can write scripts that perform various checks and mail the results to Tru64 UNIX system administrators at regular intervals.

8.1.4 Generating Alert Messages

The ASU server sends a message to a specified list of users when an administrative alert occurs. The system generates administrative alerts that relate to the ASU server and resource use. They warn about security and access problems, user session problems, problems with services, shutdown because of power loss, printer problems, and registry parameters being exceeded.

For example, the following situations will generate an alert message:

- The number of errors exceeds a threshold set in the ASU registry.
- Errors were encountered during the start of the `NetLogon` service.
- A printer is malfunctioning.

For an alert message 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 an alert message to be received, the `Messenger` service must be running on the destination computer.

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

8.1.5 System, Security, and Application Log Files

Events generated by the ASU server are automatically recorded in three event log files: system, security, and application.

An ASU event is any significant occurrence in the system (or in an application) that requires user notification. Critical events are noted in on-screen messages. An event that does not require immediate attention is recorded in one of the following event log files located in the `/usr/net/server/lanman/logs` directory:

- System - The system log files record events logged by the system components. For example, the failure of a driver or a system component to load during startup.
- Security - The security log files 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 login attempts by a user. Only administrators can view security logs.
- Application - The application log files record events logged by applications.

You can view system, security, and application log files by using either the Windows based Event Viewer or the `elfread` command.

8.1.5.1 Windows Event Viewer

The Event Viewer (`eventvwr.exe`) is installed on Windows NT systems. You can install the Event Viewer on a Windows 95 or Windows 98 system by installing the Windows based administrative interfaces. See Section 1.8.2 for more information on installing the Windows based administrative interfaces.

The Event Viewer lists events. Double click on any event to learn more about it.

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

8.1.5.2 The elfread Command

Use the `elfread` command to display log files and clear events. You can copy, move, or rename the default log file to a file that you specify.

To display a summary of the system log, enter:

```
# elfread system
```

To display a file called Monday into which you copied the system log, enter:

```
# elfread -f Monday system
```

See `elfread`(8) for more information on the `elfread` command.

8.1.6 Printer Log Files

For each printer share and each Tru64 UNIX system printer, the ASU 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 use a text editor to periodically check these log files to determine whether such errors have occurred.

8.1.7 Logging ASU Network Errors

The following sections describe where ASU network related errors are logged.

8.1.7.1 Computer Name Conflicts

If the computer name you choose for the ASU server conflicts with an existing system, an error message containing the name and address of the system that declared the conflict is generated in the following files:

- `/var/adm/messages`
- `/var/adm/syslog.dated/`*`date`*`/kern.log`

8.1.7.2 Connection Problems Between a WINS Server and an ASU Server

Messages are generated in the following log files when the ASU server, configured as a WINS client, loses and reestablishes contact with a WINS server:

- `/var/adm/messages`
- `/var/adm/syslog.dated/`*`date`*`/kern.log`

8.1.7.3 NetBIOS over TCP/IP Runs Out of Names

If NetBIOS over TCP/IP runs out of names, the following message is written to the system log (`/var/adm/messages`):

```
knbtcp: Warning - NetBIOS name limit exceeded; current limit = 32
Recommend increasing parameter "knbnames" for subsystem "knbtcp"
using sysconfigdb
```

See Chapter 7 for more information on increasing the number of NetBIOS over TCP/IP (`knbtcp`) names.

8.1.7.4 NetBEUI Runs Out of Datalinks

If NetBEUI runs out of datalinks, the following message is written to the system log (`/var/adm/messages`):

```
netbeui: Warning - link limit exceeded; current limit = 8
Recommend increasing parameter "nb_datalinks" for subsystem
"netbeui" using sysconfigdb
```

This error occurs when there are insufficient datalinks for the number of controllers configured. You need to configure two datalinks in NetBEUI for each controller configured.

See Chapter 7 for more information on increasing the number of datalinks.

8.1.7.5 NetBEUI Runs Out of Names

If NetBEUI runs out of NetBIOS names, the following message is written to the system log (`/var/adm/messages`):

```
netbeui: Warning - NetBIOS name limit exceeded; current limit = 32
Recommend increasing parameter "nb_names" for subsystem "netbeui"
using sysconfigdb
```

See Chapter 7 for more information on increasing the number of NetBIOS names.

8.1.8 Capturing All Network Packets

You can configure the ASU server to log information about all the network packets that are generated or received by the ASU server to a text file located in the `/usr/net/server/lanman/debug` directory. The file is called `Debug-`*`process`*`-`*`pid`*, where *`process`* is the name of the process and *`pid`* is the process identifier.

You can use a text editor to view the `Debug-`*`process`*`-`*`pid`* file to learn about the contents of the network packets.

When the logging of network packets is enabled, the ASU server responds slowly since all network activity is being recorded. You should enable logging only for the purpose of duplicating a problem. Stop the logging of network packets after the problem is duplicated and a `Debug-`*`process`*`-`*`pid`* file is generated.

To enable the ASU server to log network packets you can:

- Use the `kill` command, for example:

  ```
  # kill -30 pid
  ```

  Where *pid* is the process ID of any ASU process, for example the `lmx.srv` process.

  This command does not require you to restart the ASU server. Reenter the command to stop the ASU server from logging network packets.

- Edit the `lanman.ini` file, add the following parameters in the [`lmxserver`] section, and restart the ASU server:

  ```
  debug=yes
  ```

  Set the `debug` parameter to `no` to stop logging network packets.

You can add the `debugumask` parameter in the [`lmxserver`] section of the `lanman.ini` file to control user access to the debug log and crash files. The permissions you set are similar to the octal settings used by the `umask` command. The default value for the `debugumask` parameter is 0600 (Read and Write for the owner).

If the problem is caused by a process that terminated abnormally, then a subdirectory specific to that process is created in the `/usr/net/server/lanman/debug` directory. The subdirectory is called `Crash-`*`process-pid-node`*, where *`process`* is the name of the process, *`pid`* is the process identifier for the process that terminated abnormally, and *node* is the name of the node on which the process was running. A `core`, `StackTrace`, and a `ShmemTrace` file are placed in the directory.

For example, if a server process (`lmx.srv`) with a PID of 512 on a node called red crashes, `core`, `StackTrace`, and a `ShmemTrace` files are created in the following directory:

```
/usr/net/servers/lanman/debug/Crash-LMX.SRV-512-RED
```

You can use a text editor to view the `StackTrace` file to learn about the process termination.

You can use the `asustat -i` command to view the `ShmemTrace` file to learn about the state of the ASU server when the process terminated. For example, to view a `ShmemTrace` file for a server process with a PID of 512 that crashed on a node called red, enter the following commands:

```
# cd /usr/net/servers/lanman/debug/Crash-LMX.SRV-512-RED
```

```
# asustat -a -i ShmemTrace
```

8.1.9 Generating StackTrace and Core Files for ASU Processes

If you are unable to determine the cause of an ASU problem, you can generate a `StackTrace`, `ShmemTrace`, and a `core` file for each ASU process. The `StackTrace`, `ShmemTrace`, and `core` files contain information that helps you to determine the state of each started ASU service.

Generating `StackTrace`, `ShmemTrace`, and `core` files causes the started ASU processes and services to stop, and creates a directory for each process in the `/usr/net/servers/lanman/debug` directory in which a `StackTrace`, `ShmemTrace`, and `core` file is generated. The directory created is called `Crash-`*`process-pid-node`*, where *`process`* is the process name, *`pid`* is the process identifier, and *node* is the name of the node on which the process was running.

To generate a `StackTrace`, `ShmemTrace`, and `core` file for each started ASU process you must send a `SIGTRAP` to the `lmx.ctrl` PID. For example, if the PID for the `lmx.ctrl` process is 26059, enter:

```
# kill -5 26059
```

8.1.10 Generating StackTrace and Core Files for ASU Transport Link Processes

If you are unable to determine the cause of an ASU transport problem, you can generate a `StackTrace` and `core` file for each link process. The `StackTrace` and `core` files contain information that helps you to determine the state of each started ASU link process.

Generating `StackTrace` and `core` files causes the started ASU transport link processes to stop, and creates a directory for each process in the `/usr/net/servers/lanman/debug` directory in which a `StackTrace` and `core` file is generated. The directory created is called `Crash-`*`process-pid`*, where *`process`* is the link process name and *`pid`* is the process identifier.

To generate `StackTrace` and `core` files for each started ASU transport link process, you must send a `SIGTRAP` to the link PID. For example, if the PID for the `knblink` process is 685, enter:

```
# kill -5 685
```

8.2 Solving Common ASU Server Problems

This section describes some common ASU server problems and recommends resolutions.

8.2.1 The ASU Software Might Be Corrupt

If you suspect that the ASU software is corrupt, use the `fverify` command to verify the attributes for installed files related to ASU.

During the ASU installation a special inventory file called *`SUBSET`*`.inv.inst` was created in the `/usr/.smdb.` directory. Use this special inventory file as the input for the `fverify` command. For example, to verify the files in the ASUBASE*nnn* subset, enter:

```
# /usr/lbin/fverify < /usr/.smdb./ASUBASEnnn.inv.inst
```

Where *nnn* is the version of ASU. See the ASU *Release Notes* for the current version number.

See `fverify`(8) for more information on the `fverify` command.

8.2.2 The ASU Server Will Not Start

If the ASU server will not start:

- Enter the following command to verify if the ACL is corrupt. If the file is corrupt, then the command prompts you before repairing the file.

  ```
  # acladm -C
  ```

See `acladm`(8) for more information on the `acladm` command.

- Enter the following command to verify that ASU file-on-file mount points were removed:

  ```
  # mount | grep /usr/net/servers/lanman/mailslot
  ```

  If ASU file-on-file mount points display, enter the following command to remove each one:

  ```
  # umount file-on-file_mount_point
  ```

8.2.3 Difficulty Accessing the ASU Server

The following sections describe items to check if a large portion of the user community cannot access the ASU server.

8.2.3.1 Verify Network Links

Most networking hardware provides status indicators that you use to assess the state of the various network links (for example, 10-Base-T Hubs use LEDs). See your network hardware documentation for information on how to check these links for signs of problems.

If a client cannot connect to anything on a network that is otherwise functioning, then it is safe to assume that the problem is related to that client's network configuration. If, however, that client can connect to other systems on the network but not to the ASU server, then the network path to the ASU server or the account being used by that client is likely to be the source of the trouble.

Several third-party products are available that you can use to monitor the activity of the physical network. Check your network traffic periodically to determine whether or not problems are occurring with the physical network.

8.2.3.2 Verify that the Required ASU Processes Are Running

To verify that the ASU processes are running, enter:

```
# ps -ef | grep lmx
```

Information similar to the following is displayed:

```
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, might be displayed as in the preceding example. The controller starts new `lmx.srv` processes based on the number of clients supported by the server. As more client sessions start, more `lmx.srv` processes may start, each with a unique process ID and number. Information about other processes, such as `lmx.browser` and `lmx.alerter`, might be displayed.

Use the `asustat` command to display current ASU data from the system's shared memory image. Executing the `asustat -c` command displays information similar to the following that shows clients connected to `lmx.srv` processes:

```
Clients:

[000] A.SERVE~X nwnum=0, vcnum=2 on 17713 LIC=00 (NONE)     link=[000]
[002] B         nwnum=0, vcnum=1 on 17713 LIC=02 (BUILT-IN) link=[002]
[003] C         nwnum=0, vcnum=1 on 17722 LIC=02 (BUILT-IN) link=[003]
```

Notice that each client name has an associated PID number (for example, A.SERVE~X has PID 17713). This is the PID of the `lmx.srv` process that currently is serving that client. The `nwnum` value specifies the transport that is being used for the session where 0 is NetBEUI and 1 is TCP/IP. The `vcnum` value specifies whether this is the client computer's first connection or an additional connection.

The ability to determine the PID of the `lmx.srv` process that is serving a client is particularly useful when using the `asustat -w` command. This command requires a PID.

If the ASU server is not running, enter the following command:

```
# net start server
```

8.2.3.3 Verify that the Required ASU Services Are Started

Determine if the ASU services started properly. A situation can occur when several ASU server processes are running, but the ASU server cannot be accessed because a particular service did not start. This is especially true for the `NetLogon` service. To display the started ASU services, enter:

```
# net start
```

A list of started ASU services is displayed.

If the `NetLogon` and `Server` services are not displayed, there is a problem with the ASU software. The `NetLogon` service sometimes will not start because of a problem with the ASU server name, domain name, or domain configuration.

Check the event logs for problems as described earlier in this chapter.

8.2.3.4 Verify that ASU Can Communicate Using TCP/IP

If the physical network appears to be functioning properly, then determine whether the various systems on the network can communicate with each other using the TCP/IP transport protocol.

You can use the Tru64 UNIX `ping` command to test whether or not the TCP/IP transport protocol is working properly on systems.

If the `ping` command is entered on a system on which the ASU server is running and cannot locate a client, then that client cannot connect to the ASU server using the TCP/IP transport protocol.

If the `ping` command is entered on several systems and cannot locate the system on which the ASU server is running, then one of the following conditions might exist:

- The ASU server is not running. To display the started ASU services, enter:

  ```
  # net start
  ```

  If the ASU server is not running, enter the following command:

  ```
  # net start server
  ```

- The TCP/IP transport protocol is not running on the system on which the ASU server is running.
- A configuration problem is disrupting network connectivity.

If the `ping` command fails, run the `/usr/sbin/asuivp` utility to verify that the TCP/IP protocol is installed correctly.

Review the recommendations in your transport protocol software documentation.

See `ping`(8) for more information on the `ping` command.

8.2.3.5 Verify that ASU Can Communicate Using NetBIOS

ASU server communications are based on NetBIOS name sessions. Therefore, connectivity between nodes may be available but, if connectivity between NetBIOS names is not working, then the ASU server will not work.

To determine if the ASU server is communicating over the network using NetBIOS, enter:

```
# net view
```

If the ASU server name does not display, enter the `asusetup` command to reconfigure the ASU transports.

To determine if NetBEUI is posting NetBIOS names correctly, enter:

```
# nbemon -i1
```

To determine if TCP/IP is posting NetBIOS names correctly, enter:

```
# knbmon -i1
```

If names do not display, then either the transport type is not configured to run, or the ASU link process for the transport has stopped. To determine if the TCP/IP link process is running, enter:

```
# ps -e | grep knblink
```

To determine if the NetBEUI link process is running, enter:

```
# ps -e | grep dllink
```

```
# ps -e | grep nbelink
```

If the process is not running, execute `asusetup` to configure and restart the link process. If you get the error `Cannot unload drive`, you must reboot the system.

8.2.3.6 Verify Tru64 UNIX System Functionality

If network connections are working properly, verify the functionality of the Tru64 UNIX operating system on the system on which the ASU server is installed. The Tru64 UNIX operating system software provides a variety of log files and system checks that you can use to verify proper operation. See *System Administration* for information on these checks.

The ASU server is particularly sensitive to the following system problems:

- Improperly tuned kernel parameters, such as maximum number of open files
- Insufficient disk space in critical file systems such as `root` (`/`) or `/var`
- Insufficient system memory, causing excessive swapping
- CPU bound conditions
- Unbalanced disk loads

8.2.3.7 Verify that ASU Special Disk Shares Are Shared

The following special ASU disk shares are automatically shared when you install the ASU software. Do not delete, modify, or reshare these special disk shares. Clients use these special disk shares in the background.

```
ADMIN$
C$
D$
DOSUTIL
IPC$
NETLOGON
OS2UTIL
PRINTLOG
PRINT$
USERS
```

If any of these special disk shares are missing, the ASU server will not function properly. Enter the following command to display disk shares:

```
# net view \\ASU_servername
```

Special disk shares ending with a dollar sign ($) are hidden and do not display when you browse the ASU server. However, you can connect to a hidden share if you specify the share name as follows:

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

If you detect a special disk share is missing, restart the ASU server by entering the following commands:

```
# net stop server
```

```
# net start server
```

Contact your services representative if a special disk shares is still missing after you restart the ASU server.

8.2.3.8 Determine If the ASU Registry Is Corrupt

To determine whether the internal format of the registry file is corrupt, enter:

```
# regcheck -C
```

A message is displayed that reports the condition of the registry.

If a message indicates that the registry is corrupt, enter the following command to repair the registry:

```
# regcheck -R
```

A message similar to one of the following is displayed that indicates the source of the corruption:

```
Keys had larger ID’s than the next ID to allocate.
```

```
Keys did not have hash table entries.
```

```
Keys had duplicate ID’s.
Keys listed nonexistent subkeys.

Keys were not listed as subkeys by their parents.

Keys had nonexistent parents.

Keys had wrong subkey names.

Keys listed subkeys that weren’t really subkeys.

Keys had inconsistent representations.

Dead entries were found in the hash table.
```

If any corruption in the registry was repaired, enter the following command to reinitialize any missing registry values to their defaults:

```
# regload
```

Follow these steps if you are unable to repair the registry:

1. Delete the registry by entering the following command:

   ```
   # rm /usr/net/servers/lanman/datafiles/registry*
   ```

2. Reinitialize the registry to set all the registry values entries to their default values by entering the following command:

   ```
   # regload
   ```

See `regcheck`(8) and `regload`(8) for more information on these commands.

8.2.3.9 Verify the Parameters in the lanman.ini File

Default settings are used for the parameters in the `lanman.ini` file; however, you can change the default values.

To display a list of the parameters in the `lanman.ini` file and their settings, enter:

```
# srvconfig -p | more
```

See `srvconfig`(8) for more information on the `srvconfig` command and Appendix C for more information on the `lanman.ini` file.

8.2.3.10 Determine If the User Account Database is Corrupt

To determine whether the user account database is corrupt, enter:

```
# samcheck -s
```

A message is displayed that reports the condition of the user account database.

If a message indicates that the user account database is corrupt, enter the following command to repair the database:

```
# samcheck -r
```

See `samcheck`(8) for more information on the `samcheck` command.

8.2.3.11 Determine If the ACL Database Is Corrupt

Enter the following command to verify if the ACL database is corrupt:

```
# acladm -C
```

If the file is corrupt, then the command prompts you before repairing the file.

See `acladm`(8) for more information on the `acladm` command.

8.3 Solving Common Share Problems

This section describes some common problems with shared resources and recommends resolutions.

8.3.1 User Cannot Connect to a Share

If a user cannot connect to a share, ensure that:

- The share exists.
- The ASU server has not exceeded the maximum number of clients.

8.3.1.1 Verify That the Share Exists

To display a list of disk share names, enter:

```
# net view \\ASU_servername
```

If the disk share name that the user is trying to connect to does not display, it does not exist. Use the `net share` command to create the share if necessary. See Chapter 4 for more information on creating disk shares.

8.3.1.2 Determine the Maximum Number of Clients

The ASU server will only service as many clients as there are ASU licenses. The maximum number of clients is defined by the `maxclients` parameter in the server `lanman.ini` file.

To display the value assigned to the `maxclients` parameter, enter:

```
# srvconfig -g 'server,maxclients'
```

Use the `asustat -n` command to view the number of clients connected. If there are fewer clients than the value of the `maxclients` parameter, but clients still cannot connect, use the `asustat -L` command to view the current number of available ASU licenses. If all the ASU licenses are in use, no other clients can connect to the ASU server.

8.3.2 User Cannot Access a File

If a user cannot access a file, check:

- The user's Windows NT share, Windows NTFS, and Tru64 UNIX permissions for the file
- For open locks
- For insufficient `UStructs`

8.3.2.1 Viewing and Changing Windows NT Share Permissions

To view Windows NT share permissions you can use:

- The Server Manager Utility
- The `net perms` command

To use the `net perms` command to display the Windows NT share permissions for a disk share called project, enter:

```
# net perms \\project
```

To set the project Windows NT disk share permission to read for a user named peter, enter:

```
# net perms \\project /grant peter:read
```

Note

By default, all users have permission to connect to a share. Access to directories and files in the share is normally controlled through NTFS permissions. See Section 8.3.2.2 for more information

8.3.2.2 Viewing and Changing Windows NTFS Permissions

To set NTFS permission you can use:

- The Windows NT Explorer or File Manager
- The `net perms` command

To use the `net perms` command to view Windows NTFS permissions for the share called project, enter:

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

To use the `net perms` command to grant the team1 group the Windows NTFS write permission to the project disk share, enter the following command. Press Enter after you type the entire command.

```
# net perms c:/usr/net/servers/lanman/shares/project /grant team1:w
```

8.3.2.3 Checking Tru64 UNIX Permissions

You use standard Tru64 UNIX commands, such as `chown`, `chgrp`, and `chmod` to set ownership and permissions for directories and files that are associated with a disk share.

To set the permission for the world to read the `project` directory, enter:

```
# chmod 774 /usr/net/servers/lanman/shares/project
```

See `chown`(8), `chgrp`(8), and `chmod`(8) for more information on these commands.

8.3.2.4 Check for Open Locks

An application program error can sometimes leave a file open with a lock on it. A file in this state is unavailable to other users.

To correct the access problem, you can close these files by using:

- The `net session` command

  To display current sessions, enter:

  ```
  # net session
  ```

  To delete a session with a client called client1, enter:

  ```
  # net session \\client1 /delete
  ```

- The Server Manager

  Follow these steps to close a file using the Server Manager:

  1. Start the Server Manager.
  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 the name of the server in the Domain: field or browse for the server in the Select Domain: section.
  4. Double click 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.

8.3.2.5 Check for Insufficient UStructs

Follow these steps to check if there is an insufficient number of UStructs:

1. Enter the following command to display the maximum number of UStructs. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   AdvancedServer/ProcessParameters NumUStructs
   ```

2. Enter the following command to view the number of open files and file locks:

   ```
   # asustat -n
   ```

The total number of open files and file locks cannot exceed the number of UStructs. See Section 7.6 if you need to increase the number of UStructs.

8.4 Solving Common Browsing Problems

This section describes some of the common problems relating to the Computer Browser service and recommends resolutions.

8.4.1 Browser Does Not Display ASU Shares

If ASU shares do not display in browsers, restart the browser service by entering the following commands:

```
# net stop browser
```

```
# net start browser
```

8.4.2 LAN Manager Servers Do Not Show the ASU Server

If the output displayed by the `net view` command does not show the ASU server in the domain, edit the ASU registry and enable the `LmAnnounce` entry. Enabling this entry configures the ASU server to broadcast LAN Manager-style server announcements.

Follow these steps to use the `regconfig` registry editor to enable the ASU server to broadcast LAN Manager-style server announcements. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Enable the `LmAnnounce` entry by entering the following command:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   LanmanServer/Parameters LmAnnounce REG_DWORD 1
   ```

2. Restart the ASU server by entering the following commands:

```
# net stop server
# net start server
```

8.4.3 BDCs Browse Lists Do Not Show All Controllers

It can take as long as 12 minutes for the system to update the browse list. You can edit the ASU registry on the BDC to change the value of the `BackupUpdate` parameter to change the amount of time (in seconds) between updates. Note that increasing the browse update time generates increased network traffic.

Follow these steps to use the `regconfig` registry editor to decrease the time that it takes to update the browse list. The backslash (\ ) at the end of a line indicates continuation. Enter the entire command, then press the Enter key.

1. Decrease the time set in the `BackupUpdate` entry. To decrease the value of the `BackupUpdate` entry to 10 minutes (600 seconds), enter:

   ```
   # regconfig SYSTEM/CurrentControlSet/Services/\
   Browser/Parameters BackupUpdate REG_DWORD 600
   ```

2. Restart the ASU server by entering the following commands:

   ```
   # net stop server
   # net start server
   ```

8.5 Solving Common Printing Problems

This section describes some of the common problems relating to shared printer queues and recommends resolutions.

8.5.1 Client Printers and Jobs Do Not Display

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.

8.5.2 Printer Name Is Invalid

Ensure that the printer name does not contain any spaces, and that the share name is the same as the printer name.

8.5.3 No Separator Page

The default separator page is the Tru64 UNIX `LP` subsystem banner page. You can configure the ASU server to use a custom separator page by entering the `net print` command with the `separator:pathname` option.

For more information on the `net print` command, enter:

```
# net help print /options | more
```

8.5.4 Print Jobs Do Not Print

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 is not paused, held, or is in error. If it is paused or held, continue or restart the printer or print queue.
- You can print from the Tru64 UNIX system console. If you cannot print, consult your Tru64 UNIX documentation.

8.5.5 Characters Print Incorrectly

Refer to your printer manual to set the printer for no parity.

8.5.6 Trouble Printing to a Shared Client Printer

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.

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.

8.5.7 Keyboard Locks When Printing

Your keyboard may lock for a few seconds if you are using an application on a client to which a shared client printer is connected and a print job is in progress. This hesitation at the keyboard is normal under these circumstances, especially when the printer is connected to a serial port.

A

Sample ASU Installation and Configuration

This appendix shows output from of a sample ASU installation procedure and configuration procedure.

Sample Installation

The following example shows the output from a sample ASU installation procedure on a system running the Tru64 UNIX Version 5.0 or higher operating system software. In this example the base server, transports, and reference pages subsets are installed.

```
# setld -l .

The subsets listed below are optional:

     There may be more optional subsets than can be presented on a single
     screen. If this is the case, you can choose subsets screen by screen
     or all at once on the last screen. All of the choices you make will
     be collected for your confirmation before any subsets are installed.

 - Advanced Server for UNIX Core Components:
     1) Base Server
     2) Transports

 - Advanced Server for UNIX Optional Components:
     3) Client-based Server Administration (Nexus) Tools
     4) Man Pages
     5) NT Authentication for UNIX

 - Localized Advanced Server for UNIX Components:
     6) Client-based Server Administration (Nexus) Tools (Japanese)
     7) Man Pages (Japanese)

     8) ALL of the above
     9) CANCEL selections and redisplay menus
    10) EXIT without installing any subsets

Add to your choices, choose an overriding action or
press RETURN to confirm previous selections.

Choices (for example, 1 2 4-6):  1-2 4

You are installing the following optional subsets:

 - Advanced Server for UNIX Core Components:
        Base Server
        Transports

 - Advanced Server for UNIX Optional Components:
        Man Pages
```

```
Is this correct? (y/n): y

checking file system space required to install selected subsets:

File system space checked OK.

3 subset(s) will be installed.

Loading 1 of 3 subset(s)....

Transports
   Copying from . (disk)
   Verifying

Loading 2 of 3 subset(s)....

Base Server
   Copying from . (disk)
        Working....Fri Jan 14 09:07:18 EST 2000
   Verifying

Loading 3 of 3 subset(s)....

Man Pages

Copying from . (disk)
   Verifying

3 of 3 subset(s) installed successfully.


Configuring "Transports " (ASUTRAN500)

Configuring "Base Server " (ASUBASE500)

*********************************************

   When installation has completed, please run
   /usr/sbin/asusetup to configure your server.
*********************************************

Configuring "Man Pages " (ASUMANPAGE500)
```

Sample Configuration

The following example shows the output from a sample ASU configuration procedure. In this example default values are used and the ASU server is configured to use one extra listen name.

```
# asusetup

        Advanced Server for UNIX Configuration Utility

Administrators can configure the Advanced Server software by using the
default configuration values that are detected from a previous Advanced
Server configuration.  If no previous Advanced Server configuration is
detected then the default values are determined by this utility. In
either case, administrators can choose not to use the default values and
customize the Advanced Server configuration by interactively supplying
Advanced Server configuration values.
```

```
The following default configuration can be used:

   Transports : NetBIOS over TCP/IP (controller ’tu0’)
                NetBEUI (controller ’tu0’)
   Server Name:   server1
   Domain Name:   server1.dom
   Domain Role:   Primary
   WAN Support:   enabledns=yes, uselmhosts=yes

Do you want to use this default information [y/n]? y

The Advanced Server for UNIX server will be
configured using this information.

Starting the transports...
Start:  Datalink service controller_01 tu0
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
          /dev/streams/netbeui         32         66
         /dev/streams/netbeuid         32         67
         /dev/streams/nbeadmin         32         68
Microsoft Datalink Driver : Starting dllink ...
Datalink driver attached to tu0 at PPA1
dllink: done - Adapter set
Start:  NetBEUI controller_01 tu0
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
          /dev/streams/netbeui         32         66
         /dev/streams/netbeuid         32         67
         /dev/streams/nbeadmin         32         68
Microsoft NetBEUI Driver : Starting nbelink ... done
Start:  TCP/IP NetBIOS controller_01 tu0
Starting the TCP/IP NetBIOS service...
 The following STREAMS devices were created:
                          Name      Major      Minor
                          ----      -----      -----
           /dev/streams/knbtcp         32         69
           /dev/streams/knbadm         32         70
          /dev/streams/knbtcpd         32         71
TCP/IP NetBIOS: Starting knblink ...
   controller(s) configured as ’tu0’
   kernel dynamic cache will be enabled
   lmhosts file use enabled
   DNS support is enabled
   The following 1 DNS subdomains have been specified:
 asu.company.com
   NBNS server use *not* enabled
Successfully configured with controller(s) ’tu0’
TCP/IP NetBIOS name resolver started, pid=21709
TCP/IP NetBIOS service started

Enter the password for Administrator:
Re-enter password:

Creating Advanced Server for UNIX accounts database.

A clean copy of the SAM database has been written.
A copy of the original SAM database may found in:
    /usr/net/servers/lanman/samsave and
    /usr/net/servers/lanman/samsave/X
The SAM database files have the following names:
     /usr/net/servers/lanman/datafiles/Builtin
     /usr/net/servers/lanman/datafiles/Builtin.
     /usr/net/servers/lanman/datafiles/lsa
     /usr/net/servers/lanman/datafiles/lsa.
     /usr/net/servers/lanman/domains/.
Configuring registry...
reg.ini created successfully
Upgrading ...
reg.ini upgraded successfully
Checking existing registry file...
Existing registry file is OK...
processed 935 lines...
Registry file created successfully

loading /usr/net/servers/lanman/regfiles/perf009.regadm
loading /usr/net/servers/lanman/regfiles/users.regadm
loading /usr/net/servers/lanman/regfiles/machine.regadm
load registry initialization scripts...
registry load complete.

The ASU server currently listens for, and responds to,
messages sent to these network names:
 listenname      : server1
 ExtraListenNames:

You can define Extra Listen Names for the server to listen for
via the Registry parameter ExtraListenNames.

Do you want to modify the ExtraListenNames entry [y/n]? y
Enter the Extra Listen Names to add to the list.
 Press RETURN to terminate the list.

Enter an Extra Listen Name to add: server2

Enter an Extra Listen Name to add:

 ExtraListenNames:
                   server2

Enter the Extra Listen Names to remove from the list.
 Press RETURN to terminate the list.

Enter an Extra Listen Name to remove:

 ExtraListenNames:
                   server2

Are you satisfied with this list of ExtraListenNames [y/n]? y

These changes will take effect the next time
the server is started.

There are a number of registry parameters that affect how the
Advanced Server creates UNIX user accounts, such as UseNIS,
CreateUnixUser, and SpreadUnixHomeDirectory.  If you want to
change the values of these parameters, please use the regconfig
utility to change the parameters now before starting the server.
Please see the installation guide for further information.

Start the Advanced Server for UNIX [y/n]? y
The SERVER service is starting..................
The SERVER service was started successfully.
```

B

ASU Registry Entries

The value entries for which the ASU server software assigns default values are located in the following registry paths:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

   \AdvancedServer
   \Alerter
   \Browser
   \EventLog
   \LanmanServer
   \Netlogon
   \Replicator
   \UPS
```

B.1 AdvancedServer

The AdvancedServer subkey contains the following subkeys for which default value entries are set:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ad-
vancedServer

   \AlertParameters
   \FileServiceParameters
   \NetAdminParameters
   \Parameters
   \ProcessParameters
   \RpcParameters
   \ShareParameters
   \UnixAuditParameters
   \UserServiceParameters
```

B.1.1 AlertParameters

The registry path that contains value entries for the AlertParameters subkey is:

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

The following AlertParameter value entries are set by default:

`AlertAdminOnLicenseOverflow` `REG_DWORD` `0 or 1`

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

Default: 0 (message is not sent)

`AlertUserOnLicenseOverflow` `REG_DWORD` `0 or 1`

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

Default: 0 (message is not sent)

B.1.2 FileServiceParameters

The registry path that contains value entries for the FileServiceParameters subkey is:

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

The following FileServiceParameters value entries are set by default:

`AclCacheSize` `REG_DWORD` `0 - 100`

Specifies the number of entries in the ACL cache, which tracks the results of recent access checks performed on ASU 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 ASU server handles file opens in read-only compatibility mode as follows:

0 - Keeps the compatibility mode.

1 - Translates to read-only/DenyWrite mode for files with special extensions (for example, `bat`, `com`, and `exe`) specified by the value of the `EnableSoftFileExtensions` entry.

2 - Translates 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` entry is set to 1.

Default: `bat`, `com`, `exe`, `dll`, and `cmd`

`ForceDirectoryAcl` REG_DWORD 0 or 1

Determines whether the ASU server creates an ACL for a newly created directory if the client computer does not provide an explicit ACL. If an ACL is not created, one is inherited from its parent directory whenever it is needed.

Default: 1 (create new ACL)

`ForceFileAcl` REG_DWORD 0 or 1

Determines whether the ASU server creates an ACL for the client computer if an explicit ACL did not provide a newly created file. If an ACL is not created, one is inherited from its parent directory whenever it is needed.

Default: 0 (will not create new ACL)

`ForceFileFlush` REG_DWORD 0 or 1

Specifies whether to force a Tru64 UNIX `fsync`(2) system call when an SMB flush request is received. Not forcing an `fsync`(2) system call improves file server performance; files are periodically flushed to disk by the Tru64 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 (`RWXDPO`) control entry for the user on the user's Tru64 UNIX home directory when their domain user account is created.

Default: 1 (add access control entry for user)

`IgnoreUnixPermissions` REG_DWORD 0 or 1

Specifies to ignore Tru64 UNIX permissions and enforce only Windows NT and Windows NTFS permissions when domain users access Tru64 UNIX files and directories.

Note the following when the `IgnoreUnixPermissions` value entry is enabled (set to 1):

- The `nfsshare` utility will not automatically create disk shares.
- Users can link the `root` directory to their home directory and manipulate files. When disabled, users can link the `root` directory to their home directory, however, they cannot manipulate files.
- If you enable the `UnixQuotas` registry value entry, the ASU server checks Tru64 UNIX permissions even if you enable the `IgnoreUnixPermissions` value entry.

Default: 0 (enforce Tru64 UNIX permissions)

`MappingSeparator` REG_SZ *Character string of 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 Tru64 UNIX to Windows NT. The default is a tilde (~), which is the same as in the Tru64 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 called `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` entry is replaced by the default value.

Default: ~

`MaxEASize` `REG_DWORD` `1 - infinity`

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

Default: 4096 bytes

`MaxFileSizeInKB` `REG_DWORD` `100 - infinity`

The maximum file size, in KB, that a user can create on the ASU server.

Default: -1

`MaxZeroFillinInKB` `REG_DWORD` `0 - infinity`

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

Default: 50000

`MemoryMapFiles` `REG_DWORD` `0 or 1`

Specifies whether the ASU server uses the Tru64 UNIX `mmap` system call to memory map file data into the ASU 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. Mixed-case support allows clients to access file names containing uppercase characters on the Tru64 UNIX system. Enabling mixed-case support may negatively effect ASU server 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 ASU server :

0 - Specifies that there is no name space mapping enabled.

1 - Specifies that only Tru64 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 Tru64 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 Tru64 UNIX system to 8.3 and Tru64 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 ASU server waits for acknowledgment from a client of an `oplock` broken notification.

Default: 30 seconds

`ReportNTFS` `REG_DWORD` `0 or 1`

Specifies whether to report share Tru64 UNIX system volumes as NTFS or the Tru64 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 Tru64 UNIX user ID) Enabling this entry requires the -root=0 option in the /etc/exports file for the directory being exported, for example: `/usr/users -root=0`

`ShareNFSExports` `REG_DWORD` `0 or 1`

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

Default: 1 (enable sharing)

`SyncAclFileOnWrite` `REG_DWORD` `0 or 1`

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

Default: 0 (ACL changes are not forced)

`SyncNFSExports` `REG_DWORD` `0 or 1`

Specifies whether the ASU server will synchronize NFS exports with disk shares when the ASU 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 created from the NFS exports.

Default: 1 (synchronize when the ASU server starts)

`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 entry 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 entry effects only Tru64 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 alphanumeric 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` entry to a value less than 3, unless the preservation of a longer file name prefix outweighs possible name collision problems.

Default: 3 characters

`UnixAclSupport` `REG_DWORD` `0 or 1`

Allows the ASU server to use Tru64 ACLs in addition to NTFS user and group permissions.

This entry is supported only on systems running the Tru64 UNIX Version 5.0A and higher software.

Default: 0 (do not use Tru64 UNIX ACLs)

`UnixCloseCount` `REG_DWORD` `1 - 20`

The number of least recently accessed open files that the ASU server closes transparently to avoid reaching the Tru64 UNIX system's per-process limit. the ASU 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 ASU server allows clients to write to Tru64 UNIX system directories without write permission. Microsoft client software treats the read-only attribute as advisory and does not limit the behavior of directories.

The Tru64 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 ASU server (as determined by checking group memberships of the directory).

2 - Ignores Tru64 UNIX system directory permissions.

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

`UnixDirectoryPerms` `REG_DWORD` `0 - 511`

Specifies the Tru64 UNIX system permissions for newly created directories.

Default: 0755 octal (493 decimal). If you plan to enable the `UseUnixGroups` entry, then change the `UnixDirectoryPerms` value to 0775.

Set the value to 0 (zero) to specify that directories created in ASU shares inherit the Tru64 UNIX permissions from the parent directory.

The `UnixDirectoryCheck` registry entry, which can be set to bypass Tru64 UNIX security checking, will not affect the inheritence of Tru64 UNIX permissions.

`UnixFilePerms` `REG_DWORD` `0 - 4095`

Specifies the Tru64 UNIX system permissions for newly created files. If you are upgrading and previously set the `UnixFilePerms` entry, then it is not changed from what you set.

Default: 0644 octal (420 decimal).

Set the value to 0 (zero) to specify that files created in ASU shares inherit the Tru64 UNIX permissions from the parent directory.

The `UnixDirectoryCheck` registry entry, which can be set to bypass Tru64 UNIX security checking, will not affect the inheritence of Tru64 UNIX permissions.

`UnixQuotas` `REG_DWORD` `0 or 1`

Specifies whether the ASU server provides Tru64 UNIX system disk quota support.

This support ensures that creating or writing to a file is performed under the Tru64 UNIX system UID of the Tru64 UNIX system user to which the domain 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, AdvFS, 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 ASU server tries to set Tru64 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` entry is zero, this feature has no effect on the ASU server. When this value entry is enabled make sure that the `rpc.lockd` and `rpc.statd` daemons are running on the NFS server or on the Tru64 UNIX system on which the ASU server is running or it is possible for the ASU server to stall or lose data.

Default: 1 (set locks)

`UseOplocks` `REG_DWORD` `0 or 1`

Specifies whether the ASU 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 ASU server uses the Tru64 UNIX group field to store MS-DOS file and directory attributes. Enabling this entry enhances security by enforcing Tru64 UNIX group permissions, and causes the MS-DOS Archive, Hidden, and System attributes to be ignored by the ASU server.

Default: 0 (Use the Tru64 UNIX group field to store DOS attributes)

`UseUnixLocks` `REG_DWORD` `0, 1, or 2`

Specifies whether record locks created by clients are reflected in the Tru64 UNIX file system.

0 - Specifies that no locks are reflected in Tru64 UNIX file system.

1 - Specifies that locks are reflected in Tru64 UNIX file system.

2 - Specifies that the ASU server opens files with `O_NONBLOCK` set, which causes reads and writes to return with an appropriate error if the file is locked by another process.

Default: 1

The ASU server does not enforce byte-range locking across TruCluster nodes when the value of the `UseUnixLocks` entry is set to zero. Therefore, it is not recommend that you set the value to zero when the ASU server is configured in multi mode in a TruCluster cluster.

`WriteBehind` `REG_DWORD` `0 or 1`

Specifies whether the Tru64 UNIX system performs writes before or after the ASU server responds to the client. If the Tru64 UNIX system performs writes before the ASU server responds to the client, then the ASU server can report disk full errors to clients. The ASU server appears to be slower because the response is delayed. If the Tru64 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)

B.1.3 NetAdminParameters

The registry path that contains value entries for NetAdminParameters subkey is:

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

The following NetAdminParameters value entries are set by default:

`NetAdminGroupName`	REG_SZ	*`Character string`*

Specifies the Tru64 UNIX system group name assigned to the network administration `\\servername /c` command.

Default: `DOS----`

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

Specifies the Tru64 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 Tru64 UNIX system user account name assigned to a process executed by the network administration `\\servername /c` command.

Default: `lmxadmin`

B.1.4 Parameters

The registry path that contains value entries for the Parameters subkey is:

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

The following Parameters value entries are set by default:

`BigEndianLuidCompatibilityMode`	REG_DWORD	`0 or 1`

This value entry is ignored because Alpha hardware is little endian machine type.

`CheckPrintQueueInMinutes`	REG_DWORD	`1 - infinity`

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

Default: 10 minutes

`DefaultPrintQueue`	REG_SZ	*`Character string`*

Specifies the Tru64 UNIX queue name that displays for locally submitted jobs when the `ShowUnixQueues` entry is set to zero (0).

Default: `OSFqueue`

`DeletedPrintJobTimeOnQ` `REG_DWORD` `0 - infinity`

Specifies the time, in seconds, to show a job on a queue after it was deleted.

Default: 180 seconds

`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)

`ExtraListenNames` `MULTI_SZ` `list`

Specifies listen names for the ASU server. A listen name is a unique name assigned to the ASU server to which it responds on the network. Users can use any of the assigned listen names when connecting to the ASU server. For example, if an ASU server is assigned a listen name of `server1` and the extra listen names of `server2` or `server3`, users can specify `\\server1`, `\\server2`, or `\\server3` when connecting to its shares.

`HideClusterMember` `REG_DWORD` `0 or 1`

Specifies whether or not TruCluster members will be displayed in the network neighborhood and other browse functions. The `HideClusterMember` parameter does not effect whether or not the cluster alias will be displayed in the network neighborhood and in other browse functions.

Default: 0 (do not hide TruCluster members)

`MaxIpcTryCount` `REG_DWORD` `1 - infinity`

Specifies the number of `read()` system calls after which the ASU server checks to see if other work can be doner. There is a considerable amount of interprocess communication (IPC) between server processes. The ASU 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 ASU 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 ASU server from waiting indefinitely for a message to be delivered.

Default: 90 seconds

`MaxMessageSize` `REG_DWORD` `1024 - infinity`

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

Default: 65535 bytes

`MaxPrintJobs`	`REG_DWORD`	`1000 to 1000000 (one million)`	Specifies the maximum number of print jobs allowed in any class queue created by the ASU server. Default: 1000 print jobs
`MaxPrintJobName`	`REG_DWORD`	`0 to 8191`	Specifies the maximum number of characters for a print job name. Characters that exceed the value of the `MaxPrintJobName` parameter are truncated. Default: 0 characters (do not truncate print job names)
`MaxServiceWaitTime`	`REG_DWORD`	`5 - infinity`	Specifies the amount of time, in seconds, that the ASU 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 V*n.n* for UNIX
`NativeOS`	`REG_SZ`	*Character string*	Specifies an additional field in the session setup request/response. This field is generated at run time. Default: `Tru64 UNIX V`*n.n* `(Rev.` *nnnn*`)`
`SendByeMessage`	`REG_DWORD`	`0 or 1`	Specifies whether the ASU 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 ASU server has stopped. Default: 1 (send a message)
`ShowUnixQueues`	`REG_DWORD`	`0 or 1`	Specifies whether the ASU server shows Tru64 UNIX queues to clients. Default: 0 (do not show Tru64 UNIX queues)
`SizeGcBufferPoolInKB`	`REG_DWORD`	`1 - infinity`	Specifies the buffer size, in KB, allocated for each server process for client files. Default: 200 KB
`TestBits`	`REG_DWORD`	`0 - infinity`	Not currently used.

`UseClusterLicensing` `REG_DWORD` `0 or 1`

Specifies whether or not the ASU server uses cluster-wide licensing when configured in a TruCluster Server multi-instance cluster.

Default: 0 (do not use cluster-wide licensing)

B.1.5 ProcessParameters

The registry path that contains value entries for the ProcessParameters subkey is:

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

The following ProcessParameters value entries are set by default:

`CoreOk` `REG_DWORD` `0 or 1`

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

Default: 1 (create core file)

`KeepSpareServer` `REG_DWORD` `0 or 1`

Specifies whether the ASU server should have a spare `lmx.srv` process available for another client. New client connections are faster when 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 ASU server sleeps when a shared memory lock contention occurs. The ASU server retries busy locks at intervals specified by this key until the length of time specified in the value of the `MaxLockTimeInSeconds` entry elapses.

Default: 10 milliseconds

`MaxLockTimeInSeconds` `REG_DWORD` `5 - infinity`

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

Default: 60 seconds

`MaxSmbWorkerTasks` `REG_DWORD` `1 - 100`

Specifies the maximum number `SMBWORKER` tasks that can be created in any one `lmx.srv` process, and therefore the maximum number of SMBs that can be processed simultaneously by an `lmx.srv` process. Increasing this value is not recommended because throughput gains will be small and the risk of a stack overflow is increased.

Default: 8

`MaxVCPerProc` `REG_DWORD` `0 - 101`

Specifies the maximum number of virtual circuits that each `lmx.srv` process andles. This limit normally is calculated by the ASU server using the value of the `CDistribution` entry and the value of the `maxclients` parameter in the `lanman.ini` file. If the value of this key is nonzero, its value is used instead of the calculated value. If the `MinVCPerProc` value is larger than the `MaxVCPerProc` value, then `MinVCPerProc` is lowered to the value of `MaxVCPerProc`.

The `maxserverprocs` parameter in the `[server]` section of the `lanman.ini` file overrides the value for the `MaxVCPerProc` registry entry.

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

`MaxVCs` `REG_DWORD`

Specifies the maximum number of virtual circuits that can be established to the ASU 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: 1 worker task

`MinVCPerProc` `REG_DWORD`

Specifies the minimum number of virtual circuits that each `lmx.srv` process should handle before a new server process is created. If this value is 0, its value is calculated from the value of the `VCDistribution` registry value entry and the value of the `maxclient` parameter in the `lanman.ini` file.

Default: 1

`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 ASU 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.

Reasonable values are 128, 256, 512, 1024, 2048, or 4096. There should be about one hash bucket for every 8 to 15 `ustructs`.

Default: 128 buckets

`NumSERVER_SESSION` `REG_DWORD` `5 - infinity`

Limits the number of servers and Windows NT clients that can authenticate with the ASU server . This value should be large because it limits the number of Windows NT clients that can contact the ASU server. On a PDC, 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. A guideline is to allow five (5) open file and record locks per client if database applications are not being used.

Default: 1000 open files and record locks. This value is adequate for the `maxclients` key default value of 200.

`SpareServerTime` `REG_DWORD` `0 - infinity`

Specifies the minimum interval, in seconds, that a spare `lmx.srv` process is allowed to stay around 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 ASU server)

`VCDistribution` `REG_MULTI_SZ` `List`

Specifies the distribution of virtual circuits or sessions over `lmx.srv` processes. The architecture of the ASU server allows multiple sessions to be served by each `lmx.srv` process on the Tru64 UNIX system. The ASU server determines if a new session should be serviced by 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 services; the third number specifies the maximum number of virtual circuits each process should support. The value for the `VCDistribution` registry entry can be overridden by the `maxserverprocs` parameter in the `[server]` section of the `lanman.ini` file.

Default:

```
1,2,12
20,2,20
35,2,24
35,2,24
50,3,28
85,4,28
100,5,32
130,6,36
180,8,42
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

B.1.6 RpcParameters

The registry path that contains value entries for the RpcParameters subkey is:

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

The following RpcParameters value entries are set by default:

`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: 100 sessions

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

Specifies the maximum number of open server service 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

B.1.7 ShareParameters

The registry path that contains value entries for the ShareParameters subkey is:

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

The following ShareParameters value entries are set by default:

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

Default: 1 (create new directory)

`ShareReadCount` `REG_DWORD` `1 - infinity`

Specifies the number of share entries to read during share database operations.

Setting this parameter to a value greater than 1 causes the ASU server to read ahead `SHAREENTRY` structures from the share database.

Default: 25 share entries

B.1.8 UnixAuditParameters

The registry path that contains value entries for the UnixAuditParameters subkey is:

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

The following UnixAuditParameters value entries are set by default:

`Access` `REG_DWORD` `0 or 1`

Audits determining the accessibility of a file.
Default: 1

`chdir` `REG_DWORD` `0 or 1`

Audits changing the current directory.
Default: 1

`chown` `REG_DWORD` `0 or 1`

Audits changing the owner of files and directories.
Default: 1

`close` `REG_DWORD` `0 or 1`

Audits closing the file associated with a file descriptor.
Default: 1

`EnableUnixAuditing` `REG_DWORD` `0 or 1`

Audits specifying whether the ASU server uses Tru64 UNIX auditing, if it was configured into the kernel.
Default: 1

`getuid` `REG_DWORD` `0 or 1`

Audits getting the real or effective user ID.
Default: 1

`login` `REG_DWORD` `0 or 1`

Audits establishing sessions to the ASU server.
Default: 1

`open` `REG_DWORD` `0 or 1`

Audits opening a file for reading or writing.
Default: 1

`setuid` `REG_DWORD` `0 or 1`

Audits setting the user ID.
Default: 1

`stat` `REG_DWORD` `0 or 1`

Audits displaying information about a file.
Default: 1

B.1.9 UserServiceParameters

The registry path that contains value entries for the UserServiceParameters subkey is:

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

The following UserServiceParameters value entries are set by default:

```
CreatePersonalShare             REG_DWORD         0 or 1
```

Specifies whether or not the ASU server will automatically create a personal disk share when you create a Tru64 UNIX user account or map a domain user account to a Tru64 UNIX user account, delete a personal disk share when you delete its associated domain user account, and rename a personal disk share when you rename its associated domain user account.

The path for the personal disk share will be the Tru64 UNIX home directory of the user; however, if the Tru64 UNIX home directory does not exist or if there is an existing share of the same name, the ASU server will not create the personal share.

The ASU server creates a personal disk share as a hidden disk share. A hidden disk share has a name that ends with a dollar sign ($) and does not display when browsing the ASU server. For example, creating a Tru64 UNIX user account named `peter` will automatically create a personal disk share called `peter$` mapped to peter’s Tru64 UNIX home directory. A user can connect to a hidden disk share by appending the dollar sign to the share name.

Default: 0 (do not create, delete, or rename a personal share). If you enable the `CreatePersonalShare` entry, you must also enable the `CreateUnixUser` entry, which is enabled by default.

```
CreateUnixHomeDirectory         REG_DWORD         0 or 1
```

Specifies whether or not the ASU server creates a user’s Tru64 UNIX home directory when it creates a Tru64 UNIX user account.

Not creating Tru64 UNIX home directories is useful if you want to create Tru64 UNIX user accounts to assign files and directories the proper Tru64 UNIX ownership, but do not want users to log directly in to the system.

Default: 1 (create a Tru64 UNIX home directory)

```
CreateUnixUser                  REG_DWORD         0 or 1
```

Specifies whether to automatically create and assign a Tru64 UNIX user account to each new domain user account if a corresponding Tru64 UNIX account does not exist. The value of this entry must be set to 1 on each server on which Tru64 UNIX system accounts will be created.

The Tru64 UNIX account is created by default with a `/bin/sh` login shell, which enables the user to have interactive sessions to the Tru64 UNIX server by using a terminal emulator. The password for the Tru64 UNIX user account must be set by the root user before the user can log in.

While domain user account names can contain up to 20 characters, the maximum number of characters for a Tru64 UNIX user account is 8. If the domain user account name exceeds 8 characters, the Tru64 UNIX user account is created using the first 6 characters, and the last 2 characters are substituted with random characters. The user uses this new, shortened name to log in to the Tru64 UNIX server.

For example, if an domain user account name is `longusername`, then the Tru64 UNIX account might be `longush3`. The user uses this name to log in to the Tru64 UNIX server.

If `CreateUnixUser` is set to 0, then all new domain user accounts are mapped to the Tru64 UNIX system `lmworld` account, unless you enable the `MapExistingUnixUser` entry.

Default: 1 (create Tru64 UNIX user accounts)

`DeleteUnixHomeDirectory` `REG_DWORD` `0 or 1`

Whether or not when the ASU server deletes a Tru64 UNIX account, it will also delete the home directory of the account. Note that the ASU server only deletes Tru64 UNIX accounts that it created.

Default: 0 (do not delete home directories)

`Exclude` `REG_SZ` *`Character string`*

Specifies a range of the existing Tru64 UNIX user IDs that are excluded from being assigned to domain user accounts. If a domain user account is created with a name that matches an existing Tru64 UNIX user account whose ID is contained in the exclude list, a new Tru64 UNIX system user account is generated and assigned to the domain user account. This ensures that certain existing Tru64 UNIX user accounts are never automatically assigned to newly created domain user accounts, even if the `ForceUniqueUnixUserAccount` entry is set to zero (0).

Default: 0 - 100

`ForceUniqueUnixUserAccount` `REG_DWORD` `0 or 1`

Specifies whether to automatically assign an existing Tru64 UNIX system user account to a newly created domain user account. If enabled (set to 1), the system does not assign existing Tru64 UNIX user accounts. Instead, new Tru64 UNIX user accounts are created and assigned to the domain user accounts when they are created.

Default: 0 (existing Tru64 UNIX user accounts can be assigned)

`GroupUpdateTime` `REG_DWORD` `0 - infinity`

Specifies the interval, in seconds, at which the ASU server checks the Tru64 UNIX system file `/etc/group` for changes.

Default: 3600 seconds (1 hour)

`MapExistingUnixUser` `REG_DWORD` `0 or 1`

If `MapExistingUnixUser` is enabled, then when the ASU server creates or replicates a domain user account, it attempts to map the domain user account to an existing Tru64 UNIX account of the same name in lowercase letters. This automatic mapping is not done for special accounts, such as Administrator or Guest, nor for Tru64 UNIX accounts with UIDs in the Exclude range (by default, 0 to 100).

Default: 0 (Do not map new domain user accounts to Tru64 UNIX user accounts)

`MinUnixUid` `REG_DWORD` `0 - infinity`

Specifies the smallest Tru64 UNIX user identifier (UID) that the ASU server uses when creating new Tru64 UNIX accounts. The default Tru64 UNIX UID for an account is the value of the `MinUnixUid` plus the Relative ID (RID) of the corresponding domain user account.

Default: 32767 (if set to 0, the lowest possible generated Tru64 UNIX UID is 1000 since RIDs start at 1000)

`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 Tru64 UNIX system by using a terminal emulator.

Default: `/bin/sh`

`NISPasswordFile` `REG_SZ` *`Character string`*

Specifies the directory path to the NIS password file.

Default: `/var/yp/src/passwd`

`PreserveCase` `REG_DWORD` `0 or 1`

Specifies whether or not the ASU server creates Tru64 UNIX user account names using the same case that you enter to create domain user accounts.

Default: 0 (do not preseve the case; create Tru64 UNIX user accounts using lowercase letters)

`PreserveNumericUserName` `REG_DWORD` `0 or 1`

Specifies whether or not a Tru64 UNIX user account name is created with a pre-pended letter `a` when creating a domain user account whose first character is numeric.

Default: 0 (pre-pend the letter `a` to Tru64 UNIX user account names)

`SpreadUnixHomeDirectory` `REG_DWORD` `0 or 1`

Specifies whether or not the ASU server creates a Tru64 UNIX user home directories in a one-letter subdirectory that corresponds to the first letter of the user name. For example, whether or not the Tru64 UNIX home directory for a user named peter is created as `/usr/users/p/peter`. Enabling this entry allows you to create more than 32,768 user home directories under the `/usr/users` directory path.

Default: 0 (do not spread UNIX home directories)

`SyncUnixHomeDirectory` `REG_DWORD` `0 or 1`

Specifies that if the home directory of domain user account changes, then the home directory of the associated Tru64 UNIX system user account also changes to match it.

Default: 0 (do not synchronize home directories)

`SyncUnixPassword` `REG_DWORD` `0 or 1`

Specifies whether or not Tru64 UNIX user passwords are synchronized to their domain user account password when their domain password is changed.

Default: 0 (do not synchronize passwords)

`UseActiveDirectory` `REG DWORD` `0 or 1`

Whether or not the ASU server uses a Windows 2000 Active Directory to resolve Tru64 UNIX user account information. The ASU server can only use a Windows 2000 Active Directory if the Windows 2000 Single Sign On (SSO) Version 2.0 or higher software is installed on the Windows 2000 system and on the Tru64 UNIX system on which the ASU server is running. See *Security Administration* for more information about the SSO software.

Enabling this entry disables the ASU server from managing (addition, modification, or deletion) Tru64 UNIX user accounts.

Default: 0 (do not use Active Directory to resolve Tru64 UNIX user account information)

`UseNIS` `REG DWORD` `0 or 1`

Whether or not the ASU server uses NIS to create Tru64 UNIX user accounts. Enable this value entry only on a Tru64 UNIX system that is configured as an ASU PDC and a NIS master.

Default: 0 (do not use NIS)

`UserComment` `REG_SZ` *Character string*

The ASU server ignores this key. It is used on other systems to specify the comment for automatically created Tru64 UNIX accounts.

Default: Advanced Server for 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

B.2 Alerter

The registry path that contains value entries for the Alerter subkey is:

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

The following Alerter value entries are set by default:

`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 ASU server's cache of clients.
Default: 120 seconds (2 minutes)

B.3 Browser

The registry path that contains value entries for the Browser subkey is:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Ser-
vices\Browser\Parameters
```

The following Browser value entries are set by default:

`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)

`IsDomainMaster` `REG_SZ` `YES or NO`

Specifies if the ASU server is the preferred master browser, which is the same as a BDC, except that browser elections are biased when the `IsDomainMasterBrowser` (Windows NT 3.51 or earlier) registry value or the `IsDomainMaster` (Windows NT 4.0 or Windows 2000) registry value is set to `YES`.

Default: NO

`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)

B.4 EventLog

The EventLog subkey contains subkeys for the Application, Security, and System. These subkeys contain log files 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 EventLog subkey can contain 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.

The following EventLog value entries are set by default:

`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 K bytes`

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

Default: 524288 (512 KB)

`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.

B.5 LanmanServer

The registry path that contains value entries for the LanmanServer subkey is:

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

The following LanmanServer value entries are set by default:

`AccessAlert` `REG_DWORD` `0 - infinity`

Specifies the number of resource access violations that can occur before the ASU 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 ASU server waits before dropping the virtual circuit to an inactive client.

Default: 0 minutes (no automatic disconnect)

`EnableSecuritySignature` `REG_DWORD` `0 or 1`

Specifies whether the ASU server negotiates the use of SMB signing with Windows NT clients.

Default: 0

`ErrorAlert` `REG_DWORD` `0 - infinity`

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

Default: 5 errors

`Hidden` `REG_DWORD` `0 or 1`

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

Default: 0 (server is visible)

`LmAnnounce` `REG_DWORD` `0 or 1`

Specifies whether the ASU 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 ASU server sends an alert to the `alertnames` list.

Default: 5 violations

`MaxMpxCt` `REG_DWORD` `1-100`

Specifies the maximum number of simultaneous requests that a client can have to the ASU server.

Default: 50

`NullSessionShares` `REG_MULTI_SZ` `List`

Contains a list of shares for which access by null sessions is allowed. If a null session attempts to access a share that is not on the list, access is denied except for the `IPC$` share, which must always be accessible over a null session.

Default: An empty string

`RequireSecuritySignature` `REG_DWORD` `0 or 1`

Specifies whether the ASU server requires the use of SMB signing. If enabled, the ASU server refuses connections from clients and servers that do not have `EnableSecuritySignature` entry enabled. SMB signing does not consume any more network bandwidth, however it does use more CPU cycles on the client and servers, which results in slower performance.

Default: 0

`SrvAnnounce` `REG_DWORD` `1 - infinity`

Specifies the interval, in seconds, at which the ASU 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 ASU server sends to announce its presence to the network.

Default: Advanced Server for UNIX Systems

`UserPath` `REG_SZ` *`Character string`*

Specifies the Tru64 UNIX system directory to be used as a default parent directory for home directories of new user accounts.

Default: `c:\usr\users`

B.6 Netlogon

The registry path that contains value entries for the Netlogon subkey is:

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

The following Netlogon value entries are set by default:

`LogonQuery` `REG_DWORD` `60 - infinity`

Specifies the interval, in seconds, at which the ASU 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 PDC 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 ASU 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

`RefusePasswordChange` `REG_DWORD` `0 or 1`

Specifies whether to disable the ability to accept machine account password changes. Machine account password changes normally occur weekly. Disabling automatic machine password changes reduces account replication occurrences and can reduce network traffic between primary and backup domain controllers.

Default: 0 (allow password change)

`RelogonDelay` `REG_DWORD` `1 - infinity`

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

Default: 2 seconds

`Scripts` `REG_EXPAND_SZ` *`Character string`*

Specifies the location of the logon scripts directory.

Default: `%SystemRoot%\usr\net\servers\lanman\shares\ASU\repl\export\scripts`

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

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

Default: 604800 seconds (7 days)

`Update` `REG_DWORD` `0 or 1`

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

Default: 0 (do not synchronize)

B.7 Replicator

The registry path that contains entries for the directory Replicator subkey is:

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

The following Replicator value entries are set by default:

`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 2 (import).

Default: `C:\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.

The replicator will not start if the value of the `GuardTime` entry exceeds the value of the `Interval` entry divided by 2 (`Interval`/2). Using default values should work for most cases.

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:\usr\net\servers\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. Use this entry with the `Pulse` entry. This entry is ignored on import servers.

The replicator will not start if the value of the `GuardTime` entry exceeds the value of the `Interval` entry divided by 2 (`Interval`/2). Using default values should work for most cases.

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 ASU server waits the equivalent of (pulse times the 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 ASU server maintains a master tree to be replicated.

2 Import - The ASU server receives update notices from the export server.

3 Both - The ASU 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: 1 (try to update when user is logged on)

`UnixDirectoryGroup` REG_SZ *Character string*

Specifies the Tru64 UNIX group name for replicated directories.

Default: `DOS----`

`UnixDirectoryOwner` REG_SZ *Character string*

Specifies the Tru64 UNIX user account name for replicated directories.
Default: `lmxadmin`

`UnixFileGroup` `REG_SZ` *`Character string`*

Specifies the Tru64 UNIX group account name for replicated files.
Default: `DOS----`

`UnixFileOwner` `REG_SZ` *`Character string`*

Specifies the Tru64 UNIX user account name for replicated files.
Default: `lmxadmin`

B.8 UPS

The registry path that contains value entries for the Uninterrupted Power Source (UPS) subkey is:

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

The following UPS value entries are set by default:

`IgnoreSIGPWR` `REG_DWORD` `0 or 1`

Specifies whether `UPS` service is enabled.
Default: 1 (disables `UPS` service)

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

Specifies the NetBIOS name to which the ASU 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 ASU 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 ASU server repeats the message sent when it receives a `SIGPWR` signal. A value of 0 indicates to send the message one time only.
Default: 1 minute

C

The lanman.ini File

This appendix describes the `lanman.ini` file parameters that you can modify to improve ASU 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 ASU registry.

When you install the ASU 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 ASU 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/sbin` 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.

C.1 File Syntax

Within each section of the `lanman.ini` file, the following parameters are specified:

- 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 are displayed 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 some 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, for example:

   ```
   # /usr/sbin/srvconfig -p | more
   ```

2. Set parameter values in the `lanman.ini` file, for example:

   ```
   # /usr/sbin/srvconfig -s "section,parameter=value"
   ```

3. Stop and restart the ASU server.

See `srvconfig`(8) for more information on the `srvconfig` command.

C.2 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. The parameters not listed here are for debugging purposes and should not be modified.

C.2.1 server Parameters

The following table lists parameters in the `[server]` section of the `lanman.ini` file.

Parameter	Description, Value, and Default Setting
`listenname`	If set, this is the server's name on the network. If not set, the ASU server may receive client connections from the Tru64 UNIX listener on the Tru64 UNIX system name with a `.serve` extension (such as `liberty.serve`). The Tru64 UNIX system name can be determined using the uname `-n` command. To change the value of the `listenname` parameter, use the `setservername` command. See `setservername`(8) for more information on the `setservername` command. Values: Any name of up to 15 ASCII language characters, including letters, numbers, and the following characters: ! # $ % & ( ) - . ^ _ { } ~ ; Default: none
`maxclients`	Identifies the maximum number of clients that the ASU server can service. You can increase this number, however the ASU server will only service as many clients as there are ASU licenses. Default: 200
`maxserverprocs`	Specifies the maximum number of `lmx.srv` processes that the ASU server creates to service client requests. Each client get its own `lmx.srv` process until the maximum is reached, then the existing `lmx.srv` processes are assigned to additional clients in a rotating fashion. Setting `maxserverprocs` overrides the settings of the registry parameters `MinVCPerProc`, `MaxVCPerProc`, and `VCDistribution`. By default, the `maxserverprocs` value is computed from the `VCDistribution` registry value entry and from the `maxclients` parameter in the `lanman.ini` file.
`srvservices`	The list of keywords for the services that automatically start when the server is started. Because services start in the order in which they appear in the `srvservices` entry, you must ensure that `netlogon` service appears before any services that require it. Default: `alerter, netlogon, browser`

C.2.2 workstation Parameters

The following table lists parameters in the `[workstation]` section of the `lanman.ini` file.

Parameter	**Description, Value, and Default Setting**
`domain`	The name of the domain that includes the server. Values: Any name of up to 15 ASCII language characters, including letters, numbers, and the following characters: ! # $ % & ( ) - . ^ _ { } ~ ; Default: `domain`

C.2.3 lmxserver Parameters

The following table lists parameters in the `[lmxserver]` section of the `lanman.ini` file.

Parameter	**Description, Value, and Default Setting**
`allowtakeunixownership`	Specifies whether or not a domain user account that is a member of either the Domain Admins or Administrators group can take ownership of a UNIX file, regardless of the UNIX ownership and permissions set for the file. The `IgnoreUnixPermissions` registry entry must be disabled (set to 0) for this parameter to be effective. Values: yes or no Default: yes (allow taking ownership)
`anncmailslot`	The name of the mail slot used for periodic server announcements. Values: A pathname of up to a maximum of 256 characters. Default: `\\*\MAILSLOT\LANMAN` Note that backslashes 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 backslash.)
`appsources`	The names of the modules that can write to the application log file. Default: the server initializes the value of this parameter at startup
`blobchecklocks`	Specifies whether or not the ASU server will verify that no read or store is done to a blob file without a corresponding read or write lock. Values: yes or no Default: no

<table>
<tr><th>Parameter</th><th>Description, Value, and Default Setting</th></tr>
<tr><td><code>countbeans</code></td><td>Specifies whether or not transaction statistics are gathered.
Values: yes or no
Default: Yes (gather transaction statistics)</td></tr>
<tr><td><code>country</code></td><td>The country code for server-generated messages.
Values:
<table>
<tr><th>Country</th><th>Code</th><th>Country</th><th>Code</th></tr>
<tr><td>Asia</td><td>099</td><td>Latin America</td><td>003</td></tr>
<tr><td>Australia</td><td>061</td><td>Netherlands</td><td>031</td></tr>
<tr><td>Belgium</td><td>032</td><td>Norway</td><td>047</td></tr>
<tr><td>Canada</td><td>002</td><td>Portugal</td><td>351</td></tr>
<tr><td>Denmark</td><td>045</td><td>Spain</td><td>034</td></tr>
<tr><td>Finland</td><td>358</td><td>Sweden</td><td>046</td></tr>
<tr><td>France</td><td>033</td><td>Switzerland</td><td>041</td></tr>
<tr><td>Germany</td><td>049</td><td>United Kingdom</td><td>044</td></tr>
<tr><td>Italy</td><td>039</td><td>United States</td><td>001</td></tr>
<tr><td>Japan</td><td>081</td><td></td><td></td></tr>
</table>
Default: 001 (United States)</td></tr>
<tr><td><code>debugumask</code></td><td>Controls user access to debug log and crash files. The permissions you set are similar to the octal settings used by the <code>chmod</code> command.
Default: 0600 (Read and Write for the owner)</td></tr>
<tr><td><code>direxists</code></td><td>Specifies the integer access denied error code that the ASU server returns to a client when a client attempts to create a directory that exists.
Values: 5 or 80 (older applications might require 80)
Default: 5</td></tr>
<tr><td><code>enumtimeout</code></td><td>Specifies a timeout period, in seconds, for requests made of the server. The master controller process, <code>lmx.ctrl</code>, polls the server processes, <code>lmx.srv</code>, for enumeration data such as the number of sessions, open files, and so on. If one of the <code>lmx.srv</code> processes fails to respond, the <code>enumtimeout</code> parameter is used to determine how long the controller will wait for a response before moving on to the next server process.
Values: 10 seconds to 1200 seconds
Default: 300 seconds</td></tr>
<tr><td><code>lang</code></td><td>Specifies the character set that the ASU server uses to process client requests.
The ASU server supports the Tru64 UNIX locales listed in the <code>l10n_intro</code> reference page except for Japanese SJIS and Traditional Chinese. See <code>l10n_intro</code>(5) for more information on the supported locales.
Default: en_US.ISO8859-1 (U.S. English)</td></tr>
</table>

Parameter	Description, Value, and Default Setting
`listenextension`	The extension that the Tru64 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 Tru64 UNIX system name or to be the Tru64 UNIX system name with a `.serve` extension in order to avoid name conflicts with the Tru64 UNIX Listener. Values: yes or no Default: no
`listenqlen`	Maximum number of outstanding client connection requests. If the server supports numerous clients that simultaneously attempt to connect to the server and some get refused, raise the value of this parameter. Only applicable if the `listenname= parameter` is used. Values: 1 - unlimited Default: 3 requests
`maxfilesize`	The maximum file size, in KB, that the Tru64 UNIX system redirector will allow a "local Tru64 UNIX user" to create on a local system. Values: 100 - unlimited Default: 20000 KB

Parameter	**Description, Value, and Default Setting**

`msdoscodepage`	Sets the MS-DOS code page that the ASU server uses when responding to a client's request. Set this parameter to correspond to the locale to which the `lang` parameter is set, as described in the following list.
	The first list item is the `lang` parameter, followed by the character set, then the value of the `msdoscodepage` parameter:
	`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, O8859-8, cp862`
	`Korean, C5601, cp949`
	`Korean, ckorean, cp949`
	`Korean, cKR, cp949`
	`Turkish, O8859-9, cp857`
	`Japanese 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 whether or not the ASU server implements message forwarding between clients. It is recommended that you do not implement message forwarding. Values: yes or no Default: no (do not forward messages)
`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 seconds

Parameter	Description, Value, and Default Setting
`network`	The network device names and NetBIOS name-passing type for the network(s) the server should use. Values: Sets of 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 previous two devices. There are three conventions compiled into the server: • 0 = NetBIOS over NetBEUI • 1 = NetBIOS over TCP/IP 4. The name of the transport provider, as returned by the `nlsprovider` system call. (For networks not configured to accept incoming connections through the Tru64 UNIX system Listener program, this can be any arbitrary string.)
`overrideunixprotection`	Allows the deletion of a file by users who are in the same group as the owner of the file, providing that the Tru64 UNIX directory permission allows it. Values: yes or no Default: no (only the owner of a file can delete it)
`prebinduxredir`	Controls the name that the `net` command binds to when it uses the Tru64 UNIX system redirector (`uxredir`). If this parameter is set to yes, the ASU server prebinds a NetBIOS name that is used by all `net` commands. Because this name is prebound, the `net` command does not need to bind its own name, resulting in increased performance. If this parameter is set to no, then each `net` command uses its own unique name resulting in slower performance. Values: yes or no Default: yes (use prebound NetBIOS name)
`rcsdiff`	Enables rcsdiff application specific code. Values: yes or no Default: no (disabled)

Parameter	Description, Value, and Default Setting
`readonlydir`	Specifies whether or not Windows 2000 clients can write into a Tru64 UNIX directory when the ReadOnly attribute is set. Values: yes or no Default: yes (enforce the ReadOnly attribute on Tru64 UNIX directories)
`secsources`	The names of the modules that can write to the security log. Default: The server initializes the value of this parameter at startup.
`sigaltstack`	Processes unexpected signals (such as a segmentation fault) in ASU server processes on an alternate stack. You need to enable this parameter only if you see stack overflow messages for `lmx` processes in the console log. Values: yes or no Default: no (disabled)
`stacksize`	The size of the stack, in bytes, for each task internal to the server. Values:12000 - unlimited Default: 40000 bytes
`syssources`	The names of the modules that can write to the system log. Default: The server initializes the value of this parameter at startup.

C.3 Mappings of lanman.ini Parameters to Registry Entries

The following tables list the parameters in the `lanman.ini` file that were moved to the ASU registry, remained in the `lanman.ini` file, or are obsolete. The parameters that were moved to the ASU registry are listed with their registry entry name.

The `lanman.ini` file parameters are listed according to the sections in which they reside in the file.

C.3.1 server Parameters

The following table lists the status of the `server` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry 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	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

C.3.2 workstation Parameters

The following table lists the status of the `workstation` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
domain	None (lanman.ini file)	

C.3.3 uidrules Parameters

The following table lists the status of the `uidrules` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`exclude`	`AdvancedServer\UserServiceParameters`	`Exclude`
`forceunique`	`AdvancedServer\UserServiceParameters`	`ForceUniqueUnixUserAccount`
`maxuid`	`AdvancedServer\UserServiceParameters`	`MaxUnixUid`
`minuid`	`AdvancedServer\UserServiceParameters`	`MinUnixUid`
`usrcomment`	`AdvancedServer\UserServiceParameters`	`UserComment`

C.3.4 netlogon Parameters

The following table lists the status of the `netlogon` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`logonquery`	`Netlogon\Parameters`	`LogonQuery`
`maxclisess`	`AdvancedServer\Process-Parameters`	`NumCLIENT_SESSION`
`maxquery`	None (obsolete)	
`maxsrvsess`	`AdvancedServer\Process-Parameters`	`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`

C.3.5 lmxserver Parameters

The following table lists the status of the `lmxserver` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry 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`	None (obsolete)	
`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)	
`cpipperms`	None (obsolete)	

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`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`)	

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`lmxsrv`	None (obsolete)	
`lmxtimesource`	None (obsolete)	
`locale`	None (obsolete)	
`locknap`	`AdvancedServer\ProcessParameters`	`LockNapInMSec`
`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`

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`memorymap`	`AdvancedServer\FileServiceParameters`	`MemoryMapFiles`
`minsmbworkers`	`AvancedServer\ProcessParameters`	`MinSmbWorkerTasks`
`minvcperproc`	`AdvancedServer\Process-Parameters`	`MinVCPerProc`
`msdirgroup`	None (obsolete)	
`msdirname`	None (obsolete)	
`msdirowner`	None (obsolete)	
`msdirperms`	None (obsolete)	
`msgforward`	None (`lanman.ini file`)	
`msgheader`	`Alerter\Parameters`	`IncludeMessage-Header`
`nativelm`	`AvancedServer\Parameters`	`NativeLM`
`nativeos`	`AvancedServer\Parameters`	`NativeOS`
`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)	

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
prebinduxredir	None (lanman.ini file)	
qnamelen	AdvancedServer\Parameters	MaxPrintQueueNameLength
qsched	AdvancedServer\Parameters	CheckPrintQueueInMinutes
queuealloc	None (obsolete)	
relmajor	(\SOFTWARE\Microsoft\LanmanServer CurrentVersion (and elsewhere))	MajorVersion
relminor	(\SOFTWARE\Microsoft\LanmanServer CurrentVersion (and elsewhere))	MinorVersion
samdir	None (obsolete)	
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)	
shmowner	None (obsolete)	
spareserver	AdvancedServer\Process-Parameters	KeepSpareServer

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`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)	
`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`

C.3.6 ups Parameters

The following table lists that status of the `ups` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`poweraddr`	`UPS\Parameters`	`PowerFailAddress`
`powermessage`	`UPS\Parameters`	`PowerFailMessage`
`powertime`	`UPS\Parameters`	`PowerMessageInterval`

C.3.7 replicator Parameters

The following table lists the status of the `replicator` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry 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`
`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`

C.3.8 fsi Parameters

The following table lists the status of the `fsi` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry 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`		
`maxfstypes`	None (obsolete)	
`nfsroot`	`AdvancedServer\FileServiceParameters`	`RootOwnsFilesCreatedOnNFS`
`ntfs`	`AdvancedServer\FileServiceParameters`	`ReportNTFS`
`remotemounts`		

C.3.9 psi Parameters

The following table lists the status of the `psi` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`maxspoolers`	None (obsolete)	
`psaddonpath`	None (`lanman.ini file`)	

C.3.10 version Parameters

The following table lists the status of the `version` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`lan_manager`	None (obsolete)	

C.3.11 netrun Parameters

The following table lists the status of the `netrun` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`maxruns`	`NetRun\Parameters`	`MaxRuns`
`runpath`	`NetRun\Parameters`	`RunPath`

C.3.12 browser Parameters

The following table lists the status of the `browser` parameters.

Parameter	ASU Registry Path (\SYSTEM\CurrentControlSetServices)	Registry Entry Name
`backuprecovery`	`Browser\Parameters`	`BackupRecovery`
`backupupdate`	`Browser\Parameters`	`BackupUpdate`
`lmannounce`	`LanmanServer\Parameters`	`LmAnnounce`
`masterupdate`	`Browser\Parameters`	`MasterUpdate`
`morelog`	`Browser\Parameters`	`MoreLog`

D

The net Commands

You use the `net` commands to display information about or to manage disk shares, printer shares, and domain user accounts. Users use the `net` commands to request information about disk shares, printer shares, and domain user accounts.

Windows 95 clients provide `net` commands that you enter at the MS-DOS prompt. However, these commands only display information about disk shares, printer shares, and domain user accounts and cannot be used to manage them.

You enter `net` commands in lowercase at the Tru64 UNIX command prompt on a system running ASU software, using the following form:

```
# net command [/option]
```

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

Table D–1 briefly describes the `net` commands that you use to administer disk shares, printer shares, and domain user accounts.

Table D–1: Description of the net Commands

net Command	Description
`access`	Displays or modifies resource permissions on ASU 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.
`accounts`	Displays the role of ASU servers in a domain and displays or modifies password and login user requirements.
`admin`	Runs commands on a remote ASU 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`.

Table D–1: Description of the net Commands (cont.)

net Command	Description
`config`	Displays configuration information or changes the configuration of the ASU `server` service.
`continue`	Reactivates suspended services; reactivates paused shared printers when entered at a client computer.
`device`	Displays a list of device names and controls shared printers. When used without options, this command displays the status of all shared printers at the specified ASU 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 an ASU server. This command also can be entered as `net files`.
`group`	Adds, displays, or modifies global groups. This command can be entered as `net groups`.
`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.
`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 Tru64 UNIX system login name.
`password`	Changes the password for a user account on an ASU server or in a domain.
`pause`	Suspends a service. The services that can be paused are `Alerter`, `Browser`, `EventLog`, `NetLogon`, `Replicator` , `Server`, and `TimeSource`.
`perms`	Displays or modifies resource permissions and ownership information on ASU servers. This command operates on shares, directories, and files.
`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.

Table D–1: Description of the net Commands (cont.)

net Command	Description
`session`	Lists or disconnects sessions between an ASU server and clients. When used without options, this command displays information about all of the sessions on the local ASU 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 ASU server.
`sid`	Performs translations between account names and their corresponding security identifiers (SIDs).
`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`, `Browser`, `EventLog`, `NetLogon`, `Replicator`, `Server`, and `TimeSource`.
`statistics`	Displays or clears the statistics log.
`status`	Displays an ASU server's computer name, configuration settings, and a list of shared resources.
`stop`	Stops a service. The services that can be stopped are `Alerter`, `Browser`, `EventLog`, `NetLogon`, `Replicator`, `Server`, and `TimeSource`.
`time`	Synchronizes the client's clock with that of an ASU server or domain, or displays the time for an ASU server or domain.
`trust`	Establishes and breaks trust relationships between domains, and lists trust information for a specified domain.
`user`	Adds, modifies, or deletes user accounts or displays user account information.
`version`	Displays the ASU version number on the system on which the command is entered.
`view`	Displays a list of ASU servers or displays the resources being shared by an ASU server.

D.1 Online Help for net Commands

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

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

```
# net help | more
```

To display the syntax and options for a particular `net` command, enter:

```
# net help command | more
```

To display a detailed description of the options for the `net` command you selected, enter:

```
# net help command/options | more
```

Table D–2 describes the syntax conventions when viewing online help for the `net` commands.

Table D–2: The net Command Syntax Conventions

Symbol	Meaning	Example
Braces ({ })	You must choose an option contained within braces.	`{yes | no}` You must specify yes or no.
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}` You can use only one of these options.
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.

D.2 Using Special Characters

Some of the information you supply with a `net` command may contain a Tru64 UNIX or shell specific special character, for example, an ampersand (&). If you use a special character with a `net` command, you must precede the special character with the backslash escape character (\ ). For example, the following command logs a user named peter, whose password is mrkt&dev, in to an ASU server:

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

Commonly used Tru64 UNIX special characters include:

- Asterisk (*)
- Semicolon (;)
- Pipe (|)
- Square brackets ([ ])
- Parentheses [( )]
- Question mark (?)
- Ampersand (&)
- Caret (^)
- Backslash (\ )
- Dollar sign ($)
- Greater-than and less-than signs (< >)
- Blank ( )
- The at symbol (@)
- Exclamation point (!)

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

D.3 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. For example, to log a user named peter with the password changeme on to an ASU server you would enter:

```
# net logon peter changeme
```

Optionally, you can replace the password with an asterisk (*), which causes the system to prompt you for a password. In the Tru64 UNIX operating system, the asterisk (*) is a special character and must be preceded by a backslash (\ ).

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

```
# net logon peter \*
```

The following message is displayed:

```
Type your password:
```

The password is not displayed on the screen as you type.

A password that contains special Tru64 UNIX characters must be enclosed in single quotes when the user logs in. For example, to log in to the ASU server with a user name of peter and a password of !!!!!!!!, enter:

```
# net logon peter '!!!!!!!!!!'
```

D.4 Using Command Confirmation

Some `net` commands require confirmation. For example, if you enter the `net logoff` command to log off the network with connections to remote shared resources still active, the ASU 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 ASU server prompts.

D.5 Specifying a Path Name

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 provided that you have permission to create the directory.

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/net/servers/lanman/shares/test
  ```

- A c: and single quotes (') with a single backslash (\). For example:

  ```
  # net share 'test=c:\usr\net\servers\lanman\shares\test'
  ```

Each of these commands creates a share called test in the `/usr/net/servers/lanman/shares` directory on the Tru64 UNIX server.

D.6 Abbreviating net Commands Options

You can abbreviate `net` command options by typing enough letters to distinguish an option from the other options. However, you cannot abbreviate a value for an option. For example, the `net accounts` command has the options /forcelogoff:{minutes | no}, /minpwlen:length, /maxpwage:{days | unlimited}, /minpwage:days, and /uniquepw:number. You can enter the `net accounts` command and abbreviated options as:

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

Note

Do no abbreviate a `net` command options in a shell script.

D.7 Administering a Remote ASU Server

You can use the following `net admin` command to administer a remote ASU server:

```
# net admin \\servername password /command
```

The *password* variable is the administrator's password on the remote ASU server. For example, to create a remote domain user account for a user named peter and a password of changeme, the administrator (using a password of system) of the remote system enters:

```
# net admin \\server1 system  /command net user peter changeme /add
```

The ASU server assigns you administrative privileges when you log in to the Tru64 UNIX system using the root user account, even if you did not specifically log in to the ASU server by using the `net logon` command.

Having administrative privileges on a local ASU server does not mean that you have the same privileges on a remote ASU server. To remotely manage an ASU server, you must use the `net logon` command to log in to the domain of which the remote ASU server is part before you can administer it. Otherwise, you will receive an access denied error.

Entering the `net logon` command on a system configured as an ASU member server logs you into the member server, and not the PDC. To use the `net logon` command to log in to the PDC, enter:

```
# net logon administrator password /dom:domain_name.dom
```

You cannot enter the `net logon` command from a Windows client to log in to a member server.

D.8 Examples of Using net Command

The following examples show how to use `net` commands to perform common administrative tasks. These examples assume you are logged in as the administrator to a local ASU server called Server1.

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

```
# net logon username password
```

To create a domain user account for a user named peter with a password of changeme enter:

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

To place peter's user account in the Domain Admins group enter:

```
# net group "Domain Admins" peter /add
```

To view shares on the local ASU server enter:

```
# net view
```

To view the shares on a remote ASU server called server2 enter:

```
# net view \\server2
```

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

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

To create a printer share called print1 that maps to a printer called laser enter:

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

To view the connections to an ASU server enter:

```
# net session
```

To view resource permissions and ownership on a directory enter:

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

E

ASU Commands

The ASU software provides commands that you enter at the Tru64 UNIX command prompt to display information about or to manage the ASU server and its resources.

You must log in to the Tru64 UNIX system as root to use most of the ASU commands.

For more information on an ASU command, install the ASU Reference Pages subset and enter the `man` command followed by the name of the command. For example, for more information on the `asuivp` command, enter:

```
# man asuivp
```

Note

Commands in the `/usr/lbin` directory are reserved for use by the ASU server only and are not documented or supported for use by administrators or users. Do not execute, move, delete or rename the commands in the `/usr/lbin` directory.

The following table describes ASU general administration commands that are located in the `/usr/sbin` directory.

Command	Purpose
`asuivp`	Verify that the ASU software is correctly configured.
`asusetup`	Configure the ASU server.
`chaccounts`	Display or configure the ASU password expiration policy for a system.
`chacl`	Change ACL information.
`chdomain`	Change domain information.
`chgroup`	Change ASU group information.
`chuser`	Change domain user account information.
`clsetup`	Configure the classes in the Tru64 UNIX `lpr` print subsystem.

Command	Purpose
`ctlrsetup`	Configure transports for the ASU server.
`elfread`	Display and clear event logs for the ASU server.
`euctosjis`	Convert the coding of characters from Extended UNIX Code (EUC) to Shift-JIS (S-JIS) encoding.
`joindomain`	Configure the ASU server into a new domain.
`lmat`	Schedule commands or programs to run on the ASU server at a specified time or date.
`lmshare`	Configure the ASU share file without server intervention.
`lsacl`	Display ACLs placed on objects.
`mapuname`	Map and unmap domain user account names, global group names, and local group names to and from Tru64 UNIX user names.
`netevent`	Send administrative, user, and printing alerts to users submitting print jobs.
`nfsshare`	Create ASU disk shares from the file systems and directories offered as NFS exports.
`promote`	Change the role of ASU domain controller to either a primary domain controller (PDC) or a backup domain controller (BDC). If you demote a PDC to a member server, the domain user account database is removed.
`regconfig`	Query or set ASU registry key information.
`rmacl`	Delete ACLs from objects.
`setdomainname`	Configure the domain name of the ASU server.
`setservername`	Configure the name of the ASU server.
`sjistoeuc`	Convert the coding of characters from S-JIS to EUC encoding.
`srvconfig`	Display or modify the ASU server configuration information stored in the `lanman.ini` file.

The following table describes ASU troubleshooting commands that are located in the `/usr/sbin` directory. You should have a thorough understanding of the ASU software and environment before you use these commands.

Command	Purpose
`acladm`	Create, check, manage, and remove the ACL database.
`acldump`	Dump the ACL database to a text file.
`asustat`	Display statistical information retrieved from the ASU server's shared memory.
`blobadm`	Display information, check, and configure blob files.
`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.
`nbemon`	Monitor activity and status of the NetBEUI transport.
`regcheck`	Configure the ASU registry to enumerate registry parameters, dump the contents of the registry, or check and repair registry files.
`samcheck`	Check or fix the security account manager (SAM) database; or dump the change log, built-in, account, or LSA databases.

The following table describes ASU support commands that are located in the `/usr/sbin` directory. You should use these commands only with guidance from technical support personnel.

Caution

Improper use of these commands may corrupt your system and cause unexpected results, including system failure.

Command	Purpose
`aclload`	Load the ACL database from a text file.
`regload`	Create a registry file if one does not exist. Also used to reinitialize the registry to system defaults.

The following table describes ASU general-purpose commands that are located in the `/usr/bin` directory.

Command	Purpose
`asuclient`	Configure user access to a printer that is attached to an MS-DOS client.
`dos2unix`	Convert text files from MS-DOS to Tru64 UNIX format.
`lmshell`	Create an MS-DOS interface on the Tru64 UNIX server.
`net`	Request information about ASU servers and domains. Administrators can also manage ASU servers and domains by using the `net` commands.
`ud`	Convert text files between Tru64 UNIX, MS-DOS, and Macintosh formats.
`unix2dos`	Convert Tru64 UNIX text files to MS-DOS format.

F

Configuring ASU in a Version 1.x Cluster

In a TruCluster Version 1.x cluster, the ASU server runs on only one cluster member at a time. If that cluster member fails, the ASU server automatically restarts on another cluster member on which the ASU software is installed, and user conections are reestablished. Users may experience a short delay while the ASU server restarts.

You must perform the following tasks to configure the ASU server in a TruCluster Version 1.x cluster:

- Be sure that the systems meet the ASU and TruCluster prerequistes.
- Create the TruCluster disk service for the ASU server.
- Configure the ASU software.

F.1 ASU and TruCluster Software Prerequisites

You must identify at least two cluster members that will run the ASU server. One member on which the ASU server is active and one member on which the ASU server is inactive. The inactive member takes over the ASU server responsibility if the active member fails.

The cluster members must have compatible versions of software and firmware and use a SCSI-connected shared bus to access the shared disk that will contain ASU-related configuration and data files, such as the ASU share database and the user account database. The shared disk may be a single disk, multiple disks, mirrored disks, or a disk array that is accessible to systems in the environment.

If the cluster members and clients use TCP/IP, you need a TCP/IP address for the ASU disk service. Cluster members must have an entry in their `/etc/hosts` file for the ASU disk service that includes the TCP/IP address and name for the ASU disk service. The name associated with the TCP/IP address must be the ASU server name.

For example, if the the ASU server and disk service name is ASU and the IP address assigned to the service is 10.0.0.10, then a line similar to the following must be included in the `/etc/hosts` file on each cluster member:

```
10.0.0.10 ASU
```

Systems that reside in different subnets must have access to the name and address of the ASU disk service either by adding an entry in the local `/usr/net/servers/lanman/datafiles/lmhosts` file or through a DNS or a WINS server.

F.2 Creating a TruCluster Disk Service

Use the `asemgr` utility to create a disk service for the ASU server. Follow these steps to create a TruCluster disk service:

1. Edit the `/etc/hosts` file and add the TCP/IP name and address assigned to the ASU disk service.
2. Log in as root and start the TruCluster `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The `asemgr` utility displays the ASE main menu.
3. Choose the following options: Managing ASE Service, then Service Configuration, then Add a new service, then Disk Service.

   A status message is displayed. You are prompted to enter a name for the disk service.
4. Enter a name for the disk service. Enter the same name that you will use for the ASU server when you configure the ASU software.

   You are prompted to assign a TCP/IP address to the disk service.
5. 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.
6. 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.
7. Enter a mount point. For example, `/ASU`.

   You are prompted for the type of access to the mount point.
8. Enter 1, Read-write.

   You are prompted to optionally enable user and group quotas.
9. 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.
10. Enter the options you want or press the Enter key to choose the default options, which are listed in the `mount` reference page.

You are prompted to enter information about another shared disk.

11. Optionally, enter the location of another shared disk to be used by the service and repeat steps 5 through 9. Press the Enter key to continue.

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

12. Choose the Start action script option.

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

13. Choose the Add a start action script option.

    You are prompted for the full pathname for the start action script.

14. Enter the following pathname:

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

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

15. Press the Enter key.

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

16. Press the Enter key to choose the default value.

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

17. Choose the Exit option.

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

18. Repeat steps 12 through 16 replacing the word start with stop.

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

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

    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.

20. 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.

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

    You are prompted to add the service.

22. Answer yes.

    The service is added.

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

F.3 Configuring the ASU Software

Follow these steps to configure the ASU software:

1. Choose a system on which the ASU server will be active and log in as root.
2. 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 ASU server will participate in a TruCluster Version 1.x cluster.
3. Answer yes.

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

   The configuration proceeds. See Chapter 1 for more information on configuring the ASU software.

Follow these steps to configure the alternate system on which the ASU server is installed:

1. Log in as 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 ASU server will participate in a TruCluster Version 1.x cluster.
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 ASU server.
4. Enter the transport information for the ASU server.

   See Chapter 1 for more information on configuring the transport information for the ASU software.

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

F.4 ASU Licensing in a TruCluster Cluster

Although the ASU server is cluster-aware, the license management facility (LMF) is not. ASU licenses are supplied in the form of a product authorization key (PAK) called ASDU-CONNECT that you load into LMF. You must load an ASDU-CONNECT PAK in LMF on each cluster member on which you will run the ASU server.

See Section 1.9 for ASU licensing information.

F.5 Managing ASU Resources in a TruCluster Cluster

The following sections describe how to create and manage ASU disk shares, domain user accounts, and ASU printer shares in a TruCluster cluster.

F.5.1 Creating Disk Shares

When you configure the ASU server in a TruCluster cluster, links are automatically established to the shared disk in the `/usr/net/servers/lanman/shares` directory.

Shares that you create in this directory, or in any other directory on the shared disk, are accessible by all cluster members. You must ensure that shares created prior to setting up the ASU server in a TruCluster cluster are located on the shared disk. Shares created on a nonshared or local disk are not accessible by other cluster members after a failover.

F.5.2 Maintaining User Accounts

In a TruCluster cluster, the ASU server requires that the `/etc/passwd` file contain identical entries on all cluster members.

By default, adding or deleting a domain user account adds or deletes the associated Tru64 UNIX user account only in the `/etc/passwd` file on the local system and other cluster members cannot access this information.

You can make Tru64 UNIX user account information available to all cluster members by using Network Information Service (NIS) in the cluster. To do so, you must create Tru64 UNIX user accounts on the NIS master server before you create domain user accounts. This way, when you create domain user accounts, ASU does not create the Tru64 UNIX accounts locally because they already exist in the NIS database.

If you do not include NIS in the cluster you must manually maintain the local `/etc/passwd` files on each member server.

F.5.3 Maintaining Print Services

In a TruCluster cluster, the shared disk stores information for each ASU printer share. If you modify information about print services in the `/etc/printcap` file on a member server, then you must modify the `/etc/printcap` file on all the member servers to include the same information.

F.6 Removing ASU from a TruCluster Cluster

To remove the ASU server you can:

- Remove one ASU server from the TruCluster Version 1.x cluster. This method leaves the data files on the shared disk. The ASU server on the system being removed is no longer able to access the data files.
- Remove all ASU servers from the TruCluster Version 1.x cluster. This method allows you to transfer the ASU data files on the shared disk to the local disk on a system of your choice. The ASU server running on the system that has the data files can continue to store and use the information.

F.6.1 Removing One ASU Server from the Cluster

Follow these steps to remove one ASU server from the cluster:

1. If the system you want to remove from the cluster is currently running the ASU service, relocate the ASU service to an alternate system.
2. Restrict the system you want to remove from running the ASU service.
3. Either deinstall the ASU server from the system or run the `asusetup` utility and answer no when prompted if the ASU server will participate in a TruCluster Version 1.x cluster.

These steps are discussed in the following sections.

F.6.1.1 Relocating the ASU Service

Follow these steps to relocate an ASU service from the active server to an alternate server:

1. Log in as root and start the `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.
2. Choose the Managing ASE Services option, then the Relocate a service option.

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

3. Enter the number that represents the ASU service you want to relocate.

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

4. Enter the number that represents the ASU server to which you want to relocate the service.

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

F.6.1.2 Restricting a System from Running the ASU Service

Follow these steps to restrict a system in a the TruCluster Version 1.x cluster from running the ASU service:

1. Log in as root and start the `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.

2. Choose the Managing ASE Services option and then choose the Service Configuration option.

   The Service Configuration menu is displayed.

3. Enter the number that represents the ASU service.

   A list of modification options is displayed.

4. Choose the Restrict Membership option.

   A list of members displays.

5. Choose to restrict the member you want to restrict from running the ASU disk service in the cluster.

F.6.1.3 Deinstall the ASU Server

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

1. Log in to the Tru64 UNIX system as the root user and notify users that the ASU server will be unavailable.

2. Display the installed ASU subsets by entering the following command:

   ```
   # setld -i |grep ASU |grep -v not |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:

   ```
   # setld -d ASUADMnnn ASUBASEnnn ASUMANPAGEnnn ASUTRANnnn
   ```

   The *nnn* represents the version number of the ASU software. See the ASU *Release Notes* for the current version number.

   During the deinstallation you are prompted to reconfigure the ASU software, resulting in its removal from the cluster.

4. Answer yes at the prompt.

While the ASU subsets are being removed you might be prompted to save data files. You can answer no because the data files are saved on the shared disk.

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

F.6.2 Removing ASU from All Systems in a TruCluster Version 1.x Cluster

Follow these steps to remove the ASU server from all the systems in a cluster:

1. Decide which system will receive the ASU data files from the shared disk and, if necessary, relocate the ASU service to that system.
2. Restrict the ASU server to run on only the system that will receive the data files in step 1.
3. Remove the ASU server from the alternate system.
4. Remove the ASU server from the active system.
5. Remove the ASU disk service from the TruCluster cluster.

These steps are discussed in more detail in the following sections.

F.6.2.1 Relocating the ASU Service

If the system to which you want to transfer the ASU data files is not the active server, then use the following steps:

1. Log in as root and start the `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.
2. Choose the Managing ASE Services option, then the Relocate a service option.

   The Select the service that you want to relocate menu is displayed.
3. Enter the number that represents the ASU service you want to relocate.

   The Select member to run 'service name' service menu is displayed.
4. Enter the number that represents the system to which you want to relocate the ASU service.

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

F.6.2.2 Restrict the ASU Server to Run on a Single System

Follow these steps to restrict the ASU server to run on a single system:

1. Log in as root and start the `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.
2. Choose the Managing ASE Services option and then choose the Service Configuration option.

   The Service Configuration menu is displayed.
3. Enter the number that represents the ASU service.

   A list of modification options is displayed.
4. Choose the Restrict Membership option.

   A list of member names is displayed.
5. Choose to restrict all the members from running the ASU service, leaving as a member only the system to which you want to transfer the data files.

F.6.2.3 Removing the ASU Server from the Alternate System

Follow these steps to remove the ASU server from the alternate system:

1. Log in as root and start the `asusetup` utility as follows:

   ```
   # asusetup
   ```

   The `asusetup` utility detects if the ASU server was configured to run as a TruCluster service and prompts you to respond whether or not you want it to continue to run as part of the TruCluster disk service.
2. Answer no at the prompt.

   The `asusetup` utility prompts you to reconfigure the ASU server.
3. Answer yes to configure the ASU server. The `asusetup` utility continues with normal configuration questions and procedures.

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

   See Chapter 1 for more information on configuring the ASU software.

F.6.2.4 Removing the ASU Server from the Active System

Follow these steps to remove the ASU server from the active system:

1. Log in as root and start the `asusetup` utility as follows:

   ```
   # asusetup
   ```

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

2. Answer no at the prompt.

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

3. Answer yes at the prompt.

   The `asusetup` utility prompts you to reconfigure the ASU software.

4. Answer yes at the prompt.

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

   See Chapter 1 for more information on configuring the ASU software.

   If you configure the ASU 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.

F.6.2.5 Removing the ASU Disk Service

Follow these steps to remove the ASU disk service:

1. Log in as root and start the `asemgr` utility as follows:

   ```
   # asemgr
   ```

   The ASE main menu is displayed.

2. Choose the following options: Managing ASE Service, then Service Configuration, then Delete a service option.

   The Deleting a Service menu is displayed.

3. Enter the number that represents the ASU disk service that you want to remove.

   A confirmation message is displayed.

4. Answer yes at the prompt.

   The service is removed.

Index

A

administering
  ASU commands, 1–3
  net commands, 1–4
  Tru64 UNIX commands, 1–4
  Tru64 UNIX GUIs, 1–4
  Windows GUIs, 1–4
administrator password, 1–11
  configuring, 1–11
alert messages
  reviewing, 8–3
asu command
  overview, E–1
ASU directories, 1–13
ASU processes, 1–14
ASU services, 1–13
authentication
  using Windows NT Version 4.0 Server, 3–17
  Windows 2000, 1–2
  Windows NT Version 4.0 Server, 1–3

B

backup domain controller
  configuring, 1–11

C

capturing
  network packets, 8–6
computer name conflicts
  reviewing, 8–5
configuring
  administrator password, 1–11
  ASU server, 1–10
  backup domain controller, 1–11
  controllers, 1–8
  domain name, 1–10
  domain role, 1–10
  general information, 1–11
  international support, 1–19
  lmhosts file, 1–9
  member server, 1–11
  name resolution, 1–9
  NBNS, 1–9
  network information, 1–8
  number of clients, 7–1
  number of NetBIOS names, 7–3
  number of open files, 7–4
  number of record locks, 7–4
  number of server processes, 7–2
  number of transport sessions, 7–1
  primary domain controller, 1–10
  restoring previous, 1–7
  server name, 1–10
  TruCluster Version 5.x, 6–1
  WINS, 1–9
configuring ASU, 2–1
configuring in multi mode
  TruCluster Server Version 5.x, 6–2
configuring in none mode
  TruCluster Server Version 5.x, 6–22
configuring in single mode
  TruCluster Server Version 5.x, 6–12
connection problems
  reviewing, 8–5
controllers

- configuring, 1–8
- **core files**
  - generating, 8–7, 8–8

D

- **disk share**
  - attributes, 4–1, 4–5
  - creating, 4–1, 4–6
  - deleting, 4–26
  - for remote file systems, 4–23
  - for users, 4–22
  - group premissions, 4–21
  - NFS, 4–1
  - NTFS ACLs, 4–13
  - permissions, 4–10
  - special, 4–4
- **documentation**, 1–1
- **domain name**
  - configuring, 1–10
- **domain role**
  - configuring, 1–10

E

- **elfread command**
  - reviewing logs, 8–4
- **Explorer**
  - setting NTFS permissions, 4–18

G

- **generating**
  - core files, 8–7, 8–8
  - StackTrace files, 8–7, 8–8
- **groups**
  - creating, 3–20
  - deleting, 3–22

H

- **HSM**, 7–4

I

- **installation requirements**, 1–2
- **installation verification**, 1–12
- **installing**
  - ASU subsets, 1–6
  - Password Management utility, 3–10
  - preinstallation tasks, 1–1
  - Windows based interfaces, 1–15
- **international support**, 1–19

L

- **lanman.ini file**, C–1
  - file parameters, C–2
  - file syntax, C–1
  - lmxserver parameters, C–4
  - mapping to registry entries, C–9
  - server parameters, C–2
  - workstation parameters, C–3
- **licenses**, 1–18
- **licensing**
  - TruCluster Server Version 5.x, 6–29
- **lmhosts file**
  - configuring, 1–9
- **log files**
  - reviewing, 8–3
- **logging**
  - network errors, 8–5

M

- **managing**
  - TruCluster Version 1.x, F–5
- **member server**
  - configuring, 1–11
- **modes**
  - TruCluster Server Version 5.x, 6–1

N

- **name resolution**

  configuring, 1–9
NBNS
  configuring, 1–9
net command
  abbreviating, D–7
  confirmation, D–6
  creating disk shares, 4–8
  creating groups, 3–21
  creating printer shares, 5–3
  creating user accounts, 3–13
  deleting a disk share, 4–27
  deleting groups, 3–22
  example, D–8
  online help, D–3
  overview, D–1
  passwords, D–5
  setting NTFS permissions, 4–17
  setting printer share permissions, 5–5
  setting Windows NT permissions, 4–12
  special characters, D–4
  specifying a path name, D–6
network errors
  logging, 8–5
network information
  configuring, 1–8
network packets
  capturing, 8–6
NFS
  disk share, 4–1
NTFS ACLs, 4–13
number of clients
  configuring, 7–1
number of NetBIOS names
  configuring, 7–3
number of open files
  configuring, 7–4
number of record locks
  configuring, 7–4
number of server processes
  configuring, 7–2
number of transport sessions
  configuring, 7–1

P

password synchronization, 1–2
passwords
  administrator, 1–11
permissions, 4–10
  NTFS, 4–13
  printer share, 5–5
  Tru64 UNIX, 4–18, 4–21
  Windows NT, 4–11
primary domain controller
  configuring, 1–10
printer log files
  reviewing, 8–4
printer share
  attributes, 5–1
  configuring client printers, 5–6
  creating, 5–1, 5–3
  installing alternate drivers, 5–4
  permissions, 5–5
  viewing, 5–6
printers
  registry entries, 5–2

R

reconfiguring ASU, 1–13
registry
  ASU Administrator, 2–9
  changing, 2–5
  overview, 2–1
  regconfig command, 2–6
  registry editor, 2–7
  system policy editor, 2–8
  value entries, 2–4
  viewing, 2–5
registry entries
  AdvancedServer, B–1
  Alerter, B–23

  - AlertParameters, B–1
  - Browser, B–23
  - EventLog, B–24
  - FileServiceParameters, B–2
  - LanmanServer, B–25
  - NetAdminParameters, B–9
  - Netlogon, B–27
  - Parameters, B–9
  - ProcessParameters, B–12
  - Replicator, B–29
  - RpcParameters, B–16
  - ShareParameters, B–17
  - UnixAuditParameters, B–17
  - UPS, B–31
  - UserServiceParameters, B–18
- **reviewing**
  - alert messages, 8–3
  - computer name conflicts, 8–5
  - connection problems, 8–5
  - log files, 8–3
  - printer log files, 8–4
  - statistics, 8–1
  - transaction statistics, 8–2
- **reviewing logs**
  - elfread command, 8–4
  - Windows Event Viewer, 8–4

S

- **sample**
  - configuration, A–2
  - installation, A–1
- **Server Manager**
  - creating disk shares, 4–9
  - deleting a disk share, 4–27
  - setting Windows NT permissions, 4–12
- **server name**
  - configuring, 1–10
- **StackTrace files**
  - generating, 8–7, 8–8
- **starting ASU**, 1–12
- **statistics**
  - reviewing, 8–1

T

- **transaction statistics**
  - reviewing, 8–2
- **troubleshooting**
  - accessing a file, 8–16
  - accessing the ASU server, 8–9
  - browsing, 8–18, 8–19
  - connecting to a share, 8–15
  - printer shares, 8–19
  - starting the ASU server, 8–8
- **TruCluster Server Version 5.x**
  - configuring in multi mode, 6–2
  - configuring in none mode, 6–22
  - configuring in single mode, 6–12
  - licensing, 6–29
  - modes, 6–1
- **TruCluster Version 1.x**
  - configuring ASU, F–4
  - creating a disk service, F–2
  - managing, F–5
  - overview, F–1
  - removing, F–6
- **TruCluster Version 5.x**
  - configuring, 6–1

U

- **upgrading**
  - setld command, 1–5
- **upgrading ASU software**, 1–5
- **user accounts**
  - attributes, 3–1
  - authentication, 1–2
  - creating, 3–1, 3–12
  - deleting, 3–19
  - disabling, 3–12
  - grouping, 3–20
  - mapping, 3–16
  - NIS, 3–7
  - password synchronization, 1–2, 3–9
  - Tru64 UNIX, 3–4
  - Tru64 UNIX attributes, 3–5

  Tru64 UNIX home directories, 3–6
User Manager for Domains
  creating groups, 3–21
  creating user accounts, 3–15
  deleting groups, 3–22

V

verifying
  installation, 8–8
verifying installation, 1–12

W

Windows Event Viewer
  reviewing logs, 8–4
Windows NT permissions
  setting, 4–12
Windows NTFS permissions
  setting, 4–17
Windows Printer Properties GUI
  setting printer share permissions, 5–5
Windows Printer Wizard
  creating printer shares, 5–4
WINS
  configuring, 1–9