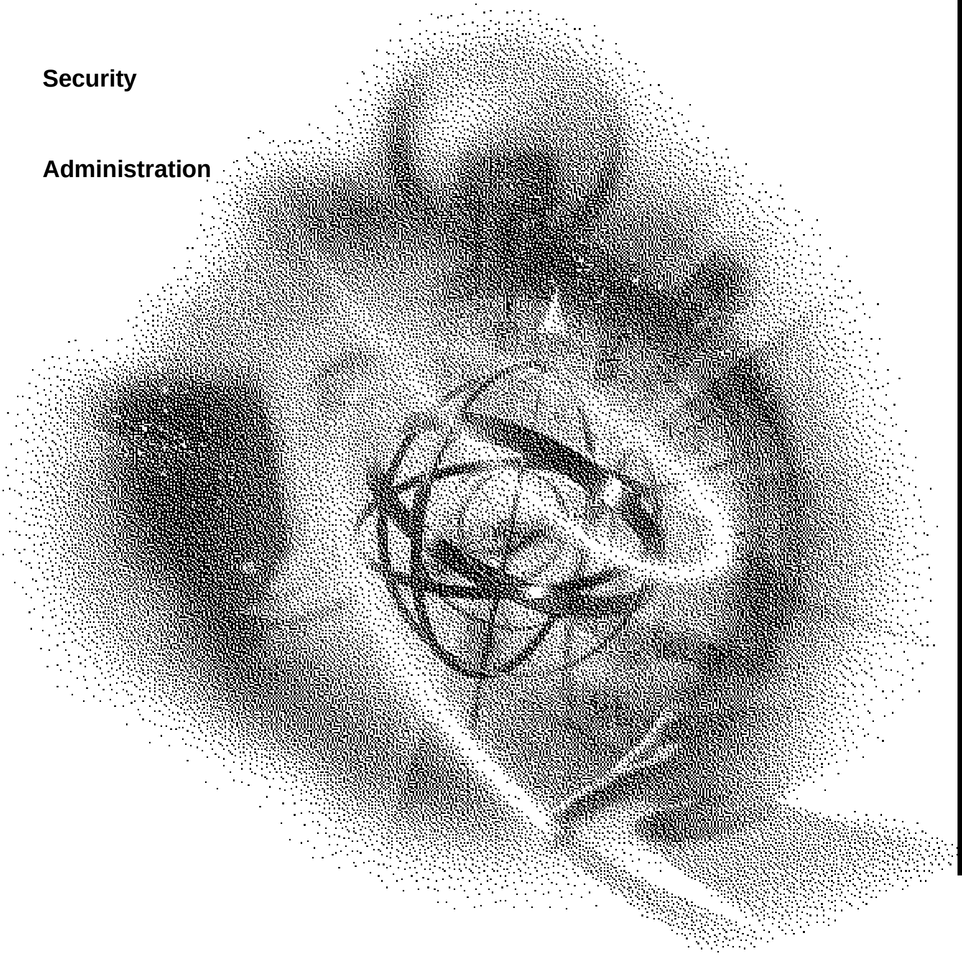
VERSION 4.11

NetWare Enhanced Security Administration

NetWare® 4™



Novell®

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software, at any time, without any obligation to notify any person or entity of such changes.

trademarks

Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. The Novell Network Symbol is a trademark of Novell, Inc.

A complete list of trademarks and their respective owners appears in “Trademarks” on page 385.

U.S. Patent Nos. 5,157,663; 5,349,642; and 5,455,932. U.S. and International Patent Pending.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

NetWare Enhanced Security Administration
September 1996
100-003611-001 A

Contents

How to Use This Manual

1 Overview of Security Mechanisms

2 Security Supplement to Guide to NetWare 4 Networks

3 Security Supplement to Installation

4 Security Supplement to Managing NetWare Directory Services Objects

5 Security Supplement to Managing Directories, Files, and Applications

22 Summary

W Network Composition Rules

Trademarks

How to Use This Manual

Introduction

This *NetWare Enhanced Security Administration* manual describes how server administrators install, configure, maintain, and audit individual NetWare® Enhanced Security servers and the combined NetWare Enhanced Security network system.

This manual is written for administrative staff (supervisors, administrators, operators, and auditors) of evaluated NetWare Enhanced Security servers. It is not intended to be distributed to nonadministrative network users.

The purpose of this document is to:

- Guide the configuration and installation of a secure server within the NetWare Enhanced Security network system.
- Guide the operation of the server in a secure manner.
- Enable administrative personnel to make effective use of the server's protection mechanisms.
- Issue warnings about possible misuse of administrative authority.

This manual addresses the recommended content of the Guidelines for Writing Trusted Facility Manuals [NCSC-TG-016] but, as described in Paragraph 1.3 of that manual, presents the information in a different order and format than the recommended outline.

Note: In Novell® documentation, an asterisk denotes a trademarked name belonging to a third-party company. Novell trademarks are denoted with specific trademark symbols, such as $^{\text{TM}}$.

Product Overview

NetWare Enhanced Security is a distributed network operating system made up of four types of network components: servers, workstations, interconnections (routers, bridges, and repeaters), and network media.

The evaluated server component described in this document may serve any number of workstations, limited only by software license restrictions.

The server component contains a Network Trusted Computing Base (NTCB) partition, which is used to enforce the security policies and protect data stored on the server. The evaluated server component must not be used to run untrusted software.

As a network system composed of these four components, NetWare Enhanced Security is designed to meet the Controlled Access implementation (Class C2) requirements of the Trusted Network Interpretation (TNI) [NCSC-TG-005] of the Trusted Computer System Evaluation Criteria (TCSEC) [DoD5200.28-STD].

The evaluated server is an IAD component as defined in Appendix A of the TNI.

Manual Overview

This manual contains supplementary trusted facility information (such as notes and warnings) for Novell's existing NetWare 4.11 administrative manuals. The NetWare 4.11 administrative manuals that are necessary when running a trusted network facility include:

Concepts	Describes the terms and concepts necessary to understand NetWare networking.
Guide to NetWare 4 Networks	Contains an overview of NetWare Directory Services^{TM} (NDS^{TM}) technolofy features and planning information necessary for the installation of NDS.
Installation	Describes the installation of a NetWare 4.11 server.
Supervising the Network	Includes procedures for managing NetWare Directory Services (NDS) technology, managing the file system, maintaining the server, auditing the network, backing up network data, and performing troubleshooting It is the primary document that describes the procedures involved in running a trusted network facility.
Utilities Reference	Contains manual pages for the server console commands and client utilities.
Print Services	Describes the configuration, management, and use of NetWare's print services.
System Messages	Contains system and error messages for NetWare 4.11.

These NetWare 4.11 documents are available online, using the DynaText* viewer provided in the NetWare 4.11 distribution media. For information on using the DynaText viewer to read the NetWare 4.11 manuals, refer to *Installing and Using Novell Online Documentation*.

If you are installing a server for the first time, refer to printed instructions (enclosed with the distribution media) for installing the viewer and documentation on a standalone system.

Warning

Do not install NetWare Enhanced Security on a server without reviewing the online documents described above. This manual is not a standalone document.

You must read *both* the online documentation and the supplementary data in this document

Because this manual contains supplementary information for an existing document set, it follows the organization of that document set and does not directly follow the outline suggested by [NCSC-TG-016].

This manual contains the following chapters.

- Chapter 1, “Overview of Security Mechanisms,” on page 21 describes the server component’s protection philosophy, how the server component fits within the NetWare Enhanced Security network security architecture, and how the server can be used to protect against various computer security threats.

- Chapter 2, “Security Supplement to Guide to NetWare 4 Networks,” on page 43 provides supplementary information for *Guide to NetWare 4 Networks.*

- Chapter 3, “Security Supplement to Installation,” on page 69 provides supplementary trusted facility information for *Installation*.

  Taken together, the *Installation* manual and this supplementary information describe the installation of the server NTCB partition.

- Chapters 4 through 14 provide supplementary trusted facility information for *Supervising the Network.*

- Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91 provides supplementary information for Chapter 1, “Managing NetWare Directory Services Objects,” of *Supervising the Network.*

- Chapter 5, “Security Supplement to Managing Directories, Files, and Applications,” on page 129 provides supplementary information for Chapter 2, “Managing Directories, Files, and Applications,” of *Supervising the Network.*

- Chapter 6, “Security Supplement to Creating Login Scripts,” on page 137 provides supplementary information for Chapter 3, “Creating Login Scripts,” of *Supervising the Network.*

- Chapter 7, “Security Supplement to Maintaining NetWare Networks,” on page 139 provides supplementary information for Chapter 4, “Maintaining NetWare 4 Networks” of *Supervising the Network.*

- Chapter 8, “Security Supplement to Managing the NetWare Directory Tree,” on page 141 provides supplementary information for Chapter 5, “Managing the NetWare Directory Tree,” of *Supervising the Network.*

- Chapter 9, “Security Supplement to Migrating Data Using the HCSS,” on page 149 addresses Chapter 6, “Migrating Data Using the High Capacity Storage System,” of *Supervising the Network.*

- Chapter 10, “Security Supplement to Maintaining the NetWare Server,” on page 151 addresses Chapter 7, “Maintaining the NetWare Server,” of *Supervising the Network.*

- Chapter 11, “Security Supplement to Maintaining NetWare SMP,” on page 163 addresses Chapter 8, “Maintaining NetWare SMP” of *Supervising the Network.*

- Chapter 12, “Security Supplement to Backing Up and Restoring Data,” on page 165 provides supplementary information for Chapter 9, “Backing Up and Restoring Data,” of *Supervising the Network.*

- Chapter 13, “Security Supplement to Managing NetWare Licensing Services,” on page 177 addresses Chapter 10, “Managing NetWare Licensing Services” of *Supervising the Network.*

- Chapter 14, “Security Supplement to Troubleshooting the Network,” on page 179 provides supplementary information for Appendix A, “Troubleshooting the Network,” of *Supervising the Network.*

- Chapter 15, “Security Supplement to Managing NetWare Server for OS/2,” on page 181 addresses Appendix B, “Managing NetWare Server for OS/2,” of *Supervising the Network.*

- Chapter 16, “Security Supplement to SFT III Management Tips,” on page 183 addresses Appendix C, “SFT III Management Tips,” of *Supervising the Network.*

- Chapter 17, “Security Supplement to Creating Menus,” on page 185 addresses Appendix D, “Creating Menus,” of *Supervising the Network*.

- Chapter 18, “Security Supplement to Print Services,” on page 187 provides supplementary trusted facility information for *Print Services*.

- Chapter 19, “Security Supplement to Concepts,” on page 221 provides supplementary information for *Concepts*.

- Chapter 20, “Security Supplement to Utilities Reference,” on page 309 provides supplementary information for *Utilities Reference*.

- Chapter 21, “Security Supplement to System Messages,” on page 339 provides supplementary information for *System Messages*.

- Chapter 22, “Summary,” on page 369 summarizes this manual, describes the need for physical and administrative security, addresses protection of the network TCB and server NTCB partition, and summarizes the warnings mentioned in previous chapters.

Thus, the TNI requirements for a trusted facility manual are satisfied by this manual, along with the corresponding NetWare documentation.

In addition, the following additional document is necessary to securely configure and run a trusted network:

Novell World Wide Web site	Updates to this manual and other NetWare Enhanced Security documentation can be found in the Technical Support area of the Novell, Inc. World Wide Web site (http://www.novell.com). We recommend that you check this area *regularly* for updated NetWare Enhanced Security information.
NetWare Enhanced Security Server (NetWare 4.11)	Describes the individual hardware devices (mother boards, storage media and controllers, network controllers, and printers) and NetWare Loadable Module (NLM) software that is permitted in an evaluated server configuration.

Security Features Users Guide (NetWare 4.11)	Describes the network security features as they apply to end users.
Auditing the Network (NetWare 4.11)	Describes the Auditcon utility, lists auditable events, and provides instructions for network auditing.

Terms and Acronyms

The following list of terms and acronyms are used throughout this document.

ACL	Access Control List
DOS	Disk Operating System
FSO	File System Object
IPX^{TM}	Internetwork Packet Exchange^{TM} (Novell)
LAN	Local Area Network
NetWare	Novell's commercial network operating system
NDS	NetWare Directory Services
NLM^{TM}	NetWare Loadable Module^{TM}
NTCB	Network Trusted Computing Base
PCP	Printer Communication Protocol. The SPX-based protocol used to communicate the contents of a print job between a NetWare Enhanced Security print server and a NetWare Enhanced Security print driver.
PSSCP	Print Server Status and Control Protocol. The SPX-based protocol used by NetWare Enhanced Security clients to configure NetWare Enhanced Security print servers, and used by NetWare Enhanced Security print drivers to establish their availability to NetWare Enhanced Security print servers.
Public object	An object that is readable by all untrusted subjects, and writable only by privileged users or subjects.

SMS^{TM}	Storage Management Services^{TM}
SPX^{TM}	Sequenced Packet Exchange^{TM} (Novell) protocol
NetWare Enhanced Security	Novell's TCSEC Class C2 trusted network operating system

User Comments

We are continually looking for ways to make our products and our documentation as easy to use as possible.

You can help us by sharing your comments and suggestions about how our documentation could be made more useful to you and about inaccuracies or information gaps it might contain.

Submit your comments by using the User Comments form provided or by writing to us directly at the following address:

Novell, Inc.
Documentation Development MS C-23-1
122 East 1700 South
Provo, UT 84606 USA

We appreciate your comments.

chapter 1 Overview of Security Mechanisms

This chapter describes the concepts involved in administering a secure network system using the NetWare® Enhanced Security server component.

- It presents security threats within a network environment and an explanation of how the server addresses those threats.
- It describes the NetWare Network Trusted Computing Base (NTCB) and discusses on how to build a Class C2 network system using the server component.
- Finally, this chapter summarizes the access control and accountability mechanisms provided by the NetWare Enhanced Security server.

Enhanced Security Concepts

Enhanced security refers to a methodology by which the evaluated server component and, consequently, the facility in which it is used, can be trusted to protect user and facility information.

The Trusted Computer System Evaluation Criteria (TCSEC) [DoD5200.28-STD] defines seven classes (D, C1, C2, B1, B2, B3, and A1) of trusted systems and the requirements for each class.

The Trusted Network Interpretation (TNI) [NCSC-TG-005], under which the server component is evaluated, interprets these requirements for trusted network systems. The TCSEC, TNI, and the textbook *Computer Security Basics* describe the following key trusted system concepts:

Security policy	The *security policy* is a statement of the access control rules enforced by a system. The server component enforces separate Discretionary Access Control (DAC) security policies for accesses to NetWare Directory Services^{TM} objects, NDS^{TM} object properties, and file system objects (such as files and directories).
Accountability	This term refers to the ability of the system to support the principle of individual accountability, that is, that the system is able to determine who you are when you login and to track (audit) your actions while you are logged in. The server component provides protocol-based Identification and Authentication (I&A) of users at network clients and auditing of those users' actions.
Assurance	At C2, *assurance* refers to the degree of trust that a product works as documented. Assurance in the server is provided by specification, and extensive testing, of the server's interfaces.
TCB, NTCB	A *Trusted Computing Base (TCB)* is the totality of hardware, firmware, and software protection mechanisms within a trusted system. As described subsequently, the server component provides a Network Trusted Computing Base (NTCB) partition that mediates all accesses by network clients to the server's protected resources.

These concepts are used throughout the Computer Security discipline, which is concerned with the assessment of trust and the evaluation of TCB protection mechanisms.

Section 1 of *Computer Security Basics* describes other types of security: physical security, Communications Security (COMSEC), and Electromagnetic Emanations Security (TEMPEST).

The server evaluation addresses only its TCB protection mechanisms and does not evaluate the server with respect to any non-TCB features (encryption, for example).

However, in order for your organization to be able to trust the server component to enforce your organization's security policies, you must provide the following non-TCB security:

- Your organization must provide trustworthy administrators for the server and the network. The server enforces rules set in place by these administrators.

  Because of the broad permissions that are necessary for administrators to perform their jobs, an administrator can deliberately or inadvertently make changes to the server that affect the protection of all the data on the server and the network.

- The server and its console must be physically secured, such that only trustworthy administrators can enter commands at the server console.

- As described throughout this manual, the server is restricted to running only trusted software. Running unevaluated NetWare Loadable Module^{TM} (NLM^{TM}) programs on the server violates the basis under which the server was evaluated.

As described in the Trusted Network Interpretation Environments Guideline [NCSC-TG-011], the environment for a Class C2 network is one in which all individual users are cleared to the maximum classification of any information on the network, but where individual accountability and a more finely-grained access control policy are required.

Network Security Threats

The general computer security threat in a NetWare Enhanced Security system is the unauthorized disclosure or modification of data protected on network servers and clients.

Chapter 4 of *Computer Security Basics* describes various types of malicious programs (viruses, worms, Trojan horses, etc.) that may run on components within the network. Because users cannot execute arbitrary code on a server, these threats generally do not apply to the server itself.

The following list addresses various threats within the network and how (or if) the server addresses the threat. Refer to *Computer Security Basics* for a more general description of malicious programs and network security.

Viruses	A *virus* is code that replicates itself within other programs (boot sector code, applications, etc.). Viruses are commonly spread by booting infected diskettes or by copying and running infected programs from a bulletin board. Network users can store viruses in files on the server, however, there is no way for a user to infect the server TCB, because there is no way for a user to cause the server to run non-TCB code. NetWare Enhanced Security clients use various TCB mechanisms and trusted facility procedures to prevent infection of the client NTCB partition. Because some server administration procedures may be performed only at client components, server administrators must ◆ Perform administrative activities using evaluated clients only ◆ Ensure that the utilities used to perform server administration are included in the evaluation for that trusted client

Worms	A *worm* is an independent program that replicates itself from one site to another. Worms are typically not a problem within the NetWare client-server architecture. As with viruses, users cannot cause a worm to execute on a server, but a user may store worms on the server.
Trojan horse	A *Trojan horse* is malicious code that hides within a program and performs a disguised function. Again, nonadministrative users cannot plant a Trojan horse in the server’s TCB code, but may use the server file system for storage of Trojan horses that are intended to run on client components.
Bombs	A *bomb* is malicious code that is planted within an application or operating system and triggered by a clock time or an external event. If the server is administered as described in this manual, nonadministrative users cannot plant bombs that will affect other users.
Trap doors	A *trap door* is a mechanism built in to a system by its designer or administrator to give that person subsequent unauthorized access to the system. This threat is addressed at C2 by specifying the server’s interfaces and testing that they operate properly.

Spoofing	There are two types of spoofing threats within the NetWare enhanced security network. Spoofing of the server’s TCB functionality is not a problem, because there is no way for a user to load spoofing programs on the server. Packet spoofing is a classic problem in distributed systems. In a packet spoofing attack, a user at a network node generates packets that purport to be from an authorized network user (such as a user, an administrator, or another server). Spoofing attacks require: ◆ The ability to send arbitrary packets on the network, and ◆ Detailed knowledge about the internals of the network components. The NetWare Enhanced Security architecture provides various mechanisms to prevent delivery of messages with invalid source IPX™ network addresses. The server checks each incoming packet to determine that the packet has the proper IPX address of the purported sender. The NCP Packet Signature mechanism provides protection against packet spoofing attacks in environments where the network media is not protected. The checksum mechanism is not required in C2 networks because the media is assumed to be protected.
Wiretap attacks	An intruder performs a wiretap attack by connecting to the network and reading (passive wiretapping) or writing or modifying packets in transit (active wiretapping). NetWare Enhanced Security networks are assumed to be protected physically or cryptographically against wiretapping.

Browsing	NetWare Directory Services performs the necessary role of a name server within a multiple-server environment. During login, NDS provides essential name services to unauthenticated users. Depending upon the configuration of the NDS [Public] object, users can browse names in the NDS Directory or can query NDS for the presence of objects having the specified name. (See Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.) Authenticated users can also browse NDS and file system objects according to the user’s rights to those objects.
Unauthorized use	The server provides various mechanisms to prevent or to detect unauthorized use. This includes login time restrictions (in half-hour increments) and address restrictions to ensure that legitimate users cannot access the system outside of a particular usage profile. The server provides intruder detection mechanisms to lock users and/or workstations when it detects more than a specified number of bad login attempts within a specified period.
Denial of service	Denial of service is a consideration for any shared resource, such as disk space, communications bandwidth, or printers. The server provides audit mechanisms to track security-relevant operations and provides an accounting mechanism to charge users for use of network resources.

Server NTCB Partition

The TNI [NCSC-TG-005] describes a Network Trusted Computing Base (NTCB) as:

The totality of protection mechanisms within a network system—including hardware, firmware, and software—the combination of which is responsible for enforcing a security policy.

For NetWare Enhanced Security, the NTCB is distributed among multiple heterogeneous client and server NTCB partitions. The server NTCB partition contains the trusted hardware, firmware, and software that implement the security policies enforced by the server component.

Because untrusted software is not permitted on the server, the entire server is included in the server NTCB partition. The implications of this are:

- Administrators are not permitted to run arbitrary NLM programs on the server.
- New software can be added to the server and existing NLM programs can be modified only by Novell during the Rating Maintenance Phase (RAMP). All such changes are analyzed with respect to their effects on the server NTCB partition.

Users access the server's protected resources by running application programs at client workstations. These applications send the following types of protocol messages to the server to request the server to perform specific services:

NCP$^{\text{TM}}$ (NetWare Core Protocol)$^{\text{TM}}$	NCP includes approximately 500 messages that provide connection services, file system services, messaging services, queue/print services, NDS services, etc. See *Concepts*.
SMSP (Storage Management Services$^{\text{TM}}$ Protocol)	SMSP is used by backup software to backup and restore the server's file system and NDS data. The evaluated server includes facilities to act as both an SMSP client (namely, SBACKUP) and SMSP server. Evaluated clients may include facilities to act as clients and/or servers.
PSSCP (Print Server Status and Control Protocol)	PSSCP is used by printer users and operators (at network clients) to control printing of the current print job.
PCP (Printer Communications Protocol)	PCP is used to configure printers, send print jobs to printers, and determine the printer status. In the NetWare Enhanced Security configuration, all network printers are connected to a server, and PCP is a server-to-server protocol.

Building a Network TCB Using the Server Component

As an administrator of an evaluated C2 server, you are probably interested in determining how to build a Class C2 network system using the server. Can you connect different versions of servers or workstations from different vendors? What kinds of workstations can you use? What kind of cabling must you use?

The NetWare Enhanced Security architecture provides for the construction of an enhanced security system made up of multiple workstations and servers from multiple vendors. Because different products may provide different security features, Novell's network security architecture identifies products using the nomenclature in Appendix A of the *Trusted Network Interpretation* (TNI) document.

The TNI nomenclature characterizes components as supporting the following policy related features

- Mandatory Access Controls (M)
- Discretionary Access Controls (D)
- Audit (A)
- Identification and Authentication (I).

NetWare Enhanced Security components generally provide some or all of the D, A, and I features. However, certain components may be evaluated as M components.

The *Trusted NetWare Security NetWork Security Architecture and Design* (NSAD) document explains that NetWare enhanced security consists of three types of components: servers, clients, interconnections, and network media. The requirements for each are summarized in the following list.

NetWare 4.11 servers	The NetWare 4.11 server is evaluated as a C2 IAD component, which means that it provides Identification and Authentication (I), audit (A) and Discretionary Access Control (D) functions within the enhanced security architecture. The architecture allows you to connect an arbitrary number of NetWare 4.11 servers within your network.
Other server components	NetWare Enhanced Security also permits you to use other server components within your network.These servers must be evaluated as C2 or higher security with respect to NetWare Enhanced Security architecture, and may provide one or more of the IAD security functions. The architecture does not permit use of unevaluated servers such as NetWare 3.11, NetWare 4.01, or NetWare 4.1.

Client workstations	The architecture permits an arbitrary number of single-user client workstations, potentially from different vendors.These products must be evaluated as C2 or higher security with respect to NetWare Enhanced Security architecture, and may provide none, some, or all of the IAD security functions. In particular, a diskless workstation might be evaluated as a class C2 nil component. This means that the work station does not provide local enforcement of Identification and Authentication, Direct Access Control, or Auditing, but is capable of being securely used within the enhanced security network. Other workstations that provide and manage shared storage for multiple sequential users might be evaluated as Class C2 DI or IAD components.
Interconnection components	The architecture permits three types of interconnection components: routers, bridges, and repeaters. Routers operate at the internetwork layer (layer 3) of the protocol stack and perform routing of IPX messages from one network segment (subnetwork) to another. Bridges operate at the link layer (layer 2) and send packets from one local area network to another. Repeaters operate at the physical layer (layer 1) by copying data from one cable to another.
NetWork media	Network media components are usually nil components, such as passive cabling.

The network security architecture provides various methods for meeting network security requirements such as prevention of "spoofing" certain protocol-based TCB functions.

You can compose a trusted Class C2 network system by interconnecting an arbitrary number of NetWare 4.11 servers, other servers, client workstations, and passive network cabling.

To determine the ratings of server and client workstation components, ask the vendor for the Evaluated Products List (EPL) entry for the product. Determine that the product

- Is currently listed on the EPL
- Was evaluated with respect to the Trusted Network Interpretation (TNI) and the Trusted NetWare Network Security Architecture and Design (NSAD)
- Is connected as described in Appendix W, “Network Composition Rules,” on page 377.

If a potential vendor is unable to provide this information, the product is probably not evaluated and is not approved for use in a C2 facility.

In addition to using C2 evaluated products, you must also provide the following protection for all servers and physical media.

- Because there is no login provided at the server console, all servers and their consoles must be physically protected. The form of protection can vary from a locked room to a guarded area.

  Console access may be granted to one or more administrators, and it is possible for multiple administrators to have access to the console at the same time.

  To provide traceability of administrative actions performed at the console, administrators must maintain a handwritten log at the console that lists the user, date and time the user started, and date and time the user finished.

- The network media (cabling, routers, etc.) must also be physically protected to prevent wiretapping attacks.

Security Mechanisms

This section summarizes the protection mechanisms that are provided by the server's NTCB partition. Some of these mechanisms occur transparently, while others must be invoked by the user or administrator.

- NetWare Enhanced Security systems are trusted to protect information—that is, to allow access to data objects only in accordance with the system's access control policies.

  The server implements separate DAC policies for NDS objects, NDS object properties, and file system objects (FSOs). These policies permit access based on a user's "need to know," as defined by authorized administrative or nonadministrative users.

- The access control mechanisms provided by the server component depend upon the principle of individual accountability. That is, each user must be identified and authenticated on some network component before that user is allowed access to the server's protected resources. The user's subsequent security-relevant actions must also be traceable.

  Identification and Authentication (I&A) requires the user to enter a security token ("This is who I am…") and authentication token ("…and here is some secret information to prove it.") The server provides traceability by allowing an auditor to audit security-relevant events within the system.

- Finally, the server provides assurances that the security policies are implemented correctly and that the system is "self-protecting."

  These assurances are provided by architectural mechanisms, by administratively precluding the execution of untrusted NetWare Loadable Module (NLM) programson the server, and by testing to demonstrate that the server works as documented.

The trust provided by the server component (within the NetWare Enhanced Security architecture) depends equally upon individual accountability for network users, proper operation of the discretionary access policy mechanisms, assurances that the server is implemented correctly, and isolation of the server from untrusted software.

The following paragraphs summarize the protection mechanisms provided by the NetWare Enhanced Security server component.

Identification and Authentication

The server allows interactive logins by users from workstation components throughout the network. Each user is identified and authenticated on some network component before that user can make any use of server resources.

The authentication mechanism is based on a user's login identifier and private password. The login identifier is unique for each individual. The password is a private text string associated with a user identifier, known only by the user, and recognizable by the server NTCB.

The server stores the password and user ID as an encrypted hashed value in an attribute of the User object within the NetWare Directory database. Authentication data is protected in the server through the use of Discretionary Access Control and encryption.

NetWare 4.11 authentication consists of two parts: network login and background authentication.

- In network login, a workstation component acting on behalf of a user participates in a protocol with the server component to obtain a credential and signature (based on the user's Rivest, Shamir, Adelman (RSA) private key), using the user's identity and password.

- Once the credential and signature are obtained, the background authentication protocol allows a workstation component to present the credential and signature to any server component, and thus gain services from that server.

Using the NetWare 4.11 login scheme, the server component provides a network login that allows access to all server components in the network and their resources. Thus, it is not necessary to log in separately to each server in the network.

Each user may have as many as three types of associated login restrictions:

- The days of the week and times of day when logins are permitted
- An account balance
- The list of IPX addresses that can be used to originate connections.

Logins that are otherwise successful (the correct password is provided) when any of these login restrictions are in effect are audited.

Approximately every half hour (on the hour and half-hour) the user’s login time and account balance restrictions are revalidated. If the authorized time limit or account balance has been reached, the user’s connection to that server is terminated.

The server provides a flexible intruder detection mechanism to detect and prevent brute-force password guessing attacks. If the number of incorrect login attempts exceed the specified parameters, the server locks that station for a configurable period of time (or until the station is enabled by an administrator).

The server also provides a NetWare 3.*x* login method that uses the same authentication materials, but uses different protocol messages to transfer the authentication materials to the server.

In a NetWare 3.*x* login, the user logs in to a “bindery context” on a single server as described in Appendix W, “Network Composition Rules,” on page 377.

Discretionary Access Control

The server NTCB partition enforces DAC policies for all named objects under its control. These policies are based on user identity, where each user has the same identity on all servers. To enforce these access controls, users must be identified and their identities authenticated.

The primary named objects controlled by the server’s NTCB partition are NDS objects, NDS object properties, and file system objects (FSOs). Each of these objects has a separate access control policy.

An overview of these policies is not presented here. For a description of the access controls on NDS objects and NDS object properties, see

- Chapter 2, “Security Supplement to Guide to NetWare 4 Networks,” on page 43
- Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91
- *Guide to NetWare 4 Networks*
- Chapter 1, “Managing NetWare Directory Services Objects,” of *Supervising the Network*
- *Concepts*

For information on file system access controls, see

- Chapter 5, “Security Supplement to Managing Directories, Files, and Applications,” on page 129
- Chapter 2, “Managing Directories, Files, and Applications,” of *Supervising the Network*

In addition to the primary named objects, other types of named objects include messages, semaphores, logical record locks, queues, queue entries, currently printing jobs, and audit trails. Each of these has an access control policy.

The policies for some types of objects cannot be changed. For example, the access policy for messages is that only the recipient of the message may read or delete it, while the acess policy for logical record locks and semaphores is that any user may lock or unlock the resource.

By contrast, queues have a confgurable access policy that the creator of the entry and all queue operators can modify. Audit trails have a configurable access policy described in *Auditing the Network*.

Audit

The server component provides three types of audit trails:

- **NDS audit trails** are associated with NDS containers (and therefore are known as "container auditing"), and are replicated along with the containers. The auditor may pre-select NDS auditing on a per-event or per-user basis.

- **File system audit trails** are associated with volumes within the server. The auditor may pre-select file system audits on a per-event, per-user, or per-file basis.

- **Workstation audit trails** are stored and protected on the server. The form and content of workstation audit trails is uninterpreted by the server component.

The server audit system accepts messages (NCPs) to configure audit characteristics, including pre-selection attributes, audit trail sizes, and what action the server should take when an audit trail fills. Additional NCPs are used to read audit trails for post-processing.

Human interfaces to generate configuration and post-processing NCPs are provided by workstation components, and therefore are not discussed further in this manual. For additional information, see *Auditing the Network.*

The audit trails containing audit records are protected by discretionary access controls. Audit trails are stored in a protected portion of the file system that is not accessible to file operations. Instead, specific NCP operations are used to read audit trails. Only users with sufficient rights to the audit trail NDS object may execute the audit NCP operations.

The server component includes mechanisms to control the loss of audit data. Warnings are provided as the size of the audit file reaches an administrator-defined threshold.

For container auditing, the administrator may elect to do one of the following:

- Continue without auditing if the benefits of so doing outweigh the risks as described in *Auditing the Network*.
- Continue but disallow any events which would require auditing (that is, events which are not auditable are allowed, but auditable events are refused).
- Roll over to a new audit file, possibly deleting old audit data.

For volume auditing, the administrator may elect to do one of the following:

- Continue without auditing if the benefits of so doing outweigh the risks as described in *Auditing the Network*
- Continue but disallow any auditable events
- Roll over to a new audit file, possibly deleting old audit data

For workstation auditing, the administrator may elect to

- Refuse to accept additional audit records
- Roll over to a new audit file, possibly deleting the old audit data

Object Reuse

The server enforces an object reuse policy to prevent scavenging of information for storage objects. In general, objects are cleared prior to their release to a subject.

System Integrity

System integrity tests required for the server are described in the Technical Support area of the Novell, Inc. World Wide Web site (http://www.novell.com). These tests may be run whenever you like. Their purpose is to verify that your server hardware and firmware are operating properly.

Administrative Users

NetWare administrators are responsible for the following areas of network operation:

- Configuring, installing, and maintaining the system hardware and installing the server software. For more information, see *Installation* and Chapter 3, “Security Supplement to Installation,” on page 69.
- Managing the NetWare Directory database.

  NDS provides the view of a single network system with one user community, one set of objects, and one access control policy. This permits administrators to partition its user community and objects into smaller sets (namely countries, organizations, and organizational units) for ease of administration.

  For more information, see Chapter 3, “Security Supplement to Installation,” on page 69 and Chapter 5, “Security Supplement to Managing Directories, Files, and Applications,” on page 129.
- Accounts administration. Because user accounts are represented as NDS user objects, accounts administration primarily involves managing the NDS User objects that represent the user accounts.

  For more information on accounts administration, see “User Account Administration (Client)” on page 116.
- Managing the server’s file system. For more information, see Chapter 5, “Security Supplement to Managing Directories, Files, and Applications,” on page 129.
- Loading and running NetWare Loadable Module (NLM) programs. For more information, see Chapter 10, “Security Supplement to Maintaining the NetWare Server,” on page 151.
- Configuring and auditing the security of the server. For more information on audit administration, see *Auditing the Network*.

- Performing backups. For more information, see Chapter 12, “Security Supplement to Backing Up and Restoring Data,” on page 165.

- Helping users with their problems.

As mentioned previously, some of these operations are performed at the server console while other operations are performed at remote client workstations.

As an administrator, you must be extremely careful when you are working at the server console. The parameters you set and the NLM programs you load directly affect the security provided by the server component.

You must also be extremely careful when you are logged in as an administrator at a network client, because your account has permissions to access and modify the access permissions enforced by the server.

Software Distribution

Your NetWare server comes packaged in a box containing several manuals, several CD-ROMs (or floppy diskettes) containing the software and documentation, and a floppy disk that contains your NetWare license.

To ensure that no one has tampered with your NetWare software, when you receive your copy of NetWare you should verify that Novell’s original seal is on the box. After you open the box, you should verify that:

- The NetWare software and documentation CD-ROMs (or floppy diskettes) are in their original shrink-wrap

- The license diskette is in its original envelope printed with the Novell license, and that the seal on the envelope is unbroken

Warning If the NetWare operating system does not recognize your license diskette, this may indicate that someone has tampered with your distribution.

Your NetWare CD-ROMs (or diskettes) and license diskette must be physically protected in case you need them to reinstall your server software.

Novell provides NetWare patches through its NetWire^{SM} online bulletin board, as well as through the Internet and certain commercial service providers.

When downloading patches, ensure that the site you are downloading from is a valid Novell site.

In addition, if you are running in the NetWare Enhanced Security configuration, you should only download those patches identified as having been included in the evaluated product.

chapter 2

Security Supplement to Guide to NetWare 4 Networks

This chapter contains supplementary NetWare® Enhanced Security information for *Guide to NetWare 4 Networks*. For a network using NetWare Enhanced Security servers, this chapter supersedes the *Guide to NetWare 4 Networks*.

Introduction

The NetWare Enhanced Security server provides compatibility with NetWare 3™ applications through Bindery Emulation. However, NetWare 3 servers are not included in the NetWare Enhanced Security architecture.

Part I—Project Approach

Project organization, training, and scheduling are important management functions when installing a trusted network using NetWare Enhanced Security servers and evaluated workstation products. The same general approach outlined in *Guide to NetWare 4 Networks* is also relevant for trusted networks.

However, there are additional tasks and additional responsibilities that must be considered when designing and installing a trusted network. For example:

- Unevaluated workstations, servers, or routers cannot be used within a trusted network.
- Even evaluated components cannot be used indiscriminately on the network.

Appendix W, “Network Composition Rules,” on page 377 describes how to determine whether a particular server or workstation can be used with other components as part of a trusted network in accordance with the network security architecture.

- NetWare Loadable Module^{TM} (NLM^{TM}) programs cannot be used indiscriminately on the NetWare Enhanced Security server. You may use only the server hardware and software identified in *NetWare Enhanced Security Server*.

- The trusted facility documentation for the NetWare Enhanced Security server includes this mnanual, *NetWare Enhanced Security Server*, and *Auditing the Network*.

  For trusted facility purposes, these documents supersede any other guidance on designing and implementing a NetWare 4 network. Consequently, you must have at least one team member with an in-depth understanding of this documentation.

  Project team training must also ensure that other members of the team become familiar with the NetWare Enhanced Security server’s trusted facility documentation.

- Because a trusted network includes evaluated components in addition to the NetWare Enhanced Security server—workstations from various vendors, for example—your project team must also become familiar with the trusted facility documentation for each additional component.

Part II—Design

Careful design of the NDS structure is essential to proper security.

Designing the Directory Tree Structure

The following sections relate to Chapter 3, “Designing the Directory Tree Structure” of *Guide to NetWare 4 Networks*.

Schema Extension

Warning The NDS schema can be modified and expanded to suit the needs of your facility. In order to modify the schema, a user must have the Supervisor right on the [Root] object. To avoid damage to the schema, do not give this right to untrusted users.

For additional information and warnings about schema extensions, see “Monitoring and Maintaining Time Synchronization” in *Supervising the Network*

Using a Naming Standards Template

Table 3-1 in *Guide to NetWare 4 Networks* refers to autodialing software and interdepartmental mail carriers. As identified in *NetWare Enhanced Security Server*, the NetWare Enhanced Security server does not include this software.

Compatibility

NetWare Client, NETX, and DOS are workstation client software. For identification of the trusted software that your workstation provides, see your workstation documentation.

Warning INETCFG.NLM is not included in the server’s NetWare Enhanced Security configuration. If you load and run INETCFG on an evaluated server, the server is no longer running in an NetWare Enhanced Security configuration. For more information on the evaluated configuration, see *NetWare Enhanced Security Server*.

Warning

NDS provides interoperability with previous NetWare products (such as NetWare 2 and NetWare 3 clients and servers) and with third-party products. However, the network security architecture requires all servers in a trusted network to be evaluated NetWare 4 servers, such as the NetWare Enhanced Security server addressed in this manual.

If you have any unevaluated servers—NetWare 2 or NetWare 3 servers, for example—on the network, there is no basis for trust in the overall network.

Planning the Directory Tree Structure

Warning

The NetWare Enhanced Security configuration identified in *NetWare Enhanced Security Server* does not permit you to install WAN hardware or NLM programs directly on the server. If your network requires wide area networking, you can use only evaluated router components to provide the WAN connectivity. Use of unevaluated components, such as routers or servers, violates the basis for trust in the entire network.

Reviewing the Directory Tree Structure

As explained in Chapter 3, “Security Supplement to Installation,” on page 69 you cannot upgrade an existing NetWare 2.*x*, 3.*x*. or 4.*x* server to a NetWare Enhanced Security configuration. If you are currently running an unevaluated version of NetWare (for example, NetWare 3.11 or 4.01) on your server, you must perform a complete installation of the server.

Identifying Leaf Object Types

AFP, MHS, and NLS NLM programs are not included in the NetWare Enhanced Security server’s evaluated configuration. It is possible to create the AFP Server and LSP Server and the MHS-related objects (Distribution List, External Entity, Message Routing Group, Messaging Server), but there is no meaningful way to use them. For more information on the evaluated configuration, see *NetWare Enhanced Security Server*.

NetWare Enhanced Security includes only NetWare 4 servers in the network security architecture. All servers must be NetWare 4 Enhanced Security servers, or equivalent. Consequently, you should not create NetWare Server objects for servers that are not running NetWare 4.

NetWare Administrator, NETADMIN, AUDITCON, and PCONSOLE are NetWare client utilities. To determine whether these utilities are included in the workstation's evaluated configuration, see your trusted workstation vendor's documentation.

Defaults

You cannot upgrade an existing NetWare 2, NetWare 3, or NetWare 4 server to a NetWare 4.11Enhanced Security configuration. If you are currently running an unevaluated version of NetWare (for example, NetWare 3.11 or 4.01) on your server, you must perform a complete installation of the server.

Determining a Partition and Replication Strategy

The following material relates to Chapter 4, "Determining a Partition and Replication Strategy" of *Guide to NetWare 4 Networks*.

The NetWare Enhanced Security configuration identified in *NetWare Enhanced Security Server* does not permit you to install WAN hardware or NLM programs directly on the server. If your network requires wide area networking, you must use evaluated router components to provide the WAN connectivity.

Designing Partition Boundaries

NDS Manager and PARTMGR are NetWare client utilities. To determine whether these utilities are included in the workstation's evaluated configuration, see your trusted workstation vendor's documentation.

Basic Functions of Replicas

Always keep current backup copies of your NetWare Directory tree, regardless of how many servers you have. For more information on the use of the NetWare Enhanced Security backup tools, see Chapter 3, "Security Supplement to Installation," on page 69.

Note that the backup software does *not* back up certain auditing information.

Planning Replica Placement

You cannot upgrade an existing NetWare 2.*x*, 3.*x*. or 4.*x* server to a NetWare 4.11Enhanced Security configuration. If you are currently running an unevaluated version of NetWare (for example, NetWare 3.11 or 4.01) on your server, you must perform a complete installation of the server.

Defaults

You cannot upgrade an existing NetWare 2.*x*, 3.*x*. or 4.*x* server to a NetWare 4.11 Enhanced Security configuration. If you are currently running an unevaluated version of NetWare (for example, NetWare 3.11 or 4.01) on your server, you must perform a complete installation of the server.

Planning the Time Synchronization Strategy

The following material relates to Chapter 5, “Planning the Time Synchronization Strategy,” of *Guide to NetWare 4 Networks*.

Time synchronization is important for keeping the relative order of recorded audit information within a multiserver network. In general, the NDS time synchronization mechanisms are sufficient to keep all server audit files consistent.

If you modify Time Synchronization parameters, be sure to monitor the clocks for the various servers to ensure that each server keeps its clocks in sync throughout the network.

The NetWare Enhanced Security configuration identified in *NetWare Enhanced Security Server* does not permit you to install WAN hardware or NLM programs directly on the server. If your network requires wide area networking, then you must use evaluated router components to provide the WAN connectivity.

External Time Sources

The server also uses time stamps for auditing security-relevant events. Use an external time source within your network only if you have confirmed that the source is sufficiently accurate for both audit and NDS replication purposes.

You cannot indiscriminately add hardware (for example, time source receivers) and software (synchronization NLM programs) to a NetWare Enhanced Security server. For identification of the NetWare Enhanced Security server configuration, see *NetWare Enhanced Security Server*.

Creating an Accessibility Plan

The following material relates to Chapter 6, "Creating an Accessibility Plan," of *Guide to NetWare 4 Networks*.

The NetWare Enhanced Security configuration identified in *NetWare Enhanced Security Server* does not permit you to install WAN hardware or NLM programs directly on the server. If your network requires wide area networking, then you must use evaluated router components to provide the WAN connectivity.

Identifying Network Connection Types

Warning

While a user's connection is attached but not authenticated, the user can perform any actions permitted for the [Public] object. Thus, if [Public] has Browse rights to the NDS [Root] object, an unauthenticated user can browse the NDS tree.

The unauthenticated user can also observe the names of User, Group, Server, and other objects and can even search the Directory for objects having certain characteristics. Further, because the user is not authenticated, these actions cannot be associated with a specific individual.

DOS, Windows, OS/2, Macintosh, and UNIX are client operating systems, and NetWare client software exists for each of these client environments. To determine which client software to use on your workstation, see your workstation vendor's trusted facility documentation.

Identifying User Types

The distinction between local and mobile users is largely irrelevant with respect to the security of the network. In an enterprise network, any user can log in to the network from any client that permits access.

However, the network security architecture does not include any components (for example, terminal servers) that would permit users to access the enterprise network from public telephone networks or switched data networks.

Identifying Global and Shared Resources

The NetWare Enhanced Security server configuration identified in *NetWare Enhanced Security Server* does not permit you to install WAN hardware or NLM programs directly on the server. If your network requires wide area networking, you must use evaluated router components to provide the WAN connectivity.

The NetWare Enhanced Security server does not include any NLM programs to support applications such as E-mail. For a definition of the software that is permitted for the NetWare Enhanced Security server, see *NetWare Enhanced Security Server*.

Identifying Bindery Services Needs

NDS Manager and PARTMGR are NetWare client utilities. To determine whether these utilities are included in the workstation's evaluated configuration, see your trusted workstation vendor's documentation.

Determining What Objects to Create

The NetWare Enhanced Security server is not distributed with a GUEST account. You can create a GUEST account, but doing so is discouraged for the following reasons:

- GUEST accounts were used in previous versions of NetWare, usually without passwords, in support of the print CAPTURE command (see *Print Services*). Creation of a GUEST account could cause confusion with this previous usage.

- A GUEST account suggests a shared account that can be used by anyone. The principle of individual accountability requires that accounts are *not* shared by multiple users.

  If you create a GUEST account, it must be associated with a specific person and must have a password to prevent its use by other individuals.

Warning

The bindery SUPERVISOR login is separate from the NDS ADMIN object and cannot be deleted. The bindery SUPERVISOR login is inaccessible only if the bindery context is null.

Protect the SUPERVISOR account by assigning and safeguarding a password. Compromise of the SUPERVISOR bindery account is as dangerous as compromise of the ADMIN NDS account.

The system administrator must set the bindery SUPERVISOR login password to something other than the password used for the ADMIN account. In addition, the bindery SUPERVISOR account should not be used for network administration.

The bindery SUPERVISOR is not an NDS object and differs from an NDS User object in several ways. It cannot be a trustee of an NDS object, but it does have the Supervisor right to all volumes on its server.

The bindery SUPERVISOR is associated with an individual server, and not with a container. Changing the bindery SUPERVISOR password on server A does not change the bindery SUPERVISOR password on server B.

Warning

The bindery SUPERVISOR has the Supervisor right to the containers specified in the SET BINDERY CONTEXT parameter. The SET BINDERY CONTEXT parameter can only be used to include containers for which the server holds a replica. Therefore, at most, the bindery SUPERVISOR has the Supervisor right to all NDS objects held on the server.

Warning: When you back up your system, the SUPERVISOR login does not get backed up with the NDS objects or the file system objects.

Warning: While the bindery SUPERVISOR account initially has the same password as ADMIN, its password is not changed by changing ADMIN’s password, nor is it disabled by disabling (or deleting) the NDS ADMIN object.

Warning: Creating a SUPERVISOR object in an NDS container and changing its password or disabling it does not have any affect on the bindery SUPERVISOR login.

Trusted NetWare does not support upgrades from an unevaluated server (for example, NetWare 3) to an evaluated C2 configuration (such as NetWare 4). Therefore, the conversion of bindery files will not occur.

Determining an Efficient Access Control Method

“Security Mechanisms” on page 33 summarizes the security features that are provided by the NetWare Enhanced Security server. These include:

- Identification and Authentication of users at client workstations, during initial network login and subsequent background authentication.
- Implementation of a Discretionary Access Control (DAC) policy for the server’s protected resources, including NDS objects, NDS object properties, and file system objects.
- The ability to record security-relevant events that occur on the server, along with the identity of the user that caused the event.
- The ability to protect residual data in the server’s storage objects (such as memory buffers and disk storage) from being accessed by subsequent users.
- Extensive trusted facility documentation (such as this manual, *NetWare Enhanced Security Server*, and *Auditing the Network*) to assist network administrators in proper configuration and operation of the trusted facility.

As described in Chapter 6, “Security Supplement to Creating Login Scripts,” on page 137, when a user logs in to a NetWare server, the LOGIN.EXE program downloads the user’s login script from the server and executes the script.

Because scripts are executed only on the workstation, they do not affect the server’s access control enforcement. To determine how to use login scripts on your workstation, see your workstation vendor’s trusted facility documentation.

Security Equivalence

Whether a user can search and navigate the NetWare Directory tree and perform other actions within the Directory depends, in part, on the rights assigned to the [Root] object and the [Public] object.

- Through security equivalence, rights assigned to the [Root] object apply to all authenticated users.

- Rights assigned to the [Public] object apply to unauthenticated users as well as to authenticated users.

Warning Because rights assigned to the [Public] object are available to unauthenticated users, be extremely careful about giving unnecessary rights to the [Public] object. For example, if you give [Public] Browse rights to [Root], users that are not logged in will be able to browse the Directory tree and search for object names.

Warning Because rights assigned to the [Root] and [Public] objects are available to all authenticated users, be extremely careful about giving unnecessary rights to these objects. For information on safe access rights for these objects, see Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.

Effective Rights

An object’s effective rights to another object depend on explicit trustee assignments, inheritance, inherited rights filtering, and security equivalences. For detailed examples of effective rights calculations, see “Effective rights” on page 228.

Object Rights

In the “Object Rights” table (in *Guide to NetWare 4 Networks*), it is not necessary to have the Browse right to verify the existence of an object’s name. The Browse right is used only when searching.

File System Attributes

Some file and directory attributes (such as Execute Only) are advisory information that client workstations may use to supplement the NetWare file system access control policy. For more information on attributes, see Chapter 19, “Security Supplement to Concepts,” on page 221.

To determine whether these attributes are enforced by your workstation, see your workstation vendor’s trusted facility documentation.

Warning Because the server does not enforce all file and directory attributes, you should not rely on attributes for protection of sensitive information. Instead, you should use NetWare file and directory rights, which are enforced by the server.

Login and Profile Scripting

As described in Chapter 6, “Security Supplement to Creating Login Scripts,” on page 137, login scripts are executed only on the workstation and do not affect the server’s access control enforcement. To determine how to use login scripts on your workstation, see your workstation vendor’s trusted facility documentation.

User Object ADMIN

Although INSTALL only creates one administrative user object (ADMIN), this does not mean that you must limit the network to only one administrator.

If you have more than one administrator, you must create an administrative account (a User object) for each administrator and give each user the Supervisor object right to the [Root] object. When this is completed, you can delete the ADMIN object or disable Supervisory permissions to [Root].

Warning

Do not delete the ADMIN object until you have provided, and tested, an alternate means of getting Supervisory access to [Root].

Providing individual administrative accounts has the following benefits:

- A separate administrative account for each administrator, each with its own password, provides individual accountability of administrative users. It also helps meet the *Trusted Network Interpretation* requirement to audit all actions taken by computer operators and system administrators. (Auditing of administrative actions at the server console is performed manually.)

- Having multiple administrative accounts provides a means for correcting any situations where an administrator inadvertently deletes his or her administrative account.

- If your administrative accounts are subject to attack, disabling the ADMIN account (but leaving it in place) may cause intruders to attack that account rather than other administrative accounts.

If the administrator also functions part-time in a nonadministrative role, create two accounts (for example, MSMITHand MSMITH-ADM). Give the administrative object (MSMITH-ADM) the Supervisor right to the [Root] object and give the nonadministrative object (MSMITH) default user rights.

When the administrator logs in an administrative role, he or she uses the administrative account. When the administrator is performing nonadministrative work, such as editing documents, use the nonadministrative account. For more information on creating user accounts, see Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.

Warning

Because administrative accounts have permissions that affect more than the account itself, you must protect your administrative password. Do not enter your password at unevaluated client workstations or for untrusted utilities running on an evaluated workstation. Do not write your password down or share it with other users or administrators.

Designing a Data Protection Plan

The following sections relate to Chapter 7, “Designing a Data Protection Plan,” of *Guide to NetWare 4 Networks*.

Establishing a Redundant Hardware System

NetWare SFT III support is not provided in the server’s NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Developing a Backup and Restore Strategy

The server’s NetWare Enhanced Security configuration does not include the following backup software:

- Third-party backup packages
- Target Service Agents (TSAs) for earlier NetWare releases, such as NetWare 3.11 or 4.01
- TSAs for NetWare SQL™
- TSAs for NetWare clients

For a listing of the NetWare Enhanced Security software, see *NetWare Enhanced Security Server*. For information on the SMS architecture for a NetWare Enhanced Security server, see Chapter 12, “Security Supplement to Backing Up and Restoring Data,” on page 165.

Data Protection Guidelines

For the names and versions of the backup NLM programs for the NetWare Enhanced Security server, see *NetWare Enhanced Security Server*. In a NetWare Enhanced Security configuration, you should not necessarily use the latest version of the backup software. You must only use the versions specified in *NetWare Enhanced Security Server*.

Periodically check with Novell for updates to *NetWare Enhanced Security Server*, which will list specific names and versions of backup software, drivers, and other server software. You cannot replace your NetWare Enhanced Security software with newer versions unless the newer version is listed in *NetWare Enhanced Security Server*.

If you upgrade any software on your server, it must be from a reliable source. Reliable sources include Novell's NSEPro CD-ROM, Novell's NetWire source, and Novell's Wide World Web site. Do *not* load software from other Web sites.

Designing an Application Management Strategy

The following material relates to Chapter 8, "Designing an Application Management Strategy," of *Guide to NetWare 4 Networks*.

Novell's Yes Program

For the NetWare Enhanced Security server, the Novell Yes program is used to identify the specific server, network, storage, and printer hardware that may be used in a NetWare Enhanced Security server. As specified in *NetWare Enhanced Security Server*, any hardware (and associated machine-dependent drivers and configuration files) in the four Yes categories can be used with the server provided the hardware

- Is Yes-certified
- Meets the specific Enhanced Security requirements stated in *NetWare Enhanced Security Server*.

Note that *NetWare Enhanced Security Server* prohibits loading certain NLM programs (for example, database NLM programs) on a NetWare Enhanced Security server, even if the NLM program is Yes-certified.

Using NetWare Application Management Tools

The NetWare Administrator, NetWare Application Manager (NAM), and NetWare Application Launcher (NAL) are client utilities. To determine whether you can use these utilities on your workstation, see your workstation vendor's trusted facility documentation.

Identifying Efficient Licensing and Metering Tools

The NetWare Licensing Service NLS. NLM program is not included in the server's NetWare Enhanced Security configuration. For more information on the server's evaluated configuration, see *NetWare Enhanced Security Server*.

Application Management Guidelines

NetWare Application Manager, NetWare Application Launcher, and the FLAG utility are client utilities. To determine whether you can use these utilities, see your workstation vendor's trusted facility documentation.

Part III—Implementation

You cannot upgrade from a previous unevaluated version of NetWare or another network operating system to a NetWare Enhanced Security server.

As described in Chapter 3, "Security Supplement to Installation," on page 69, you must install the NetWare Enhanced Security server from scratch, then define such necessary configuration data as User and Group objects.

Developing a Migration Strategy

The following sections relate to Chapter 9, "Developing a Migration Strategy," of *Guide to NetWare 4 Networks.*

Warning

You cannot migrate a previous unevaluated version of a NetWare server or another network operating system to an NetWare Enhanced Security server. Consequently, you must provide a manual means (such as creating new NDS objects with the desired attributes, creating new server configuration files, and copying client utilities) to move this data to the NetWare Enhanced Security server.

Determining a Client Migration Method

The following operating systems, client protocol software, utilities, and topics listed in this section apply primarily to workstation clients. See your trusted workstation vendor's documentation to determine whether the following software and capabilities are included in your workstation's evaluated configuration.

- Operating systems: DOS, Windows, Windows 95, OS/2, Mac OS, Windows NT, UNIX
- Client protocol software: NetWare Client, NetWare Client 32, Personal NetWare, NetWare NFS Services, NETX
- Other software: NWSTART, NWSTOP, ODI and NDIS drivers, NetWare Application Launcher, NT File Manager
- Topics: Migration of client software to NetWare 4, workstation backup, Automatic Client Upgrade

The NetWare Enhanced Security server configuration does not include the NLM programs required for SNMP, dynamic host configuration (DHCP), or client based backup using SMS. For more information on the server software configuration, see *NetWare Enhanced Security Server*.

The NDS protocol uses RSA public key encryption to protect against active wiretap attacks on the network media. The use of RSA encryption and packet signature, by itself, is not sufficient to meet the network security requirements.

Determining a Server Migration Method

Warning None of the automatic upgrade methods listed in *Guide to NetWare 4 Networks* are approved for upgrading an earlier NetWare server or another vendor's server to a NetWare Enhanced Security configuration.

None of the various automatic upgrade methods have been confirmed to leave the upgraded server in a configuration that is consistent with the other guidance in this manual. This includes NDS object and property rights, file system trustee rights, and password configuration.

The only permissible method for migrating bindery objects to a NetWare Enhanced Security configuration is to install the NetWare Enhanced Security server (in accordance with Chapter 3, “Security Supplement to Installation,” on page 69) and then to manually create new NDS objects with the desired attributes.

The only permissible method for migrating file system objects is to manually copy those files to the NetWare Enhanced Security server and manually set the desired trustee rights.

Maintaining Bindery Services in a NetWare 4 Environment

The NetWare 4.11 Enhanced Security server provides emulation for those NetWare 3 NetWare Core Protocol (NCP) messages that request services from the bindery.

Bindery services permits existing NetWare 3 applications (which expect to find the bindery, but not NDS) to interact with the NetWare Directory database on a NetWare 4.11 server as if it were a NetWare 3 bindery-based server.

Setting a Bindery Context

The server performs bindery services by mapping bindery requests to objects within the NetWare Directory tree. Bindery services are controlled by setting the bindery context to the location within the tree where the emulated objects are stored.

Warning

You can disable bindery services (and the processing of the associated bindery NCP messages) by executing the command “SET BINDERY CONTEXT=” (setting Bindery Context to a null string) at the server console or including it in the server’s AUTOEXEC.NCF file. However, if you disable the bindery context, NetWare 3 applications that require the bindery will not work.

NDS Manager and PARTMGR are NetWare client utilities. to determine whether you can use these utilities on your workstation, see your trusted workstation vendor’s documentation.

Planning Bindery Services

The NetWare Enhanced Security server is not distributed with a GUEST account. You can create a GUEST account, but doing so is discouraged for the following reasons:

- GUEST accounts were used in previous versions of NetWare, usually without passwords, in support of the print CAPTURE command (see *Print Services*). Creation of a GUEST account could cause confusion with this previous usage.

- A GUEST account suggests a shared account that can be used by anyone. The principle of individual accountability requires that accounts are *not* shared by multiple users.

  If you create a GUEST account, it must be associated with a specific person and must have a password to prevent its use by other individuals.

Warning

The bindery SUPERVISOR login is separate from the NDS ADMIN object and cannot be deleted. The bindery SUPERVISOR login is inaccessible only if the bindery context is null.

Protect the SUPERVISOR account by assigning and safeguarding a password. Compromise of the SUPERVISOR bindery account is as dangerous as compromise of the ADMIN NDS account.

The system administrator must set the bindery SUPERVISOR login password to something other than the password used for the ADMIN account. In addition, the bindery SUPERVISOR account should not be used for network administration.

The bindery SUPERVISOR is not an NDS object and differs from an NDS User object in several ways. SUPERVISOR cannot be a trustee of an NDS object, but it does have the Supervisor right to all volumes on its server.

The bindery SUPERVISOR is associated with an individual server, and not with a container. Changing the bindery SUPERVISOR password on server A does not change the bindery SUPERVISOR password on server B.

Warning

The bindery SUPERVISOR has the Supervisor right to the containers specified in the SET BINDERY CONTEXT parameter. The SET BINDERY CONTEXT parameter can only be used to include containers for which the server holds a replica. Therefore, at most, the bindery SUPERVISOR has the Supervisor right to all NDS objects held on the server.

Warning

When you back up your system, the SUPERVISOR login does not get backed up with the NDS objects or the file system objects.

Warning

While the bindery SUPERVISOR account initially has the same password as ADMIN, its password is not changed by changing ADMIN’s password, nor is it disabled by disabling (or deleting) the NDS ADMIN object.

Warning

Creating a SUPERVISOR object in an NDS container and changing its password or disabling it does not have any effect on the bindery SUPERVISOR login.

As described previously, you cannot upgrade from a previous unevaluated version of NetWare or another network operating system to a NetWare Enhanced Security server.

Maintaining NetWare 3 Servers Using NetSync

Warning

NetSync requires an unevaluated NLM program (NETSYNC3.NLM) to be loaded on the server. This NLM program is not included in the NetWare Enhanced Security server configuration. Loading this NLM program invalidates the assumptions for trust in the entire network. For information about the evaluated server configuration, see *NetWare Enhanced Security Server*.

Warning

The network security architecture permits only evaluated NetWare 4 servers, such as the NetWare Enhanced Security server, to be used in a trusted network. If you install unevaluated servers (such as servers running NetWare 2.x, NetWare 3.x, or an earlier version of NetWare 4), you invalidate the basis for trust in the entire network.

Maintaining a Mixed NetWare 4 Environment

In addition to performance and administrative factors, you should install an evaluated version of NetWare 4 on all servers to ensure that the servers operate as described and as evaluated. Even though different versions of NetWare 4 and NetWare 3 interoperate, you invalidate the assumptions for trust in the network when you have NetWare 3 servers attached to the network.

As described previously, you cannot upgrade from a previous unevaluated version of NetWare (2.*x*, 3.*x*, 4.0, 4.01 or 4.1) to a NetWare Enhanced Security server.

NetWare Enhanced Security Server identifies the specific versions of the server NLM programs—for example, DS.NLM—that make up the NetWare Enhanced Security server configuration. You can only upgrade a server NLM program when

- The server is already in the NetWare Enhanced Security configuration
- A new version of *NetWare Enhanced Security Server* identifies newer versions of NLM programs for the NetWare Enhanced Security configuration

Because only NetWare 4.11 servers and their successors will occur in a trusted network, you can disregard Table 9-1 of the *Guide to NetWare 4 Networks*. That is, there should never be NetWare 4.01 or 4.02 servers on a trusted network.

Using NetWare 4.11 Utilities

Warning

NetWare Enhanced Security Server and Chapter 20, “Security Supplement to Utilities Reference,” on page 309identifies the server console utilities that are permitted for a NetWare Enhanced Security server. If you load any unevaluated NLM programs on a NetWare Enhanced Security server, you invalidate the basis of trust in the entire network.

For client utilities listed in Chapter 20, “Security Supplement to Utilities Reference,” on page 309, review your workstation vendor’s trusted facility documentation to determine whether the utility can be used on the workstation.

Establishing a Pilot System

NDS Manager and PARTMGR are client workstation utilities. To determine whether you can use these utilities on your workstation, see your workstation vendor's trusted facility documentation.

As described previously, you cannot migrate from a previous unevaluated version of NetWare or another network operating system to a NetWare Enhanced Security server. You can establish a pilot system to test this capability, but you will be unable to use it when setting up your network.

Implementing NetWare 4 Services

The following sections relate to Chapter 11, "Implementing NetWare 4 Services," of *Guide to NetWare 4 Networks*.

For a listing of TCB utilities that you can use at the workstation client to manage the NDS Directory, see your workstation vendor's documentation. Possible utilities include, but are not limited to, the following:

- NWADMIN (NetWare Administrator)
- NETADMIN
- PCONSOLE
- AUDITCON
- UIMPORT

Completing General Tasks

The Trusted NetWare architecture requires all of its workstations and servers to be trusted. Consequently, you must not interconnect your workstations and servers to an information superhighway that contains any components that are not evaluated using the same criteria and network security architecture as the NetWare Enhanced Security server. The problem is with interconnecting the server to nonevaluated components, not with having a country object below the [Root] object.

For information on migrating workstations to NetWare 4, see your workstation vendor's trusted facility documentation.

NetWare Administrator, NETADMIN, NDS Manager, PARTMGR, and PCONSOLE are client utilities. To determine whether you can use these utilities, see your workstation vendor's trusted facility documentation.

Implementing NDS on Various Network Types

The NetWare Enhanced Security server configuration uses only the IPX protocol stack. TCP/IP, SAA, and NACS are not included in the NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Part IV—Appendixes

The following sections relate to the appendixes in *Guide to NetWare 4 Networks*.

NDS Object Classes and Properties

This section relates to Appendix A, "NDS Object Classes and Properties," of *Guide to NetWare 4 Networks*.

The NetWare Enhanced Security server configuration does not include NLM programs to support AFP, MHS, and NLS services.

It is possible to create the AFP Server, the NLS-related objects (NLS Product, NLS License Certificate, and NLS License Server), and the MHS-related objects (CommExec, Distribution List, External Entity, Message Routing Group, and Messaging Server), but there is no software on the server to use them.

For more information on the server's evaluated configuration, see *NetWare Enhanced Security Server*.

Referencing and Using Leaf Objects

The following sections relate to Appendix B, “Referencing and Using Leaf Objects,” of *Guide to NetWare 4 Networks*.

Messaging-Related Leaf Objects

MHS is not included in the NetWare Enhanced Security server configuration. It is possible to create the various MHS-related leaf objects, but there is no meaningful way to use them.

For more information on the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

NetWare Licensing Services Leaf Object

NLS is not included in the NetWare Enhanced Security server configuration. It is possible to create the LSP Server object, but there is no meaningful way to use it.

For more information on the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Server-Related Leaf Objects

AFP is not included in the NetWare Enhanced Security server configuration. It is possible to create the AFP server object, but there is no meaningful way to use it.

For more information on the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Template Examples

The following sections relate to Appendix C, “Template Examples,” of *Guide to NetWare 4 Networks*.

NetWare 4 Server Worksheet

Remember that all hardware installed on the server must be permitted by *NetWare Enhanced Security Server*. This includes the server platform (for example, the motherboard), network boards, storage hardware, and printers that pass the relevant Yes tests for the hardware and that satisfy the specific hardware requirements identified in *NetWare Enhanced Security Server*.

Server Migration

As explained in Chapter 3, “Security Supplement to Installation,” on page 69, you cannot migrate an existing NetWare 2.*x*, 3.*x*. or 4.*x* server to a NetWare Enhanced Security configuration. If you are currently running an unevaluated version of NetWare (for example, NetWare 3.11 or 4.01) on your server, you must perform a complete installation of the server.

Workstation Configuration Worksheet

For specific guidance on configuring individual workstation products, see your vendor’s trusted workstation vendor’s documentation.

Supplemental Information

This section relates to Appendix D, “Supplemental Information,” of *Guide to NetWare 4 Networks*.

The supplemental documents listed in this appendix do not necessarily describe the NetWare Enhanced Security configuration. If you reference these documents, remember that the NetWare Enhanced Security documentation (this manual, *NetWare Enhanced Security Server*, and *Auditing the Network*) take precedence over any other documentation.

The availability of context-sensitive help, online Windows help, and online DynaText documentation depend on your workstation vendor’s evaluated configuration. To determine whether these are available, see your vendor’s workstation documentation.

Remember that only those DynaText documents that are specifically referenced by the NetWare Enhanced Security documentation should be used for installing and administering a trusted network facility using NetWare Enhanced Security servers.

chapter 3 Security Supplement to Installation

This chapter contains NetWare® Enhanced Security information that supplements the NetWare 4.11 *Installation* manual. *Installation*, along with the warnings and other supplementary information in this chapter, describes the installation of a Network Trusted Computing Base (NTCB) partition for a NetWare Enhanced Security server.

As mentioned in "Server NTCB Partition" on page 28, the server NTCB partition includes all hardware, firmware, and software responsible for enforcing the server component's security policies. For the server, all software is TCB software; there is no non-TCB software loaded on the server.

The tasks that are permitted for a trusted network include the installation of a new NetWare Enhanced Security server (hardware, software, and configuration data) and the upgrade of an existing NetWare Enhanced Security server to a newer release.

Depending upon the size of the organization and facility, these tasks may be performed by a NetWare administrator or by an installation engineer. In either case, the individual(s) must be trusted to follow the organization's security policies.

The NetWare Enhanced Security Server Configuration

NetWare Enhanced Security Server describes the hardware and software permitted for a Enhanced Security server component. *NetWare Enhanced Security Server* is incorporated by reference in this chapter and should be consulted when planning the hardware and software configuration for an NetWare Enhanced Security server.

The hardware permitted for a NetWare Enhanced Security configuration includes all file server platforms (such as system boards), storage hardware (disks, tapes, controllers,etc.), network hardware, and printers that have been certified for this release by the Novell® Yes program, subject to the constraints listed in *NetWare Enhanced Security Server*.

That is, you can use and Yes-certified device permitted by *NetWare Enhanced Security Server*, and can use any associated machine-independent device drivers in your NetWare Enhanced Security server.

For information on how to determine if a specific device is Yes-qualified, see *NetWare Enhanced Security Server*.

Warning

Do not use unevaluated hardware (that is, hardware not identified in *NetWare Enhanced Security Server*. The use of unevaluated hardware violates the basis of trust provided by the server evaluation. The addition of even one unevaluated hardware component will invalidate your server’s C2 rating.

NetWare Enhanced Security Server also lists the machine-independent software that is included in the NetWare Enhanced Security configuration. In addition to the initialization software and server operating system, it identifies the NetWare Loadable Module^{TM} (NLM^{TM}) programs that can be loaded and run on a NetWare Enhanced Security server.

Warning

Do not run unevaluated NLM programs on a server with a NetWare Enhanced Security server. Further, do not run unevaluated versions of the operating system (SERVER.EXE) and supporting NLM programs.

Because the server TCB software does not provide a means to protect itself from untrusted software, the use of unevaluated software violates the server’s basis of trust. The addition of even one unevaluated NLM program will invalidate your server’s C2 rating.

Prepare to Install

This section contains supplementary enhanced security information for Chapter 1, “Prepare to Install,” of *Installation*.

Warning

Because this chapter provides supplementary information to *Installation* and is not a complete document by itself, you must read the online installation manual *before* you install the server software. If you already have one or more NetWare 4.1 servers online, you can read *Installation* at a workstation using the DynaText* viewer provided in the NetWare 4.1 distribution media.

If this is the first server in your facility, install the Dynatext viewer and online documentation on a standalone workstation so that you can read *Installation* while you’re installing the server. For DynaText installation instructions, see *Installing and Using Novell Online Documentation*.

Appendix W, “Network Composition Rules,” on page 377 explains how to determine if you can securely install the server into a specific segment of your network. The network security architecture provides for evaluation of many different types of components, some of which are incompatible with other, and relies on each administrator to follow the guidance in the appendix.

Warning

If you do not follow the guidance in Appendix A when you install components on the network, you may create configurations that are not permitted by the network security architecture. This could allow users to disrupt the operation of trusted components (by sending untrusted routing data, for example), to communicate directly from one workstation to another without mediation by the server, or to access residual data in server packets.

Warning

The server be physically protected, such that the server console (keyboard and screen) can be accessed only by trusted administrative personnel. This requirement can be met by placing the server in a locked room, with keys to the room distributed only to the administrator(s) that are trusted to properly install, configure, and administer the server.

Using the SECURE CONSOLE command on a physically unprotected server does *not* meet the C2 requirements for server protection.

Further, the newtork security architecture also requires physical or cryptographic protection of the networking media (cabling, routers, etc.).

Set Up Hardware

Setting up the server hardware involves the following additional considerations for a NetWare Enhanced Security server:

- Acquire the computer sytem and its peripherals. The NetWare Enhanced Security configuration permits a variety of Yes-certified file servers, storage hardware, network hardware, and printer products. you may use any of the hardware products permitted in *NetWare Enhanced Security Server*.

Warning

Installing any hardware not permitted in *NetWare Enhanced Security Server* violates the basis of trust in the NetWare Enhanced Security server and in the entire network.

- Use FDISK to reserve space for a DOS partition on the hard disk, as identified in *Installation*. The NetWare Enhanced Security server uses this partition for booting the server and for storing device drivers for certain peripherals.

- If you are installling NetWare 4 onto a previously used computer, you must reformat the disk to remove all existing software.

Warning

Previously used disk drives may contain malicious software. If such software is left on the disk, it could corrupt or modify the server's security enforcing mechanisms.

- Install DOS. You may only use the specific DOS version, release, and auxiliary software (such as utilities or extensions) identified as installation software in Chapter 4, "Machine-Independent Software,"of *NetWare Enhanced Security Server*. Follow the procedures in the DOS product's documentation.

Warning

The use of any version of DOS not specified in *NetWare Enhanced Security Server* violates the basis of trust in the NetWare Enhanced Security server and the network.

Hardware Requirements

NetWare supports various link layer protocols, but only Ethernet is inclued in the NetWare Enhanced Security configuration. Any of the Ethernet cabling specifications (10Base-2, 10Base-5, 10Base-T) are permitted.

Novell’s Yes Program

The server’s NetWare Enhanced Security configuration includes file server, storage, network, and printer hardware that

- Is Yes-certified
- Meets the additional requirements stated in *NetWare Enhanced Security Server*

You can use any hardware and supporting machine-dependent software (such as drivers) that meet these criteria.

Prepare to Install on a Windows 95 Machine

Warning The NetWare Enhanced Security configuration does not permit isntallation on a Windows 95 machine. To install thte NetWare Enhanced Security server on a workstation that is currently runnning Windows 95, you must format the disk, install DOS, and then install NetWare 4.11.

Installing from a Remote Network Installation Area

Warning Do not install a new server over the network from a non-C2 (for example, NetWare 2.*x*, 3.1*x*, or 4.0*x*) server.

Warning FILTCFG.NLM is not included in the server NetWare Enhanced Security configuration, so you must not use it to view IPX$^{\text{TM}}$ protocol filters (that is, to determine if the server is RIP-filtered).

Simple Installation (Console)

This section contains supplementary enhanced security information for Chapter 2, “Simple Installation,” of *Installation*.

Choose the Type of Installation

Installation of client software and creation of client diskettes are not part of the server installation. Refer to you workstation’s trusted facility documentation for information on how to install the workstation client software.

Name Your Server and Copy Boot Files

Warning

The name of the server will be public information that can be determined by any user on the network. Consequently, you should not give the server a sensitive name (a project name, for example).

Install NetWare SMP (Conditional)

Warning

The NetWare Enhanced Security configuration does not include the NLM programs (SMP, MPDRIVER, and .PSM driver files) necessary to support NetWare Symmetric MultiProcessing (SMP). For the list of NLM programs, see *NetWare Enhanced Security Server*.

Load the Device Drivers

Warning

Installation identifies drivers for various storage and bus architectures. These drivers are included in the NetWare Enhanced Security configuration only if they have been approved by the Yes program and meet the specific requirements in *NetWare Enhanced Security Server* for storage hardware. For a description of the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Load the LAN Drivers

Warning

Installation identifies drivers for various cabling systems and network boards. These drivers are included in the NetWare Enhanced Security configuration only if they have been approved by the Yes program and meet the specific requirements for network hardware stated in *NetWare Enhanced Security Server*. For a description of the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

The network architecture uses only the Enthernet protocols. Consequently, only Ethernet drivers are available.

Install NetWare Directory Services

Warning In the NetWare Enhanced Security configuration, if you are integrating the new server into an existing NetWare Directory tree, the tree must consist solely of evaluated C2 servers.

Warning If you are installing a new server into an NetWare Directory tree with existing users, be aware that these users may be able to login to the server before you can enable file server auditing. If this is not acceptable for your facility, you can either create a temporary network with only one workstation or disable logins and log out all users until the server is configured.

For more information on the NDS^{TM} User object ADMIN and the bindery object SUPERVISOR, see Chapter 2, “Security Supplement to Guide to NetWare 4 Networks,” on page 43.

Review the Created Trustee Assignments (Optional)

Warning Giving [Public] the Browse right to the [Root] object of the NetWare Directory tree allows users to browse the NetWare Directory tree before logging in.

For further information on setting NDS object and object property rights, see Chapter 2, “Security Supplement to Guide to NetWare 4 Networks,” on page 43 and Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.

Other Installation Options

The creation of DOS, Windows, and OS/2 client installation diskettes is outside the scope of the server installation. These diskettes are useful only if the client trusted facility manual identifies them as necessary to install the client TCB.

If you create DOS, Windows, or OS/2 client installation diskettes, check with the client (workstation) vendor to determine that the diskettes do not invalidate any security assumptions required for the client.

Warning

You *can* make Upgrade/Migrate disks, but you *cannot* use those disks to upgrade an existing NetWare 2.*x*, 3.*x*. or 4.*x* server to an NetWare Enhanced Security configuration. There is no approved method for upgrading unevaluated NetWare 2.*x*, 3.*x*, or 4.*x* servers to a NetWare Enhanced Security configuration.

If you are currently running an unevaluated version of NetWare (such as NetWare 3.11 or 4.01) on your server, you must perform a complete installation of the server as described previously.

Custom Installation (Console)

This section contains supplementary enhanced security information for Chapter 3, “Custom Installation,” of *Installation*.

The “Custom Installation” option permits you to tailor the server installation to your special facility requirements, such as partitioning, mirroring, or spanning volumes across multiple drives. While this provides increased flexibility (with respect to the “Simple Installation”), it requires additional planning and additional care to avoid configuring the server in a nonsecure manner.

Warning

TCP/IP and AppleTalk* protocols are not included in the NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Warning

If you intend to boot the server from diskette, you must ensure that the boot diskette contains the same version and release of DOS that is specified in Chapter 4, “Machine-Independent Software ,” of *NetWare Enhanced Security Server*. Booting from a different version of DOS violates the basis of trust in the NetWare Enhanced Security server.

Choose a Server Boot Method

The NetWare Enhanced Security server may only be booted from a DOS partition.

Making the server bootable from diskette does *not* provide any additional trust. Because NetWare Enhanced Security requires a physically protected server, booting from hard disk is equally trustworthy and is more convenient than booting from diskette.

Choose the Type of Installation

Installation of client software and creation of client diskettes are not part of the server installation. Refer to your workstation strusted facility documentation for information on installing the the workstation client software.

Name Your Server and Assign an IPX Network Number

Warning Do not assign the server a specific IPX internal network number, unless you have a mechanism to ensure that the proposed number is not already used by another server on the same internetwork.

Install NetWare SMP (Conditional)

The NetWare Enhanced Security server configuration does not includ the NLM programs (SMP, MPDRIVER, and PSM driver files) necessary to support Symmetric MultiProcessing (SMP). For a list of allowable NLM programs, see Chapter 4, "Machine-Independent Software," of *NetWare Enhanced Security Server*.

Load the Device Drivers

Warning Do not install unevaluated hardware in the server. *Installation* identifies drivers for various storage and bus architectures. These drivers are included in the NetWare Enhanced Security configuration only if they have been approved by the Yes program and meet the specific requirements for storage hardware stated in *NetWare Enhanced Security Server*. For a description of the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Load the LAN Drivers

Warning Do not install unevaluated hardware in the server. *Installation* identifies drivers for various cabling systems and network boards. These drivers are included in the NetWare Enhanced Security configuration only if they have been approved by the Yes program and meet the specific requirements for network hardware stated in *NetWare Enhanced Security Server*. For a description of the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

The network architecture uses only the Ethernet protocols. Consequently, only Ethernet drivers are available.

The NetWare Enhanced Security server does not include TCP/IP. For more information on the NetWare Enhanced Security server configuration, see *NetWare Enhanced Security Server*.

Manage NetWare Volumes

Warning

Do not enable data migration in the evaluated configuration.

Warning

HCSS, SFT III^{TM}, NetWare for Macintosh, and additional name spaces (MAC.NAM, OS2.NAM, NFS.NAM, FTAM.NAM) are not included in the server's NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

FLAG and NetWare Administrator are client utilities. Refer to you workstation's trusted facility documentation to determine whether you can use these utilities.

Install NetWare/IP (Conditional)

The NetWare Enhanced Security server does not include the TCP/IP suite of protocols on NetWare/IP. Consequently, you should disregard the information in this section.

Installing NetWare Directory Services

Warning

If you are integrating the new server into an existing NetWare Directory tree, the tree must consist solely of C2 servers.

Warning

If you are installing a new server into an NetWare Directory tree with existing users, be aware that these users may be able to log in to the server before you can enable file server auditing. If this is not acceptable for your facility, you can either create a temporary network with only one workstation or disable logins and log out all users until the server is configured.

For more information on the NDS user object ADMIN and the bindery SUPERVISOR object, see Chapter 2, "Security Supplement to Guide to NetWare 4 Networks," on page 43.

Review the Created Trustee Assignments (Optional)

Warning

By giving [Public] the Browse right to the [Root] object of the NetWare Directory tree, users are able to browse the NetWare Directory tree before they log in. For further information on setting NDS object and object property rights, see Chapter 2, “Security Supplement to Guide to NetWare 4 Networks,” on page 43 and Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.

Modify the STARTUP.NCF File

Warning

If you modify STARTUP.NCF to add SET commands, make sure that the SET commands are consistent with the guidance in “Configuring SET Parameters (Console)” on page 85.

Warning

Do not run unevaluated NLM programs on a server within an enhanced security network. Do not load additional name space NLM programs, such as MAC.NAM, OS2.NAM, NFS.NAM, FTAM.NLM. As described in *NetWare Enhanced Security Server*, these NLM programs are not included in the evaluated configuration.

Modify the AUTOEXEC.NCF File

Warning

If you modify the AUTOEXEC.NCF to specify SET parameters, make sure that the parameters are consistent with the guidance in “Configuring SET Parameters (Console)” on page 85. One way to ensure that the parameters are set correctly for NetWare Enhanced Security is to run SECURE.NCF from the AUTOEXEC.NCF file.

Warning

Do not run unevaluated NLM programs on a server within an enhanced security network. If you edit AUTOEXEC.NCF to LOAD additional NLM programs, make sure that the NLM programs are part of the NetWare Enhanced Security configuration.

Perform Other Installation Options

The creation of DOS, Windows, or OS/2 client installation diskettes is outside the scope of the server installation. These diskettes are useful only if the client trusted facility manual identifies them as necessary to install the client TCB.

If you create DOS, Windows, or OS/2 client installation diskettes, check with the client (workstation) vendor to determine that the diskettes do not invalidate any security assumptions required for the client.

Warning Do not upgrade NetWare 3.1*x* Print Services.

Warning You can make upgrade/migrate disks, but you cannot use those disks to upgrade an existing NetWare 2.*x*, 3.*x*, or 4.*x* server to a NetWare Enhanced Security configuration. There is no approved method for upgrading unevaluated NetWare 2.*x*, 3.x, or 4.*x* servers to a NetWare Enhanced Security configuration.

If you are currently running an unevaluated version of NetWare (such as 3.11 or 4.01) on your server, you must perform a complete installation of the server as described previously.

Warning NetWare for Macintosh, MHS, and INETCFG.NLM are not included in the NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Warning The NetWare Enhanced Security server does not include support for TCP/IP, NetWare DHCP, or AppleTalk protocols. For more information see *NetWare Enhanced Security Server*.

Warning Because the NetWare Enhanced Security server does not include INETCFG.NLM, you cannot perform the configure NetWork Protocol tasks metioned in this section.

Install NetWare Server for OS/2 (Console)

This section contains supplementary NetWare Enhanced Security information for Chapter 4, “Install NetWare Server for OS/2,” of *Installation*.

Warning NetWare Server for OS/2 is not included in the server’s NetWare Enhanced Security configuration and should be disregarded for purposes of running NetWare Enhanced Security. For a description of the server’s NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Install NetWare 4.11 SFT III (Console)

This section contains supplementary NetWare Enhanced Security information for Chapter 5, “Install NetWare 4.11 SFT III,” of *Installation*.

Warning NetWare 4.11 SFT III is not included in the server’s NetWare Enhanced Security configuration and should be disregarded for purposes of running NetWare Enhanced Security. For a description of the server’s NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Install NetWare Clients (Console)

This section contains supplementary NetWare Enhanced Security information for Chapter 6, “Install NetWare Clients,” of *Installation*.

Installation of NetWare clients (such as DOS, Windows, OS/2, and Macintosh) is addressed in each respective client’s component documentation. The installation of a client Network Trusted Computing Base (NTCB) partition may or may not follow the instructions in this paragraph. Refer to the client installation instructions for further information.

As explained in Chapter 6 of *Installation*, one reason for installing the first client workstation is to provide access to the DynaText online documentation. However, while you are installing the network, you can access DynaText from a standalone PC.

Calculate RAM Requirements

This section contains supplementary NetWare Enhanced Security information for Appendix A, “Calculate RAM Requirements,” of *Installation*.

Note that the NetWare Enhanced Security server configuration allows only the NLM programs listed in Chapter 4, “Machine-Independent Software,” of *NetWare Enhanced Security Server*. Therefore, you do not need additional memory for name spaces or other specialized applications.

Name Space Requirements

This section contains supplementary NetWare Enhanced Security information for Appendix B, “Name Space Requirements,” of *Installation*.

The NetWare Enhanced Security server configuration does not provide support for additional name spaces. Therefore, you should disregard this appendix.

Country Codes

There is no supplementary NetWare Enhanced Security information for Appendix C, “Country Codes,” of *Installation*.

Install to Boot From Floppy Diskette (Console)

Boot Diskette Advantages and Disadvantages

If you intend to boot the server from diskette, you must ensure that the boot floppy contains the version and release o DOS specified in Chapter 4, “Machine-Independent Software,” of *NetWare Enhanced Security Server*.

Install to Boot From Floppy Diskette

This section contains supplementary NetWare Enhanced Security information for Appendix D, “Install to Boot from Floppy Diskette,” of *Installation*.

Making the server bootable from diskette does not provide any additional trust. Because NetWare Enhanced Security requires a physically protected server, booting from hard disk is equally trustworthy and is more convenient than booting from diskette.

Creating Client Diskettes (Console)

This section contains supplementary NetWare Enhanced Security information for Appendix E, “Creating Client Diskettes,” of *Installation*.

Warning

The creation of DOS, Windows, or OS/2 client installation diskettes is not part of the server installation. These diskettes are useful only if the client trusted facility manual identifies them as necessary to install the client TCB.

If you create DOS, Windows, or OS/2 client installation diskettes, check with the client (workstation) vendor to determine that the diskettes do not invalidate any security assumptions required for the client.

Install Using RCONSOLE (Console)

This section contains supplementary NetWare Enhanced Security information for Appendix F, “Install Using RCONSOLE,” of *Installation*.

Warning

REMOTE.NLM is not included in the server’s NetWare Enhanced Security configuration. Consequently, you cannot run RCONSOLE and this information should be disregarded for purposes of running NetWare Enhanced Security. For a description of the server’s NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Understanding Driver Architecture

This section contains supplementary NetWare Enhanced Security information for Appendix G, “Understanding Driver Architecture,” of *Installation*.

As explained in Chapter 6, “Storage Hardware and Software,” of *NetWare Enhanced Security Server*, the NetWare Enhanced Security configuration includes both monolithic and NWPA drivers. Third-party drivers are Yes-certified along with the associated hardware, and can be included in the NetWare Enhanced Security configuration.

Warning

Do not use any drivers that are not permitted in the NetWare Enhanced Security Server. Use of other software on the server violates the basis of trust for the server and the network.

Red Box CD-ROM Drivers (Console)

This section contains supplementary NetWare Enhanced Security information for Appendix H, “Red Box CD-ROM Drivers,” of *Installation*.

Warning

For a listing of NetWare Enhanced Security CD-ROM device drivers, see *NetWare Enhanced Security Server*.

Configuration and Review (Console, Client)

After you have installed the server, you must perform certain steps to configure the server in a secure state:

- Configure the server boot configuration files to set the operating system parameters to a secure state
- Set the audit configuration
- Define the USER_TEMPLATE (before you add any new users to NDS)
- Review NDS rights
- Review file system rights
- Configure your printers and print queues

These steps are outlined in the following sections.

Configuring the Boot Configuration Files (Console)

If you did not edit the server boot configuration files during a custom installation described (as described in “Custom Installation (Console)” on page 76), then you must run INSTALL.NLM to modify the server boot configuration. This includes:

- Defining certain SET parameters
- Ensuring that the server unloads DOS after it boots

For instructions on using INSTALL.NLM from the console of a running server to edit the STARTUP.NCF and AUTOEXEC.NCF files, see “Creating or Editing a Server Batch (.NCF) File” in Chapter 7 of *Supervising the Network*.

As an alternative, you may used a trusted client utility to edit the AUTOEXEC.NCF file (which is stored in the SYS:SYSTEM directory). To edit your STARTUP.NCF file, you may bring down the NetWare server and use the Novell DOS EDIT utility.

Configuring SET Parameters (Console)

For a description of server SET parameters, supported values, and default values, see “SET” in *Utilities Reference*. The server parameters are primarily concerned with performance optimization issues and, generally, do not affect the security provided by the server TCB.

The following list identifies security-relevant parameters and their required settings (if any).

Miscellaneous Parameters	Allow Unencrypted Passwords	This parameter must be set to OFF. The server does not support NetWare 2.*x* logins.
NCP^{TM} Parameters	NCP Packet Signature Option	This option provides additional security where there is a threat that NCP messages may be modified on the wire. It is not required for C2 security.
Miscellaneous Parameters	Allow Audit Passwords	This parameter must be set to OFF in the NetWare Enhanced Security configuration.
Miscellaneous Parameters	Check Equivalent To Me	This option provides additional security. It is not required for C2 security.
NCP Parameters	Reject NCP Packets with Bad Lengths	This parameter must be set to ON in the NetWare Enhanced Security configuration.
NCP Parameters	Reject NCP Packets with Bad Components	This parameter must be set to ON in the NetWare Enhanced Security configuration.
Miscellaneous Parameters	Enable SECURE.NCF	This parameter must be set to ON in STARTUP.NCF. By so doing, the server will run SECURE.NCF on every system boot, thus setting all other parameters listed here to their required values.

If you did a simple install or a custom install, you must edit the STARTUP.NCF file or the AUTOEXEC. NCF file to define the previous SET values. You may do this by including the following command in either of the files:

```
SET ENABLE SECURE.NCF=ON
```

Warning The SET command documentation includes a description of the NetWare SFT III parameters. NetWare SFT III is not included in the NetWare Enhanced Security configuration, and the NetWare SFT III parameters are not visible at the server console.

Warning If you modify a SET parameter for the server, do not define a value outside the range of supported values defined in *Utilities Reference*.

Removing DOS from Memory (Console)

In the NetWare Enhanced Security configuration, DOS is used only to boot the server operating system.

The REMOVE DOS command reclaims the DOS memory for system cache and causes the server to reboot when it gets an EXIT command at the console.

Warning You must edit the AUTOEXEC.NCF file to remove DOS after booting. Use the REMOVE DOS command.

Warning After you REMOVE DOS, you will be unable to edit the STARTUP.NCF file on the DOS partition using the INSTALL program.

To edit this file, use INSTALL.NLM (or a trusted client utility) to remove the REMOVE DOS command from AUTOEXEC.NCF, reboot the server, run INSTALL.NLM to edit STARTUP.NCF, run INSTALL.NLM (or a trusted client utility) to add the REMOVE DOS command back into AUTOEXEC.NCF, and reboot the new configuration.

Alternately, you may DOWN the server and use the Novell DOS EDIT utility to modify STARTUP.NCF.

Configuring Auditing (Client)

The server is installed with file system (volume) auditing disabled. NDS auditing is defined for each container, so if a server is installed into an existing NetWare Directory tree, auditing of each NDS container is defined by the existing container auditing configurations.

If the server is installed into an existing NetWare Directory tree, any user defined in the network can access the server. This is done by logging in to an existing server and background authenticating to the new server.

While any NDS activities will be audited (according to the replica's auditing configuration), attempts to perform non-NDS activities (such as access files, shutdown server, etc.) are not audited.

The user cannot gain access to any protected resources (other than the public LOGIN directory) in this way (unless he or she has the Supervisor right to the new server's NDS object), but you need to be aware that access attempts are not audited.

To set the volume auditing configuration, you must login to the new server from a client workstation and run the AUDITCON utility. The audit configuration cannot be set from the server console. For information on using AUDITCON to define the volume auditing configuration, see *Auditing the Network*.

You must set the auditing configuration separately for each of the server's volumes. As described in *Auditing the Network*, the choice of what to audit should be defined by your organization's requirements for protection.

Setting User Templates (Client)

NetWare 4.11 provides two methods of specifying default properties for newly created User objects.

- The USER_TEMPLATE is a user object that specifies default properties for user objects creted by the client utilities NETADMIN and UIMPORT.

- NetWare 4.11 provides a new template object class that allows the NetWare Administrator utility to use one of several templates when creating a new user.

These two template mechanisms are further described in "User Account Administration (Client)" on page 116.

To determine which utilities can be used at your workstation, see your workstation trusted facility documentation. Then, determine which method (USER_TEMPLATE user object or the new Template object class) to use for your network.

Regardless of which method you choose, you must set up one or more templates before you add any users to a container.

Review NDS Rights (Client)

If you are installing the first server in an NetWare Directory tree, you should review the NDS rights in the tree before you make the server available for general use.

For a description of administering the NetWare Directory tree, see Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91 and Chapter 1, “Managing NetWare Directory Services Objects,” of *Supervising the Network*.

Warning Novell advises, but does not require, that you turn off Scan rights to the [Root] NDS object.

As described in Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91, if you have Scan rights enabled for the [Root] object, users can read the names of NDS objects before they login to NDS.

If Scan rights are disabled, unauthenticated users can query the NDS name base for the existence of specific names, but will be unable to read the names of objects.

If you are installing a server into an existing NetWare Directory tree, the existing NDS rights will continue to be enforced.

Review File System Rights (Client)

You should also review the installed file system rights for each server volume before you make the server available to other users.

For information on file system administration, see

- Chapter 5, “Security Supplement to Managing Directories, Files, and Applications,” on page 129

- Chapter 2, “Managing Directories, Files, and Applications,” of *Supervising the Network*

Configure Printers (Client)

For a description of print administration, see

- Chapter 18, “Security Supplement to Print Services,” on page 187

- *Print Services*

Upgrading the Server (Console)

NetWare Enhanced Security provides a capability to upgrade one Enhanced Security version of the server to its successor. This will be used to upgrade the initial candidate Enhanced Security release to the evaluated C2 version, using upgrade information available “on the wire” by calling Novell’s NetWire^{SM} service.

Novell intends to use the same approach when it subsequently modifies the server software under the NSA’s Rating Maintenance Phase (RAMP) program. Procedures for upgrading from the candidate Enhanced Security release to an evaluated C2 release are defined in the release notes.

There is no approved method for upgrading unevaluated NetWare 2.*x*, 3.*x*, or 4.*x* servers to a NetWare Enhanced Security configuration. If you are currently running an unevaluated version of NetWare (such as NetWare 3.11 or 4.01) on your server, you must perform a complete installation of the server as described previously in this chapter.

chapter 4

Security Supplement to Managing NetWare Directory Services Objects

This chapter contains supplementary NetWare® Enhanced Security information for Chapter 1, “Managing NetWare Directory Services Objects,” of *Supervising the Network*.

The first several headings of this chapter provide supplementary information for the corresponding headings in Chapter 1 of *Supervising the Network*.

“User Account Administration (Client)” on page 116 describes the use of NDS™ objects to perform user account administration.

“Protecting Administrative Accounts (Client)” on page 126 describes criteria for protection of administrator accounts.

“Import/Export of NDS Objects” on page 128 describes the import and export of NDS objects. The use of NetWare Directory Services™ technology to perform audit administration is described in *Auditing the Network*.

Warning For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility, the NDS Manager utility, and the NETADMIN text utility. They may also include other utilities.

However, any client program that generates the proper NetWare Core Protocol™ (NCP™) messages can manipulate the NetWare Directory database on behalf of the user logged in at that client connection.

Default Objects and Rights for NetWare 4.11

This subsection provides supplementary information for the section “Default Objects and Rights for NetWare 4.11” in Chapter 1 of *Supervising the Network*.

This includes the default NDS object and NDS object property rights for newly created objects, as shown in Table 4-1. These rights are shown as an ACL entry of the form: [Who has the rights], [Rights to what], [Default rights].

The term [Entry Rights] means the rights to the object itself, while [All Attribute Rights] means rights to all attributes of the object. Values not in brackets (such as Network Address) are actual property names. The term “not used” means that while the object can be created, it is not used in the NetWare Enhanced Security configuration.

For example, the [Creator] of a Group object has Supervisor rights to the object’s [Entry Rights], meaning that the creator has Supervisor object rights to the object. The [Root] object has Read rights to the Member object property, meaning that every user can read the membership of the group object.

Table 4-1
Default Object and Object Property Rights

Object Class Name	Default Object Rights	Default Object Property Rights
AFP Server (not used)	[Creator], [Entry Rights], {S}	[Public], Messaging Server, {R}
	[Self], [Entry Rights], {S}	[Public], Network Address, {R}
Alias	[Creator], [Entry Rights], {S}	
Application (DOS)	[Creator], [Entry Rights], {S}	
Application (Windows)	[Creator], [Entry Rights], {S}	
Application (Windows 95)	[Creator], [Entry Rights], {S}	

Table 4-1
Default Object and Object Property Rights

Object Class Name	Default Object Rights	Default Object Property Rights
Application (Windows NT)	[Creator], [Entry Rights], {S}	
Audit File	[Creator], [Entry Rights], {S}	
Bindery Object	[Creator], [Entry Rights], {S}	
Bindery Queue	[Creator], [Entry Rights], {S}	[Root], [All Attribute Rights], {R}
Computer	[Creator], [Entry Rights], {S}	
Country	[Creator], [Entry Rights], {S}	
Directory Map	[Creator], [Entry Rights], {S}	
External Entity	[Creator], [Entry Rights], {S}	[Root], Member,{R}
Group	[Creator], [Entry Rights], {S}	[Root], Member,{R}
Distribution List (not used)	[Creator], [Entry Rights], {S}	

Message Routing Group (not used)	[Creator], [Entry Rights], {S}
	[Self], [Entry Rights], {B}
		[Root], Member, {R}
		[Self], [All Attribute Rights], {R}

Table 4-1

Default Object and Object Property Rights

Object Class Name	Default Object Rights	Default Object Property Rights

Messaging Server (not used)	[Creator], [Entry Rights], {S}
	[Self], [Entry Rights], {B}
	[Self], [Entry Rights], {S}
		[Public], Messaging Database Location, {R}
		[Public], Messaging Server Type, {R}
		[Public], Network Address, {R}
		[Self], [All Attribute Rights], {R}
		[Self], Status, {R,W}

NetWare Server	[Creator], [Entry Rights], {S}	[Public], Messaging Server, {R}
		[Public], Network Address, {R}

NetWare Server	[Creator], [Entry Rights], {S}	
NetWare Server	[Creator], [Entry Rights], {S}	

NetWare Server	[Creator], [Entry Rights], {S}
	[Self], [Entry Rights], {S}
		[Public], Network Address, {S}

Organization	[Creator], [Entry Rights], {S}	
Organizational Role	[Creator], [Entry Rights], {S}	
Organizational Unit	[Creator], [Entry Rights], {S}	[Self], Login Script, {R}

Print Server	[Creator], [Entry Rights], {S}
	[Self], [Entry Rights], {R}
		[Public], Network Address, {R}

Table 4-1
Default Object and Object Property Rights

Object Class Name	Default Object Rights	Default Object Property Rights
Printer	[Creator], [Entry Rights], {S}	
Profile	[Creator], [Entry Rights], {S}	
Queue	[Creator], [Entry Rights], {S}	[Creator], [Entry Rights], {S}
Template	[Creator], [Entry Rights], {S}	
User	[Creator], [Entry Rights], {S}	[Public], Message Server, {R}
	[Root], [Entry Rights], {B}	[Root], Group Membership, {R}
		[Root], Network Address, {R}
		[Self], [All Attribute Rights], {R}
		[Self], Login Script, {R,W}
		[Self], Print Job Configuration, {R,W}
Volume	[Creator], [Entry Rights], {S}	[Root], Host Resource Name, {R, W}
		[Root], Host Server, {R}

For objects that are installed “from the box,” the [Creator] is ADMIN. Note that the ability for a user to create the object in the first place derives from the user having a Create right to the container in which the object is created.

When you create an object, the server optimizes the ACL to remove unnecessary entries. Typically, this means that the ACL entry “[Creator], [Entry Rights], {S}” is removed, since in most cases the creator of an object has the Supervisor rights to the container where the object is found, and hence has the Supervisor rights to the newly created object by inheritance.

If, however, the creator only had the Create rights to the container, then the ACL for the newly created object retains the “[Creator], [Entry Rights], {S}” entry, since the creator would not otherwise have any rights on the newly created object.

Thus, if you create an object and then set its Inherited Rights Filter, you may no longer have access to the object, even though the “[Creator], [Entry Rights], {S}” ACL entry would appear to give you such rights.

Warning Table 1-1 under “Default Objects and Rights for NetWare 4.11” in *Supervising the Network* describes the default objects and rights after upgrading from an earlier version of NetWare (such as NetWare 3.11) to NetWare 4.11.

This information does not pertain to NetWare Enhanced Security facilities, because there is no approved method for upgrading unevaluated NetWare 2.*x*, 3.*x*, or 4.*x* servers to a NetWare Enhanced Security configuration.

Users may request additional rights to existing objects or object properties. You must not grant any nonadministrative user any NDS object rights except Browse.

However, you may grant nonadministrative users rights to certain properties of NDS objects. Table 4-2 lists those properties that nonadministrative users may be given rights for.

The rights that are listed are Read (R) and Write (W). You may also grant the Compare (C) right to any property for which Read rights are listed. You may also grant the Add or Delete Self (A) right to any property for which Write rights are listed.

Note that not all properties pertain to all NDS objects (for example, there is no “Aliased Object Name” property in a “User” object).

Explanations of property uses and what objects each is used in can be found in the NetWare Directory Services Schema Specification, which is part of the NetWare SDK.

Warning The rights shown in Table 4-2 are the maximum you may assign in the NetWare Enhanced Security configuration. Client-based tools (such as NETADMIN and

NetWare Administrator) may or may not prevent you from assigning additional rights. It is your responsibility as an administrator to *not* assign more rights than are shown.

Warning Also note that the rights shown are the maximum *effective* rights that may be granted. Effective rights can be derived from security equivalence and inheritance, as well as being directly assigned to a user. When assigning rights to any NDS object property, review how effective rights are computed, as described in *Guide to NetWare 4 Networks* and *Concepts*.

Warning Do not make nonadministrative users security equivalent to any NDS Server object such as NetWare Server, AFP Server, or Print Server.

You should never assign any rights to [Public] beyond what is included in the NetWare Enhanced Security configuration, since any user, whether logged in or not, is security equivalent to [Public]. If you want to allow all users access to a property, it is better to assign those rights to [Root] or to the container the users are in.

Certain properties are *Hidden* properties; they cannot be read or written no matter what rights users have. Other properties are *Publicly Readable* properties; they can be read by all users (even before logging in), no matter what rights the user has. Still other properties are *Read-Only*; they cannot be written no matter what rights users have.

All of these types of properties are shown in Table 4-2. Note that the ability to read *Read-Only* properties and to write *Publicly Readable* properties is controlled by the normal access restrictions.

Your site security policy may be more restrictive than the rights shown here; this table simply lists the maximum rights that should be granted to nonadministrative personnel.

For example, if you rely on accounting services for billing purposes, you probably do not want to allow users to modify their account balances. However, if you are not using accounting, there is no harm in allowing such modifications to occur.

Many entries in the table are identified as information that would be useful to potential intruders. For example, if an intruder knows that a user account is not required to have a password, then he or she can determine that the account is more likely to not have a password (or at best a weak password) than an account that is required to have a password.

Thus, you may not want to allow as much access as is permitted by this table. In particular, it is best only to allow users to see their own values for any parameters that have to do with login and password restrictions (such as times of day, last login time, minimum password length).

By default, all information that would be useful to intruders is protected, except those items marked as “Public Read.”

Table 4-2

Maximum Property Rights

Object Properties	Maximum Rights	Comments
Account Balance	RW	If you perform accounting, you would not want to permit users to write this.
ACL	R	You may not want to allow users to read other users’ ACLs, lest they determine who would be a good target for an attack.
Aliased Object Name	R	Allowing users to change this could allow replacement of the object to which a user logs in.
Allow Unlimited Credit	RW	If you perform accounting, you would not want to permit users to write this.
App Blurb	RW	
App Contacts	RW	
App Drive Mappings	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.
App Flags	RW	
App Icon	RW	

Table 4-2

Maximum Property Rights

Object Properties	Maximum Rights	Comments
App Parameters	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.
App Path	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.
App Printer Ports	RW	
App Shutdown Script	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.
App Startup Script	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.
App Working Directory	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.
Audit A Encryption Key	(None)	Used by servers, modified only by servers
Audit B Encryption Key	(None)	Used by servers, modified only by servers
Audit Contents	(None)	Read access provides the ability to read audit data, and must be restricted to administrators. Write access provides the ability to append audit data, and must be restricted to NTCB partitions of workstation components.

Table 4-2

Maximum Property Rights

Object Properties	Maximum Rights	Comments
Audit Current Encryption Key	(None)	Used by servers, modified only by servers
Audit File Link	(None)	Used by servers and trusted clients, modified only by administrators
Audit Link List	(None)	Used by servers, modified only by administrators
Audit Path	(None)	Used by servers and trusted clients, modified only by administrators
Audit Policy	(None)	Used by servers, modified only by administrators
Audit Type	(None)	Used by servers and trusted clients, modified only by administrators
Authority Revocation	(None)	“Read-Only” property
Auto Start	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software
Back Link	(None)	“Read-Only” property
Bindery Object Restriction	RW	“Read-Only” property. Not used in the Enhanced Security configuration.
Bindery Property	RW	“Read-Only” property. Not used in the Enhanced Security configuration.
Bindery Type	RW	“Read-Only” property. Not used in the NetWare Enhanced Security configuration.
C (Country)	R	
CA Private Key	(None)	“Read-Only” and “Hidden” property
CA Public Key	R	“Public-Read” and “Read-Only” property

Table 4-2
Maximum Property Rights

Object Properties	Maximum Rights	Comments
Cartridge	RW	Malicious software could modify this to confuse other software as to cartridges available, but this would not have any impact on system security.
Certificate Revocation	(None)	“Read-Only” property
Certificate Validity Interval	R	Seeing this might help an intruder determine how to proceed with an attack.
Common Certificate	RW	
CN (Common Name)	R	
Convergence	R	
Cross Certificate Pair	R	
Default Queue	R	
Description	RW	Informational only
Desktop	RW	
Detect Intruder	R	Seeing this might help an intruder determine how to proceed with an attack.
Device	RW	
DS Revision	RW	
EMail Address	RW	“Public-Read” property. Informational only.
External Name	RW	Informational only
External Synchronizer	R	Not currently used

Table 4-2
Maximum Property Rights

Object Properties	Maximum Rights	Comments
Facsimile Telephone Number	RW	Informational only
Full Name	RW	Informational only
Generational Qualifier	RW	Informational only
GID	R	While not used for access controls by NetWare, may be used by some clients.
Given Name	RW	Informational only
Group Membership	R	While not directly used for access control, administrators may examine this property to find group membership.
High Convergence Sync Interval	R	
Higher Privileges	R	Not currently used
Home Directory	RW	Modification could cause a user to execute malicious code from another user's directory.
Home Directory Rights	R	You may not want to allow users to read this property, because and intruder could use this as the basis for an attack.
Host Device	R	
Host Resource Name	R	
Host Server	R	
Inherited ACL	R	
Initials	RW	Informational only
Intruder Attempt Reset Interval	R	Seeing this might help an intruder determine how to proceed with an attack.

Table 4-2

Maximum Property Rights

Object Properties	Maximum Rights	Comments
Intruder Lockout Reset Interval	R	Seeing this might help an intruder determine how to proceed with an attack.
L (Locality)	RW	Informational only
Language	RW	Informational only. Modifying this could cause applications to become unusable.
Last Login Time	R	
Last Referenced Time	R	
Launcher Config	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.
LicenseID	RW	
License Database	RW	
Locked by Intruder	R	Seeing this might help an intruder determine how to proceed with an attack.
Lockout After Detection	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Allowed Time Map	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Disabled	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Expiration Time	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Grace Limit	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Grace Remaining	R	Seeing this might help an intruder determine how to proceed with an attack.

Table 4-2

Maximum Property Rights

Object Properties	Maximum Rights	Comments
Login Intruder Address	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Intruder Attempts	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Intruder Limit	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Intruder Reset Time	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Maximum Simultaneous	R	Seeing this might help an intruder determine how to proceed with an attack.
Login Script	RW	Modification could cause a user to execute malicious code from another user’s directory.
Login Time	R	Seeing this might help an intruder determine how to proceed with an attack.
Low Convergence Reset Time	R	
Low Convergence Sync Interval	R	
Mailbox ID	RW	“Public-Read” property. Informational only.
Mailbox Location	RW	“Public-Read” property. Informational only.
Member	R	While not directly used for access control, administrators may examine this property to determine group or list membership.
Members of Template	R	
Memory	RW	Informational only

Table 4-2
Maximum Property Rights

Object Properties	Maximum Rights	Comments
Message Routing Group	RW	Not used in NetWare Enhanced Security configuration
Message Server	RW	Not used in NetWare Enhanced Security configuration
Messaging Database Location	RW	Not used in NetWare Enhanced Security configuration
Messaging Server	RW	Not used in NetWare Enhanced Security configuration
Messaging Server Type	RW	Not used in NetWare Enhanced Security configuration
Minimum Account Balance	RW	If you perform accounting, you would not want to permit users to write this.
Network Address	R	Used in print servers for verifying printer validity
Network Address Restriction	R	Seeing this might help an intruder determine how to proceed with an attack.
New Objects's DS Rights	R	You may not want to allow users to read this property, because and intruder could use this as the basis for an attack.
New Objects's FS Rights	R	You may not want to allow users to read this property, because and intruder could use this as the basis for an attack.
New Objects's Self Rights	R	You may not want to allow users to read this property, because and intruder could use this as the basis for an attack.
NNS Domain	R	Not used in NetWare Enhanced Security configuration
Notify	RW	
NRD: Registry Data	RW	

Table 4-2
Maximum Property Rights

Object Properties	Maximum Rights	Comments
NRD: Registry Index	RW	
O (Organization)	RW	Informational only
Obituary	(None)	“Read-Only” and “Hidden” property
Object Class	R	“Read-Only” property
Operator	RW	Used for controlling access to queues and printers
OU (Organizational Unit)	RW	Informational only
Owner	RW	Informational only. If used to indicate the cognizant administrator, it should be restricted.
Page Description Language	RW	Informational only
Partition Control	R	“Public-Read” and “Read-Only” property
Partition Creation Time	R	“Read-Only” property
Partition Status	R	“Public-Read” and “Read-Only” property
Password Allow Change	R	Seeing this might help an intruder determine how to proceed with an attack.
Password Expiration Interval	R	Seeing this might help an intruder determine how to proceed with an attack.
Password Expiration Time	R	Seeing this might help an intruder determine how to proceed with an attack.
Password Minimum Length	R	Seeing this might help an intruder determine how to proceed with an attack.
Password Required	R	Seeing this might help an intruder determine how to proceed with an attack.

Table 4-2
Maximum Property Rights

Object Properties	Maximum Rights	Comments
Password Unique Required	R	Seeing this might help an intruder determine how to proceed with an attack.
Passwords Used	(None)	“Hidden” property
Path	RW	
Physical Delivery Office Name	RW	Informational only
Postal Address	RW	Informational only
Postal Code	RW	Informational only
Post Office Box	RW	Informational only
Postmaster	RW	Informational only
Print Job Configuration	RW	
Print Server	RW	
Printer	R	Used for enforcing access to print queues
Printer Configuration	RW	
Printer Control	RW	
Private Key	(None)	“Hidden” and “Read-Only” property
Publisher	RW	
Product	RW	
Profile	RW	
Profile Membership	RW	
Public Key	R	“Public-Read” and “Read-Only” property
Queue	R	

Table 4-2
Maximum Property Rights

Object Properties	Maximum Rights	Comments
Queue Directory	R	Used by print servers to find print jobs
Received Up To	R	“Read-Only” property
Reference	(None)	“Hidden” and “Read-Only” property
Replica	R	“Public-Read” and “Read-Only” property
Resource	RW	
Revision	R	“Public-Read” and “Read-Only” property
Role Occupant	RW	Informational only
S (State or Province)	RW	Informational only
SA (Street Address)	RW	Informational only
SAP Name	R	Used for printer access controls
Security Equals	R	Seeing this might help an intruder determine how to proceed with an attack.
Security Flags	R	Seeing this might help an intruder determine how to proceed with an attack.
See Also	RW	Informational only
Serial Number	RW	Informational only
Server	R	Used for gaining access to print queues
Server Holds	R	If you perform accounting, you would not want to permit users to write this.
Set Password After Create	R	You may not want to allow users to read this property, because and intruder could use this as the basis for an attack.
Setup Script	RW	If clients use the NetWare Application Launcher, modification of this property could cause the client to execute malicious software.

Table 4-2

Maximum Property Rights

Object Properties	Maximum Rights	Comments
Status	RW	Informational only
Support Connections	RW	Informational only
Supported Gateway	RW	Informational only
Supported Services	RW	Informational only
Supported Typefaces	RW	Informational only
Surname	RW	Informational only
Synchronized Up To	R	“Read-Only” property
Telephone Number	RW	Informational only
Title	RW	Informational only
Transaction Database	RW	
Trustees of New Object	R	You may not want to allow users to read this property, because and intruder could use this as the basis for an attack.
Type Creator Map	RW	Informational only
UID (User ID)	R	While not used for access controls by NetWare, may be used by some clients.
Unknown	RW	Informational only
Unknown Base Class	RW	“Read-Only” property
User	R	Used for access control to print queues
Version	RW	Informational only
Volume	R	Used for printer configuration

Table 4-2
Maximum Property Rights

Object Properties	Maximum Rights	Comments
Volume Space Restrictions	RW	

Depending upon your organization's requirements, you may grant Read and Write rights for users other than the user referenced by the User object. For example, you may have an organization where a personnel manager is the only user that can modify personnel data (for example, title and telephone number).

However, in most cases, you will want the user to manage his or her own contact information (postal address, mailbox location, telephone number, etc.) by providing the user Read and Write access to those properties and all other users Read access to the properties.

Warning Use special caution when assigning trustees to a user template object. If you provide nonadministrative users with rights to modify the user template object, the changes they make will apply to any new users created in the future.

Warning Container and leaf object names are public information. Consequently, you shouldn't give sensitive names to objects within the Directory.

If you give the [Public] object Browse right to the NetWare Directory tree, any user can read the object names (but not the contents of objects or their properties) before logging in.

To prevent this from happening, disable the [Public] Browse right. Unauthenticated users will still be able to do name searches within the DIB (by querying the DIB for a specific name), but will not be able to read the names directly.

Setting Up Administration Utilities (Client)

The NetWare Enhanced Security network architecture permits the use of a variety of trusted (Enhanced Security) client components (for example, DOS, Windows* or OS/2* workstations).

Because various clients may have different file system structures or may use nonstandard application programs, the client installation instructions in *Supervising the Network* may or may not apply to the client component you are using.

For specific information on how to install your client NTCB partition, see your client vendor's Enhanced Security documentation.

Warning

In NetWare's client-server architecture, server administrators perform many functions (such as account administration or audit administration) at a workstation client rather than at the server console. All software you use at this workstation (namely, the workstation operating system, client networking software, and administrative utilities) must be trusted.

You must not run any untrusted (that is, unevaluated) software on the client while you are functioning as an administrator for the server. Refer to your client documentation for a listing of TCB utilities (such as NetWare Administrator or NETADMIN) that you can use at the client to administer the server.

Rights Needed to Create and Manage Objects

References in this chapter to the term "object" are used to refer to NetWare Directory Services (NDS) objects.

Managing Trustee Assignments to Objects (Client)

Warning

For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

Warning

Do not give the [Public] object any additional rights beyond those in the distribution (that is, "out of the box") software. Rights to the [Public] object are available to all users on the network, including those users who are not yet logged in.

Warning

Before assigning additional rights to NDS objects, see the restrictions in "Default Objects and Rights for NetWare 4.11" on page 92.

In the paragraph starting “KSMITH’s trustee assignment to MARKETING”, note that this assignment overrides only those rights granted explicitly to KSMITH and otherwise inherited, and does not override any rights granted to an object to which KSMITH is security equivalent.

Creating Container Objects (Client)

Warning NetWare Message Handling Service^{TM} (MHS), NetWare Licensing Services (NLS), and AppleTalk* Filing Protocol (AFP) are not included in the server component’s NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Refer to your client documentation for a listing of TCB utilities that you can use at the client to create container objects. Possible utilities for clients include, but are not limited to, NetWare Administrator (for Windows or OS/2), NETADMIN, and NLIST.

Warning NetWare Directory Services technology provides the ability to organize users and network resources (such as servers, volumes, and printers) within container objects (such as Organization or Organizational Unit) that follow the administrative organization of the enterprise. The client tools make it easy for you to create, configure, and delete these container objects.

As administrator, it is your responsibility to review the properties of these container objects to determine that they implement your enterprise’s security policies.

Warning When you create a new container object, the client utilities allow you to define a user template for that container. If you intend to add User objects to this container, see “User Account Administration (Client)” on page 116 for a description of the important properties of user templates.

You do not have to define a user template at this point, but you must define the template before you add any users to the container.

Creating Leaf Objects (Client)

Warning

AppleTalk Filing Protocol (AFP), NetWare Licensing Services, and NetWare Message Handling Service (MHS) are not included in the server component's NetWare Enhanced Security configuration.

The administrative tools permit you to create AFP Server, Distribution List, External Entities, Message Routing Group, and Messaging Server objects, but there is no reason for you to create these objects since there is no software on the server to use them.

In addition to the leaf objects shown in Figure 1-3 (under "Creating Leaf Objects") and in Table 1-5 (under "How to Use Leaf Objects"), you can create Audit File and Communications Server objects.

Warning

For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

Warning

Before you create any User objects, create a User Template object that defines the necessary NetWare Enhanced Security characteristics for each user in that container. For the information necessary to set up a User Template object, see "User Account Administration (Client)" on page 116.

Managing Groups of User Objects (Client)

For a listing of TCB utilities that you can use at the client to manage NDS Group, Profile, Organizational Role, and User Template objects, see your client documentation. Utilities for clients may or may not include NetWare Administrator (for Windows or OS/2) and NETADMIN. They may also include other utilities.

Warning

Group and Organizational Role objects are abstractions for managing security equivalences (see "Security Equal To" in *Concepts*). Thus, a user that is made a member of Group object FOO is, by convention, made security equivalent to FOO (that is, client utilities such as NetWare Administrator and NETADMIN do this, but it is not done by the server).

Internally, the server permits Group objects to include other Group objects; however, the server does not expand more than one level of such security equivalence calculations. To prevent confusion, the NetWare Administrator and NETADMIN client utilities do not permit you to make a group a member of another group. If you use other client utilities to manage group membership, you should avoid making groups members of other groups.

Warning As described in Chapter 6, “Security Supplement to Creating Login Scripts,” on page 137, Profile objects contain login scripts that are interpreted and executed by the client LOGIN.EXE program when a user logs in.

It is generally the client administrator’s responsibility to define these scripts, but it is your responsibility to ensure that any administrative login scripts execute properly on any workstations you use for server administration.

Warning When creating or modifying user templates, you must observe the restrictions shown in “User Account Administration (Client)” on page 116.

Searching for Objects (Client)

For a listing of TCB utilities that you can use at the client to search for NDS objects having certain properties, see your client documentation. Utilities for clients may or may not include NetWare Administrator, NETADMIN, and NLIST. They may also include other utilities.

Warning “User Account Administration (Client)” on page 116 describes certain requirements (Password Required, Minimum Password Length) that are necessary in NetWare Enhanced Security. You should periodically use the search facility to identify potential problems with the security configurations.

Examples include:

- Search for users whose object does not require a login password. Select “Password Required, Not Present.”
- Search for users who have a password shorter than the required length. Select “Minimum Password Length, Less Than” and type in the minimum required length in characters.
- Search for users that are security equivalent to administrative accounts. For example, select “Security Equivalent, Equal To” and enter the fully qualified name of the administrative account.

Moving Objects in the Directory Tree (Client)

For a listing of TCB utilities that you can use at the client to move leaf and container objects in the Directory tree, see your client documentation. Utilities for clients may or may not include NetWare Administrator, NETADMIN, and NCUPDATE. Other utilities may also be included.

Warning

Moving a leaf or container object from one container to another may cause users to have different rights to the object. This is because the user inherits rights from the new container, which may have different rights than the original container.

Before moving an object, be sure to examine the destination container to determine any inherited rights that might conflict with your local security policy.

Deleting Objects from the Directory Tree (Client)

For a listing of TCB utilities that you can use at the client to delete objects in the Directory tree, see your client documentation. Utilities for clients may include NetWare Administrator and NETADMIN. They may also include other utilities.

Do not attempt to restore deleted NDS objects from backups. NDS backups are intended for use only to restore NDS after all partitions have been lost.

Warning

"Deleting Objects from the Directory Tree" in *Supervising the Network* provides cautions about potentially losing access to part of the Directory tree when you delete user objects. These are particularly significant for administrative users, who may have the only access to certain objects in the Directory.

Warning

"Cautions when Deleting User Objects" in *Supervising the Network* explains the risks in deleting user objects. The same risks occur when deleting any other object (such as a group) that has the only rights to another object. Use the same precautions of transferring rights to another object before deleting an object.

Renaming Leaf and Container Objects (Client)

For a listing of TCB utilities that you can use at the client to rename objects in the Directory tree, see your client documentation. Utilities for clients may include NetWare Administrator and NETADMIN. They may also include other utilities.

Changing Object Property Values (Client)

For a listing of TCB utilities that you can use at the client to change object property values, see your client documentation. Utilities for clients may include NetWare Administrator and NETADMIN. They may also include other utilities.

Warning Because the NetWare Directory tree is a distributed and replicated database, a change you make may not take immediate effect (that is, within a specified number of seconds). For information about managing NDS replicas and how to determine if NDS replicas are in synchronization, see “Monitoring and Maintaining Time Synchronization” in *Supervising the Network*.

User Account Administration (Client)

The preceding sections describe the management of arbitrary container and leaf objects within the NetWare Directory tree. They describe procedures for using the NetWare Administrator and NETADMIN client utilities to create, move, rename, delete, and modify NDS objects.

Depending upon your client, you will use these same procedures to add, modify, and delete user accounts. This is because user account data is stored in an NDS User object within an Organization or Organizational Unit container in your NetWare Directory tree.

For a listing of TCB utilities that you can use at the client to perform server account administration, see your client documentation. Utilities for clients may or may not include NetWare Administrator and NETADMIN. They may also include other utilities.

You can only use a NetWare Enhanced Security client workstation, and the specific tools that are included in that workstation’s evaluated configuration, to perform account administration activities.

Configuring a User Template Object

User objects exist within an Organization or Organizational Unit container object that is associated with the company, department, division, project, or other administrative unit where the user works.

Once you configure a User Template object, review its contents to make sure that it addresses the required password restrictions and any other desired characteristics that you want to apply to all user accounts.

Required Settings for User Templates

For a NetWare Enhanced Security network facility, you must define a User Template in the container object before you begin adding user accounts.

User Template is an object that contains a template for the creation of User objects that are subsequently created in that container. When you are using the UIMPORT or NETADMIN utilities, the user template is a User object called USER_TEMPLATE. There can be at most one user template per container.

When using the NetWare Administrator utility, you may create multiple user templates by creating objects of class template. (See “Creating Leaf Objects” in *Supervising the Network*). In this case, the required settings apply to every user template you create.

Define the following NetWare Enhanced Security password restrictions for each User Template.

- Select “Password Required.”

  For both NetWare Administrator and NETADMIN, this is found in the “Password Restrictions” menu.

- Define the “Minimum Password Length” as eight characters.

  For both NetWare Administrator and NETADMIN, this is found in the “Password Restrictions” menu.

- Select “Account Disabled” to prevent use of accounts before the initial password is defined. If you fail to set this option, then intruders may be able to take control of newly created accounts before you set a password for the account.

  For both NetWare Administrator and NETADMIN, this is found in the “Login Restrictions” menu.

Recommended Settings for User Templates

The following “Password Restrictions” settings are recommended, but not required, for NetWare Enhanced Security servers. For more information on managing user passwords, refer to the Department of Defense Password Management Guidelines [CSC-STD-002-85].

- Select “Allow User to Change Password.” Administrators *can* set and change user passwords, but is it preferable to allow each individual user to change his or her own password.

  For both NetWare Administrator and NETADMIN, this is found in the “Password Restrictions” menu.

- Select “Force Periodic Password Changes.” Some users will not change their passwords unless you force them to. This mechanism disables user accounts if the user does not change his or her password within the specified time.

  For both NetWare Administrator and NETADMIN, this is found in the “Password Restrictions” menu.

- Select “Require Unique Password”. This option prevents a user from reusing one of his or her most recent eight passwords.

  For both NetWare Administrator and NETADMIN, this is found in the “Password Restrictions” menu.

Optional Settings for User Templates

Depending upon your facility requirements, you may choose to configure any of the following additional account restrictions in the User Template object. These do not directly address Enhanced Security requirements, but may provide additional security in your facility.

- **Login Time Restrictions.** You can prevent user accounts from being accessed during nonbusiness hours by specifying an acceptable usage profile in this menu.

  For both NetWare Administrator and NETADMIN, this is found in the “Login Time Restrictions” menu.

- **Network Address Restrictions.** You should configure this menu to use IPX^{TM}/SPX^{TM} protocols. (Note that you cannot specify network and node addresses in the User Template, since these will probably be specific to each user.)

  For both NetWare Administrator and NETADMIN, this is found in the “Network Address Restrictions” menu.

  You may wish to set default Print Job Configuration, Login Script, Group Membership, or Postal Address in the User Template.

  For information on print administration, see Chapter 18, “Security Supplement to Print Services,” on page 187.

  For information on login scripts, see Chapter 6, “Security Supplement to Creating Login Scripts,” on page 137.

Adding a User Account

Once you’ve added one or more User Templates that define the security configuration for all User objects in your Organization or Organizational Unit container, the creation of user accounts is straightforward.

The NetWare Administrator and NETADMIN client utilities provide menus for entering the user’s login name and other personal data. By selecting an entry, you can automatically create a home directory for the user.

Each user must have his or her own account. Do not allow users to share accounts, because you will be unable to determine from an audit trail who the responsible individual is.

Warning

User names are publicly accessible to all other users of the network. Consequently, you should not assign usernames that contain sensitive information.

For example, if the name of “Project X” is sensitive, do not create a username (or any other NDS object) called “Project X Administrator.”

If [Public] has Browse rights to the root of the NetWare Directory tree (the default), anyone (even a user who is not logged in) will be able to see the object name. Even if [Public] does not have Browse rights to the root, not logged in users will be able to verify the existence of particular objects.

Warning

Do not reuse user names within a container. That is, if a user John Smith represented by the object JSMITH leaves the organization and a new person named Jane Smith joins the organization, you should not use the name JSMITH for the new person's user object. If you do, you may be unable to determine from an audit trail who the responsible user is for a given action.

There is no problem, however, with having two objects with the same name in different containers.

To ensure that the user account is properly protected, you must perform the following additional procedures.

Adding a User Account Using NetWare Administrator

Warning

For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

Procedure

If the NetWare Administrator graphical utility is one of the evaluated tools for your trusted workstation you may use it to add a user account. To do so, follow this procedure.

Procedure

1. **Select "Use User Template."**

   This is not the default setting; if you do not use this setting, the user account can be created without any password protection. You can select a user template using the NDS browser.

2. **Select "Define Additional Properties," then select "Create" to cause the user object to be created.**

3. **Select "Password Restrictions."**

   This menu provides a screen for entering the user's initial password.

   You must define an initial password for each user when you create the account, and then give that password to the user in a trusted manner (for example, in a face-to-face meeting or by mailing it to the user in a sealed envelope).

   Many users will use the initially assigned password without changing it, so do not select a password that would be easy for an attacker to guess (such as the person's name or login account).

4. **Select “Login Restrictions” and enable the account.**

   Do not do this until you’ve set the password, or an intruder may be able to use the account before the legitimate user can take control.

Once you’ve completed these steps, you may wish to tailor Login Restrictions, Login Time Restrictions, or Network Address Restrictions for the specific user.

After you’ve completed creating the user account, but before you enable it, you may want to set the per-user audit flag and/or the audit flag on the user’s home directory. For instructions for setting these audit configuration values, see *Auditing the Network*.

NetWare password quality restrictions are limited to checking the password length and its uniqueness relative to other passwords the user has used in the past.

If you used the template facility to define the rights to files and directories, you should verify that the newly created user is authorized to have the access rights provided.

Client systems may enforce additional password quality restrictions on NetWare passwords (for example, does the password have at least one alphabetic and one numeric character). Any such enforcement is done entirely by the client, and not by the server.

Warning

For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

Procedure

If you are using NETADMIN, follow this procedure.

Warning

The “Copy the User Template Object” parameter must be set to Yes. This is the default setting, but if you do not use this setting, the user account can be created without any password protection.

Procedure

1. **When you have filled in the other fields in the menu, press** <F10> **to create the User object.**

2. **Select the newly created user, and select “Change Password.”**

   You must define an initial password for each user when you create the account, and then give that password to the user in a trusted manner (for example, in a face-to-face meeting or by mailing it to the user in a sealed envelope).

   Many users will use the initially assigned password without changing it, so do not select a password that would be easy for an attacker to guess (such as the person’s name or login account).

3. **Select “Account Restrictions” and then “Login Restrictions” and enable the account.**

   Do not do this until you’ve set the password, or an intruder may be able to use the account before the legitimate user can take control.

Once you’ve completed these steps, you may wish to tailor Login Restrictions, Login Time Restrictions, or Network Address Restrictions for the specific user.

After you’ve completed creating the user account, but before you enable it, you may want to set the per-user audit flag and / or the audit flag on the user’s home directory. For instructions for setting these audit configuration values, see *Auditing the Network*.

NetWare password quality restrictions are limited to checking the password length and its uniqueness relative to other passwords the user has used in the past.

Client systems may enforce additional password quality restrictions on NetWare passwords (for example, does the password have at least one alphabetic and one numeric character). Any such enforcement is done entirely by the client, and not by the server.

Disabling a User Account (Client, Console)

Warning

For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

The client administrative utilities (NetWare Administrator, NETADMIN) provide straightforward interfaces for disabling user accounts. For example, in NetWare Administrator, select “Login Restrictions,” then “Disable User Account.”

Warning

Disabling an account will cause any connections in use by the account to be terminated within 30 minutes and will prevent future logins to that account. However, it does not prevent someone who is already logged in to one server from background authenticating to another server.

If a disabled user were to perform background authentication, their connection would be terminated within 30 minutes. Even if the user is not logged in to any servers, if his or her workstation retains the information used for background authentication, then he or she will still be able to perform background authentication after their account has been disabled.

To force a user off the network immediately, you must delete his or her NDS User object. Changing the password or disabling the account will not stop the user.

Once his or her NDS object is deleted (and the NDS change is propagated through the network (as described in “Viewing and Managing NDS Synchronization Status (Console)” on page 145), the user will be unable to background authenticate and will be logged out of all servers.

Once you delete the User object, if you reinstate the user you will need to reassign all trustee rights and group memberships, reset audit flags, etc.

Configuring Intruder Detection

The server provides the ability to monitor invalid login attempts at a workstation, and to disable any further logins if a configurable threshold is exceeded. Intruder detection is a useful mechanism for countering brute force password guessing attacks, since it slows down the overall rate at which an attacker can enter password guesses.

The parameters for intruder detection are defined for Organization and Organizational Unit containers. Consequently, the settings you define for each container apply to all login attempts to servers within that container. The following settings are provided:

Detect Intruder	This setting determines if intruder detection is enabled for a container. While intruder detection is not required for NetWare Enhanced Security operation, the recommended setting is ON.
Login Intruder Limit	This setting determines how many invalid passwords will be tolerated by the server before locking the account. The number should be set high enough to permit a valid user to correct for typographical errors, etc., and low enough to prevent continued password guessing. The recommended range is 3 to 6 attempts.

Intruder Attempt Reset Interval	This value defines how long the server waits before resetting invalid login attempts to zero. Together with the Login Intruder Limit, this determines the maximum rate for password guessing attacks. For example, if the Login Intruder Limit is 5 and the Reset Interval is one hour, then an intruder can make up to five password guesses per hour.
Intruder Lockout Reset Interval	This period determines how long the Reset Interval workstation will be locked after intruder detection takes effect. It should be set sufficiently long (for example, two to four hours) for you to determine the cause of the lockout.

Warning

Administrative accounts (and ADMIN in particular) are a logical choice for password guessing attacks.

If intruder detection is enabled for the container, anyone with physical access to a workstation on the network could lock the administrative account. Providing this does not happen to all of your administrative accounts, you can use one administrative account to reenable others.

However, if this happens to all administrative accounts (for example, if ADMIN is the only administrative account you have), then go to the server console and type “ENABLE LOGINS”. While this will not have any impact on ADMIN, it will allow you to log in as SUPERVISOR using bindery emulation.

Note that this will only enable SUPERVISOR at the server where the command was typed, and will not have any impact on other servers in your network.

Once logged in, you may be able to reenable administrative accounts. As a safety measure, however, you should have at least one container that does not have intruder detection enabled, and make sure that there is an administrative account in that container (preferably called something other than ADMIN, so as not to attract an intruder’s attention).

Because an attacker will not be blocked from attacks on this account, be sure that audit logs on the container are reviewed carefully for evidence of attempted break-ins.

When the server disables a workstation, it displays an alert message to the server console (indicating the account and network address that is locked) and a notification to the workstation.

To unlock a user account using NetWare Administrator, select the user object, “Details,” and “Intruder Lockout,” and then reset the locked box.

Deleting a User Account

Deleting user accounts is straightforward; delete the user’s NDS object, and the user will subsequently be unable to log in to that object.

In addition, you should archive and then delete the user’s home directory.

Protecting Administrative Accounts (Client)

“Protecting Administrative Accounts (Client)” on page 126 provides an explanation of what administrators do in a NetWare Enhanced Security system.

When initially installed, your NetWare system has one NDS administrative account, ADMIN, and one bindery administrative account on each server, SUPERVISOR.

You must create additional NDS administrative accounts by creating User objects and assigning them rights either directly or by making them security equivalent to other objects (for example, ADMIN).

For additional warnings associated with the bindery SUPERVISOR account, see “Setting a Bindery Context” on page 60.

Only trusted individuals should be granted rights to modify the security-relevant NDS properties (such as user passwords). Your organization may have a site security policy that is more restrictive. For example, you may restrict the changing of phone numbers to trusted individuals.

Before assigning any NDS rights, you should check both the maximum rights described in this document and your site security policy to ensure that you are not violating either set of rules.

If you have more than one administrator, you must create an administrative account for each administrator. Then you should disable the ADMIN account. By so doing, you will be able to determine from audit trails which administrator performed a given action, thus providing accountability.

Because administrative accounts can be used to modify the behavior of your NetWare servers, it is important that they be properly protected.

Passwords for administrative accounts should be chosen especially carefully to prevent intruders from gaining access. While there is no specific requirement, it’s a good idea to change administrative passwords frequently (monthly, for example).

Intruder detection can be used to deny access to administrative accounts. Be sure that you have at least one account that is not subject to intruder lockout for every object.

That is, if you have a container with its own administrator, be sure there is some administrator (probably in a different container) whose account cannot be locked out who can manage that container. Otherwise, an attacker may be able to prevent you from gaining access to your system.

If you perform both administrative and nonadministrative tasks (for example, setting user passwords *and* writing memos), you should have two or more accounts. Use of the administrative account should be restricted to those occasions when you are performing administrative actions.

When using your administrative account, you must only use that software identified by your client vendor as being part of the NTCB partition. By so doing, you will minimize the risks from accidents, as well as minimize the effects of erroneous or malicious software.

Import/Export of NDS Objects

The NetWare operating system does not provide for the import or export of NDS objects.

The backup and restore facilities described in Chapter 12, “Security Supplement to Backing Up and Restoring Data,” on page 165 and in Chapter 9, “Backing Up and Restoring Data,” of *Supervising the Network* are intended for backing up and restoring NDS data within a network, not for interchange of NDS data among servers on different networks.

Client components may include facilities to perform the importing or exporting of NDS objects. Consult your client trusted facility manual to determine if such facilities are included, and if so how those facilities manage import and export of access control information (namely, trustee lists).

chapter 5

Security Supplement to Managing Directories, Files, and Applications

This chapter contains supplementary NetWare® Enhanced Security information for Chapter 2, “Managing Directories, Files, and Applications,” of *Supervising the Network*.

Most sections provide supplementary information for the corresponding headings in *Supervising the Network*. The final section, “Import/Export of File System Objects” on page 136, describes the importing and exporting of file system objects.

Planning Directory Structures

Warning

The contents of the SYS:LOGIN directory (and all subdirectories) are public and may be read by users before they login to the server component. This is necessary to support diskless clients and to facilitate upgrades and maintenance of the software required by a client to log in to the server.

Because the SYS:LOGIN directory can be publicly read, you should never copy any additional programs or data (beyond that in the distribution) into the SYS:LOGIN directory, unless you are able to accept the risk that unknown users may have access to those programs or data.

You should not assign any trustees to the SYS:LOGIN directory, to any file in SYS:LOGIN, to any subdirectory of SYS:LOGIN, etc. Depending on the NCP operation used, unlicensed users may or may not have access to files or subdirectories with explicit trustee assignments, even if the trustee assignment is for [Public].

Warning

The High Capacity Storage System (HCSS) is not included in the server’s NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

The NetWare Enhanced Security network architecture permits using the server component’s file system for storage of client TCB and non-TCB programs. As far as the server is concerned, these programs are data files, subject to the server’s access control policy.

For descriptions of if and how the server is used for the storage of client TCB programs, see your client documentation.

Warning Any directory or file with explicit or inherited File Scan rights for the [Public] user can be listed by all users on the server. Consequently, you shouldn't give such objects sensitive names (such as FIRINGS.TXT), even if no one can read the data within the files.

NetWare Application Manager^{TM} is a client utility. For information on how to use it in the evaluated configuration, see your vendor's client documentation.

Creating Directories and Copying Files (Client)

Warning For a listing of trusted computing base utilities that you can use at the client to manage NDS^{TM} (NetWare Directory Services^{TM}) objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

Any client program that generates the proper NetWare Core Protocol^{TM} (NCP^{TM}) messages can manipulate the file system on behalf of the user logged in to that client connection.

Warning The High Capacity Storage System (HCSS) is not included in the server's NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Warning Macintosh*, OS/2*, and UNIX® name spaces are not supported in the server's Enhanced Security configuration. DOS is the only name space supported by the server.

Loading Operating Systems and Applications onto the Network (Client)

For a listing of TCB utilities (such as FLAG) that you can use at the client to manipulate trustee rights to client operating system and application directories on the server, see your client documentation.

However, any client program that generates the proper NetWare Core Protocol (NCP) messages can manipulate the file system on behalf of the user logged in to that client connection.

The NetWare Enhanced Security network architecture permits using the server component's file system for the storage of client TCB and non-TCB programs. However, client operating systems and applications vary from one client component to another.

For descriptions of how that component uses the server for storage of client operating systems and applications, see your client documentation.

Fake root directories can be used in login scripts to map a drive to a nonroot directory on the server. The server does not prevent access to directories located above the fake root, and should not be relied on as a security measure.

Creating and Using Directory Map Objects (Client)

A Directory Map object is a particular type of NDS object that contains a pointer to a directory in the file system. Interpretation of the Directory Map object is performed solely by the client—that is, the server does not convert an access to a Directory Map object into the corresponding access to a file system directory.

The creation of Directory Map objects by administrators and subsequent accesses to Directory Map objects by network users are subject to the server's NDS access control policies.

Warning

For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

Setting Up and Using NetWare Application Management Software

NetWare Application Manager and NetWare Application Launcher^{TM} are client utilities. For descriptions of how to use them in the evaluated configuration, see your client documentation.

Making the File System Secure and Accessible (Client)

This section describes trustee rights to files and directories (which apply to specific named users, groups, or roles) and directory/file attributes (which apply to all users). It contains procedures for:

- Adding a trustee to a directory or file
- Deleting a trustee from a directory or file
- Modifying a trustee's rights to a directory or file
- Viewing and modifying the Inherited Rights Filter for directories and files
- Changing attributes of a directory or file
- Changing the owner of a directory or file.

For a description of the server's file system access control policy, see *Security Features User Guide*.

Warning Directory and file attributes are not addressed in the server component access control policy (they are considered to be additional features). Because these features are not addressed in the access control policy, you should not use these attributes to protect information in directories or files.

Access to files and directories is controlled primarily by trustee rights, not by ownership. However, there are a few NetWare Core Protocol file requests in which the file owner has additional rights not explicitly granted by trustee rights.

Warning For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and the NETADMIN text utility. They may also include other utilities.

Warning To maintain a NetWare Enhanced Security facility, you must ensure that trusted computing base (TCB) files and directories are protected such that nonadministrative users cannot read or modify the contents of the TCB files and directories.

The following table identifies the required file system rights for key TCB directories.

Volume root directory	Do not define any administrative or nonadministrative trustees for the volume root directory (for example, SYS:\). Explicit access rights (such as File Scan) to the root directory are not required in order for users to access lower-level directories and are inherited at lower-level directories, thus making it much more difficult to protect lower-level files and directories. For example, a user with a trustee assignment to the SYS:PUBLIC\FOO directory has an implicit File Scan right to all parent directories (including SYS:\ and SYS:PUBLIC). Thus, the user does not require explicit trustee assignments for the parent directories. Further, without an Inherited Rights Filter (IRF) or explicit trustee assignment, the trustee rights assigned to SYS:PUBLIC\FOO are inherited for all subdirectories and files below that directory (for example, SYS:PUBLIC\FOO\BAR).
SYS:SYSTEM	The SYS:\SYSTEM directory contains the server's NetWare Enhanced Security NLM^{TM} programs and TCB data files. It should not have any administrative or nonadministrative trustees. Any user who is security equivalent to the volume SYS: (such as ADMIN in the standard configuration) can read or write any file or directory in the volume.
SYS:PUBLIC	This directory is commonly used as a shared storage directory for non-TCB data, such as client utilities and documentation. To make the directory accessible to all users, the [Public] trustee should be given Read and File Scan rights to SYS:PUBLIC (this is done automatically as part of installation). Because this directory stores files that may be used by a client TCB, you should not provide Create, Write, Modify, or Delete rights to any nonadministrative users.

SYS:CDROM$$.ROM	This directory contains prebuilt indexes of CD-ROMs that have been mounted on the server. It should not have any administrative or nonadministrative trustees.
User home directories	The user trustee should be given all rights to his or her home directory. You may wish to restrict Supervisor and/or Access Control rights to prevent users from allowing other users to access their files.
SYS:LOGIN	The SYS:LOGIN directory contains the client programs and data files necessary for a user to log in to the server. You should not define any nonadministrative trustees to this directory. Because the server gives File Scan and Read rights to the SYS:LOGIN directory before the user logs in, you must not use this directory for the storage of arbitrary data. Further, you must not permit general users to store data in this directory.
SYS:_NETWARE	The SYS:_NETWARE directory contains the server's audit configuration and audit files. You cannot add trustees to this directory. This directory can be accessed only by the server operating system.
SYS:QUEUES	The SYS:QUEUES directory contains files that have been queued for printing. You should not define any nonadministrative trustees to this directory.
SYS:DELETED.SAV	The SYS:DELETED.SAV directory contains files that have been deleted, but not purged, when the directory they were in was deleted. This directory should not have any administrative or nonadministrative trustees.
SYS:DOC	The SYS:DOC directory contains the online NetWare documentation. To make the directory accessible to all users, the [PUBLIC] trustee should be given Read and File Scan rights. Because the security of the server depends in part on your ability to access the security documentation (such as this manual) you should not provide Created, Write, Modify, or Delete rights to any nonadministrative users.

Beyond the restrictions described above, there are no other limitations on rights assignments in the NetWare Enhanced Security configuration.

However, your site security policy may require protection of other directories. For example, if you keep shared applications (such as word processing or spreadsheet programs) on your NetWare server, then you will probably want to give nonadministrative users Read and File Scan rights to the applications directories (but not Access Control, Write, Delete, Modify, Erase, or Create rights).

Warning

Use an Inherited Rights Filter (IRF) to restrict inherited rights to subdirectories and files within the file system.

In general, you cannot close off access to a subdirectory (e.g., SYS:PUBLIC\FOO\BAR) by giving the user a restricted trustee assignment to the parent directory (SYS:PUBLIC\FOO). However, a specific trustee assignment to SYS:PUBLIC\FOO\BAR would override an assignment to the same trustee for SYS:PUBLIC\FOO.

Note that the IRF filters out access rights for all users except those with Supervisor rights. For more information, see “Rights” in *Concepts*.

Warning

If you change the rights in a trustee assignment to a file or directory, the changes will take effect for the next file open attempt. However, a user who currently has the file open will not have that access revoked.

If you must immediately enforce access control changes, you must either close all user connections or bring down and reboot the server.

Warning

Deleting a trustee from a directory or file can *increase* a user’s rights, if by so doing it allows rights assigned higher up in the tree to be inherited further down. When deleting a trustee of a sensitive directory, be sure you understand the implications to access controls for other files and directories.

Viewing Effective Rights and Other Information (Client)

Warning

For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility, the NETADMIN text utility, FILER, and NDIR. They may also include other utilities.

Salvaging and Purging Deleted Files and Directories (Client)

Warning For a listing of trusted computing base utilities that you can use at the client to manage NDS objects, see your client documentation. Utilities for clients may or may not include the NetWare Administrator graphical utility and FILER. They may also include other utilities.

Because any trustee with Create, Read, and File Scan rights can undelete a file, it isn't really gone when you delete it. If you want to make sure that a file cannot be recovered, you should do one of the following:

- Before you delete the file, make yourself a trustee with Create, Read, and File Scan rights, and then set an IRF to block all rights to the file (which means that no else will have the Create, Read, and File Scan right unless they also have Supervisor rights).
- Set the Purge Immediate attribute before deleting the file. When a file is purged, it cannot be recovered.
- If the PURGE utility is supported in your client (workstation) TCB, use the PURGE command to purge the directory the file is in when the file is deleted.

Import/Export of File System Objects

The NetWare operating system does not provide for the import or export of file system objects.

The backup and restore facilities described in Chapter 12, "Security Supplement to Backing Up and Restoring Data," on page 165 and in Chapter 9, "Backing Up and Restoring Data," of *Supervising the Network* are intended for backing up and restoring file system data within a network, not for interchange of file system data among servers on different networks.

Client components may include facilities to perform the importing or exporting of file system objects. Consult your client trusted facility manual to determine if such facilities are included, and if so how those facilities manage import and export of access control information (namely, trustee lists).

chapter

6 Security Supplement to Creating Login Scripts

This chapter contains supplementary NetWare® Enhanced Security information for Chapter 3, "Creating Login Scripts," of *Supervising the Network*.

Login scripts are NDS™ (NetWare Directory Services™) object properties associated with NDS container, profile, and user objects. The client LOGIN.EXE program (for DOS, Windows*, and OS/2*) interprets and executes these scripts on the client component after a user or administrator logs in to the server component.

The server NTCB partition treats these login scripts as arbitrary data stored in the NDS object properties. It enforces the NDS object property policy for accesses to the login scripts, thus controlling who can read and modify login scripts. The server does not, however, interpret the contents of login scripts or determine the adequacy of login scripts.

Because the login script executes on the client and not on the server component, it is the responsibility of the client administrator to define and install login scripts. For more information on defining the login scripts for each specific client component, see your client documentation.

Warning

As a server administrator, you must ensure that your login script executes properly on any workstations that you use for administration of the server. Check to make sure that your login script does not include any commands that are not part of the TCB for the client that you are using.

Further, you must protect your login script and profile properties so that they cannot be modified by nonadministrative users.

Warning

As a server administrator, you are responsible for resolving potential conflicts involving login scripts. For example, there may be multiple client administrators that share a single container login script.

chapter 7

Security Supplement to Maintaining NetWare Networks

This chapter contains supplementary NetWare® Enhanced Security information for Chapter 4, “Maintaining NetWare 4 Networks,” of *Supervising the Network*.

Introduction

Warning Before installing any patches on your NetWare 4™ server, you must verify that the patches have been included in the NetWare Enhanced Security configuration. *NetWare Enhanced Security Server* identifies the version of each NetWare program included in the evaluated configuration.

NetWare patches and updates may also affect client programs such as the NetWare Administrator utility. Before installing patches that affect client programs, verify that the patched version is included in the evaluated configuration for the client component you are using. Updating to unevaluated client or server software may invalidate the C2 rating of your server or client workstation.

Identifying Network Monitoring and Maintenance Tools

NetWare Administrator, NETADMIN, NDS Manager, and PARTMGR are all client tools. To determine whether these tools are included in the client evaluated configuration, see your client vendor’s trusted facility manual.

Monitoring and Maintaining Network Communication

Warning You must use only evaluated components (including routers and WAN links) in the NetWare Enhanced Security configuration.

Monitoring and Maintaining Replica Synchronization

Warning The RCONSOLE utility relies on NLM^{TM} programs that are not included in the NetWare Enhanced Security configuration. Therefore, you must use DSREPAIR at the server console and not using a remote console session.

Monitoring and Maintaining Time Synchronization

Use extreme caution in adjusting time synchronization. The NetWare Enhanced Security configuration relies on accurate time values for determining when users are authorized to be logged in, for NDS^{TM} (NetWare Directory Services^{TM}) replication, and for accurate recording of audit events.

If your server clock is inaccurate, your audit trails may not accurately represent when events occurred. If your server clock is not synchronized with other clocks in the network, replication of NDS changes may be performed incorrectly, causing incorrect results.

Warning The EDIT utility is not part of the NetWare Enhanced Security configuration. To edit the TIMESYNC.CFG file, you should use a trusted editor running on a trusted client. To identify an editor that can be used for editing system configuration files, see your client documentation.

Monitoring and Maintaining Backward Compatibility

Warning Existing NetWare servers cannot be upgraded to the NetWare Enhanced Security configuration. Rather, you must install NetWare in the evaluated configuration onto a newly formatted disk. Additionally, older NetWare servers (that is, before NetWare 4.11) must not coexist in an NetWare Enhanced Security network.

chapter **8**

Security Supplement to Managing the NetWare Directory Tree

This chapter contains supplementary NetWare® Enhanced Security information for Chapter 5, “Managing the NetWare Directory Tree,” of *Supervising the Network*.

As described in *Guide to NetWare 4 Networks*, NetWare Directory Services™ (NDS™) is a hierarchical distributed database that contains management information about servers, users, printers, etc.

About NetWare Directory Services

For a listing of TCB utilities that you can use at the client to manage NDS partitions, see your client documentation. Possible utilities include, but are not limited to, the NDS Manager and PARTMGR utilities described in the associated text in *Supervising the Network*.

However, any client program that generates the proper NetWare Core Protocol™ (NCP™) messages can manipulate the NetWare Directory database on behalf of the user logged in to that client connection.

DSREPAIR and DSMERGE are NLM™ programs that can be loaded and run at the server console. However, DSTRACE is a SET parameter rather than an NLM program. It is controlled by entering SET DSTRACE=ON or SET DSTRACE=OFF.

Creating and Managing Directory Services Partitions (Client)

Warning

The NetWare Enhanced Security network architecture requires that all network servers must be NetWare Enhanced Security servers (running NetWare 4.11 or later). Thus, there will not be any NetWare 3^{TM} servers on the network.

Refer to your client documentation for a listing of TCB utilities that you can use at the client to manage NDS partitions. Possible utilities include, but are not limited to, the NDS Manager, PARTMGR, and NCUPDATE utilities described in the associated text in *Supervising the Network*.

However, any client program that generates the proper NetWare Core Protocol (NCP) messages can manipulate the NetWare Directory database on behalf of the user logged in to that client connection.

Warning

The associated information in *Supervising the Network* suggests limiting access to partition management by restricting access to the files NDSMGR16.EXE, NMSNAP16.DLL, and NDSMGR32.DLL in SYS:PUBLIC, which are used for partition management, or to PARTMGR.EXE itself.

This procedure is not necessary (nor would it be effective), since the server protects partitions by performing access checks on each incoming NCP message.

Removing NetWare Directory Services from a Server (Console)

Warning

The NetWare Enhanced Security network architecture allows the server component to provide NDS support to client NTCB partitions—for example, to store client authentication and audit data. Make sure that this data exists elsewhere in a master replica, or (if this server contains the master replica) that you designate another server as holding the master.

Warning

Before removing NDS from a server, make sure that all changes to the partition are synchronized to other replicas. This will be easier to do if you disable workstation logins (DISABLE LOGIN) and take down any existing connections (CLEAR STATION).

Deleting a NetWare Server Object from the NDS Database (Console, Client)

For a listing of TCB utilities that you can use at the client to delete a server object from NDS, see your client documentation. Possible utilities include, but are not limited to, the NDS Manager and PARTMGR utilities described in the associated text in *Supervising the Network.*

Repairing the NetWare Directory Database (Console)

REMOTE.NLM is not loaded in the NetWare Enhanced Security server configuration, consequently, you cannot access the server via a remote console (RCONSOLE). For further information on the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Merging NDS Trees (Console)

Warning REMOTE.NLM is not loaded in the NetWare Enhanced Security server configuration, consequently, you cannot access the server via a remote console (RCONSOLE). For further information on the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server.*

Warning Merging NetWare Directory trees could result in users gaining or losing rights, if there are users who are trustees of [Root].

The Access Control List (ACL) for the [Root] of the merged tree is calculated as follows:

- Any rights for trustees other than [Root] or [Public] are copied from the source tree to the merged tree.

- Any rights for trustees other than [Root] or [Public] are copied from the target tree to the merged tree.

  Note that, other than [Root] and [Public], there cannot be any trustees of the [Root] of both the source and target trees. This is because the only trustees other than [Root] and [Public] are actual NDS objects, which would be part of one tree or the other, but not both.

- Any rights for the [Public] trustee from the source tree are discarded.

- Any rights for the [Public] trustee from the target tree are copied to the merged tree.

- Any rights for the [Root] trustee in the source tree are added to the rights for the [Root] trustee in the target tree, and the result is copied to the merged tree.

  That is, if [Root] in the source tree has the Read rights to the Login Script property of the source [Root], and [Root] in the destination tree has the Write rights to the Login Script property of the target [Root], then the merged tree will have [Root] as a trustee with both Read and Write rights for the Login Script property.

For example, if the ACL of the [Root] of the source tree (ALPHA) is:

SMITH.ALPHA	[Entry Rights]	Create
JONES.ALPHA	[All Properties Rights]	Read
[Public]	Bindery Property	Read, Write
[Public]	[All Properties Rights]	Read
[Root]	[All Properties Rights]	Compare

And the ACL of the target tree (BETA) is:

SMITH.BETA	Access Control List	Read
[Public]	Bindery Property	Read
[Root]	[All Properties Rights]	Write
[Root]	Bindery Property	Add or Delete Self

Then the ACL of the merged tree (BETA) will be:

SMITH.ALPHA	[Entry Rights]	Create
JONES.ALPHA	[All Properties Rights]	Read
SMITH.BETA	Access Control List	Read
[Public]	Bindery Property	Read
[Root]	[All Properties Rights]	Compare, Write
[Root]	Bindery Property	Add or Delete Self

Note that the [Public] trustee has rights from the target tree (the rights from the source tree are discarded), while [Root] has the union of rights from the source and target trees.

Viewing and Managing NDS Synchronization Status (Console)

When a change is made to an NDS object in a master replica or read/write replica, there may be an arbitrarily long delay before NDS can synchronize the change to all replicas throughout the network. The following procedure explains how an administrator can determine that a specific change has propagated to each replica.

Procedure

1. **Determine which NetWare Directory partition contains the objects you wish to modify.**

2. **Make the change(s) using a client utility.**

   To determine what tools may be used for changing NDS objects and NDS object properties, see your client documentation.

3. **At the console of any server with a read/write copy of the replica for the partition you've changed, enter either of the following commands:**

   `SET NDS TRACE TO SCREEN=ON` <Enter>

   or

   `DSTRACE=ON` <Enter>

   (The two commands are equivalent.)

4. **Observe the DS trace messages and look for a message of the form:**

   ```
   SYNC: End sync of partition <name> All processed
   = YES.
   ```

   When this message appears, all replicas have synchronized all changes, so your change is now copied to all replicas. There is also a similar message:

   ```
   SYNC: Update to server <CN=name> successfully
   completed
   ```

   This message indicates that a server has synchronized with one replica of the partition, but does not indicate that all replicas have been synchronized. Only the "All Processed" message indicates that the change has been propagated to all replicas of the partition.

5. **You may turn off tracing after observing synchronization by using either of the following console commands:**

   `SET NDS TRACE TO SCREEN=OFF` <Enter>

   or

   `SET DSTRACE=OFF` <Enter>

   (The two commands are equivalent.)

6. **Repeat the process for objects in other NetWare Directory partitions.**

Warning

It may take an arbitrarily long time before the synchronization occurs. If you do not see the synchronization message within approximately one minute, you should verify that the other servers holding replicas of the partition are up and that there are no network problems.

Depending on the values of the NDS synchronization parameters, it may take more or less time for the synchronization to occur. For information regarding the NDS SET parameters, see Chapter 20, “Security Supplement to Utilities Reference,” on page 309 and “SET” in *Utilities Reference*.

chapter 9

Security Supplement to Migrating Data Using the HCSS

This chapter contains supplementary NetWare® Enhanced Security information for Chapter 6, “Migrating Data Using the High Capacity Storage System,” of *Supervising the Network*.

Warning

The High Capacity Storage System (HCSS) is not included in the server’s evaluated configuration and should be disregarded for purposes of running a trusted facility. For a description of the server’s NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

chapter 10 Security Supplement to Maintaining the NetWare Server

This chapter describes routine maintenance operations performed by a NetWare® Enhanced Security administrator. It includes the procedures described in Chapter 7, “Maintaining the NetWare Server,” of *Supervising the Network*.

Starting the Server (Console)

There are several ways to boot the server. As described in “SERVER” in *Utilities Reference*, the simplest method is to add a SERVER.EXE command to the server's AUTOEXEC.BAT file. Subsequently, when you power on the server, it loads the server operating system, as follows:

1. The Basic Input/Output Services (BIOS) firmware on the system board loads DOS. In turn, DOS executes the C:AUTOEXEC.BAT file and, by inclusion, SERVER.EXE.

2. SERVER.EXE is a DOS program that loads the NetWare Enhanced Security core operating system into memory, initializes the server hardware for its own use, executes the STARTUP.NCF file, mounts volume SYS:, executes the AUTOEXEC.NCF and INITSYS.NCF files, and displays the NetWare console prompt (:) at the server console.

Warning: Do not specify the optional parameters (–s, –na, –ns) when you boot the server for normal operation. This is because the STARTUP.NCF, AUTOEXEC.NCF, and INITSYS.NCF files help initialize the server's secure state. Use the boot options only when you are debugging the server, and at that time be extremely careful.

Warning: Use only the version of DOS identified in *NetWare Enhanced Security Server* ro boot your NetWare server. When running DOS, use only those DOS commands identified in *NetWare Enhanced Security Server*.

Using the Console (Console)

As described previously, when you boot the server it displays a colon (:) prompt at the server console. When you see this prompt, you can enter any of the console commands, such as BROADCAST (send a message to all users), DISABLE LOGIN (prevent users from logging in to the server), and LOAD (load an NLM™ program into memory). For additional information on using the console commands, see *Utilities Reference*.

The server provides the ability to switch between the server console screen and screens provided by other NLM programs. For example, if you've loaded PSERVER, MONITOR, and SERVMAN NLM programs, you can type <Ctrl>+<Esc> (simultaneously press <Ctrl>and <Esc>) and you will see a screen similar to the following:

```
Current Screens
1. System Console
2. NetWare 386 Print Server
3. Monitor Screen
4. Server Manager
Select Screen to View:
```

Thus, you would type 1 to return to the system console (where you will see the console colon prompt) or 3 to bring up the screen for MONITOR.NLM.

When you are finished, you can press <Ctrl>+<Esc> again to select a different screen.

Alternately, you can press <Alt>+<Esc> repeatedly to cycle sequentially through the screens.

Warning

In order to run a NetWare Enhanced Security facility using the server component, you must keep a manual log of all administrators who use the server console. For more information, see *Auditing the Network*.

Common Management Tasks

This section addresses the “Common Management Tasks” section in Chapter 7 of *Supervising the Network*.

Sending Console Messages to Workstations (Console)

Warning

Do not use this mechanism to send messages containing sensitive information. You cannot tell whether a user is physically at a workstation when you send a message.

Booting the Server with the EXIT Command (Console)

Warning

The remote console (RCONSOLE.NLM) is not part of the NetWare Enhanced Security configuration and should not be loaded.

Because your AUTOEXEC.NCF file must contain a REMOVE DOS command (as described in Chapter 3, “Security Supplement to Installation,” on page 69), the computer will automatically reboot DOS when you type EXIT.

Depending on the contents of your AUTOEXEC.BAT, DOS may or may not reboot the server operating system after the computer restarts.

Loading a NetWare Loadable Module (Console)

Warning

Do not load NLM programs from diskette. All NetWare Enhanced Security NLM programs can be accessed from the SYS:SYSTEM directory on hard disk.

For information on unloading NLM programs (that is, removing them from memory and freeing up the memory to cache), see “UNLOAD” in *Utilities Reference*.

Loading and Binding LAN Drivers (Console)

Warning

The specific network media, interface controllers, and drivers are defined by Novell's Yes program. For information about determining the most recent set of LAN drivers included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server.*

Warning

INETCFG.NLM is not included in the NetWare Enhanced Security configuration. Instead, use the LOAD and BIND commands at the console prompt or INSTALL.NLM to load network drivers.

Warning

Only the IPX^{TM} protocol stack is included in the NetWare Enhanced Security configuration. TCP/IP and AppleTalk* are not supported.

Viewing and Adding Server Search Paths (Console)

If you run only the NetWare Enhanced Security configuration (no unevaluated NLM programs) on your server, it should not be necessary to add or delete search paths. All the NetWare Enhanced Security NLM programs are included in the SYS:SYSTEM directory.

Installing, Uninstalling, and Configuring a Server Product (Console)

Warning

Before installing new software or configuring the existing server software, review the installation warnings in Chapter 3, "Security Supplement to Installation," on page 69. Install *only* those products identified in *NetWare Enhanced Security Server*.

Copying NetWare Files (Console)

Warning

Before installing new software or configuring the existing server software, review the installation warnings in Chapter 3, "Security Supplement to Installation," on page 69.

Extracting NetWare Files from the Installation CD-ROM (Client)

Warning

Do not use NWXTRACT to install files or NLM programs that are not part of the server NetWare Enhanced Security configuration.

Creating or Editing a Server Batch File (Console)

Warning

Before editing the server batch files, review the installation warnings in Chapter 3, "Security Supplement to Installation," on page 69.

Editing Text Files from the Server Console (Console)

Warning

EDIT.NLM is not included in the server’s NetWare Enhanced Security configuration.

Changing the Server Keyboard Type

Warning

KEYB.NLM is not included in the server’s NetWare Enhanced Security configuration.

Viewing and Setting Server Time and Time Zone (Console)

Warning

If you modify Time Synchronization parameters, be sure to monitor the clocks for the various servers to ensure that each server keeps its clocks synchronized with other servers. If a clock drifts out of synchronization, audit timestamps may not be valid.

Changing a Server’s Name or IPX Internal Network Number (Console)

Warning

Before performing these procedures, review the installation warnings in Chapter 3, “Security Supplement to Installation,” on page 69.

Monitoring and Optimizing the Server

This section addresses the “Monitoring and Optimizing the Server” section in Chapter 7 of *Supervising the Network*.

Assessing Server RAM (Console)

Warning

As described in Chapter 3, “Security Supplement to Installation,” on page 69, the AUTOEXEC.NCF file must be configured to remove DOS automatically each time the server boots. Consequently, you will not be able to free up additional memory by running REMOVE DOS.

Prioritizing Server Processes (Console)

Warning

SCHDELAY.NLM is not included in the NetWare Enhanced Security configuration. Consequently, do not use “LOAD SCHDELAY” to set an initial priority for a newly loaded process. Instead, after you LOAD an NLM program, use MONITOR to increase or decrease the scheduling delay.

Improving Server Performance (Console)

Warning

You cannot migrate files from the hard disk to other media (such as magneto-optical) using the High Capacity Storage System (HCSS). The required NLM programs are not included in the NetWare Enhanced Security configuration.

Viewing the Server Error Log (Console, Client)

Warning

The SYS$LOG.ERR file is not intended to meet the NetWare Enhanced Security auditing requirements. For information on the files used for audit collection and audit administration, see *Auditing the Network*.

Even though SYS$LOG.ERR is not used for management of a NetWare Enhanced Security network, it does contain security-relevant information and should be protected from access by general users.

The NETADMIN and FILER utilities run on the client component. For information on client utilities, see the client's trusted facility manual.

Maintaining Volumes

This section addresses the "Maintaining Volumes" section in Chapter 7 of *Supervising the Network*.

Creating Volumes (Console)

Warning

HCSS.NLM is not included in the NetWare Enhanced Security server configuration. Consequently, you cannot create volumes on magneto-optical volumes. For a complete list of NetWare Enhanced Security components, see *NetWare Enhanced Security Server*.

Deleting Volumes (Console)

Warning

HCSS.NLM is not included in the NetWare Enhanced Security server configuration. See *NetWare Enhanced Security Server*.

Warning

If you delete a volume, you will lose all the audit data associated with the volume. Be sure to back up all audit data before deleting the volume.

Renaming Volumes (Console)

Warning Do not attempt to rename volume SYS: to another name. Volume SYS: is required for proper operation of the server TCB.

Warning If you rename a volume, you will lose all the audit data associated with the volume. Be sure to back up all audit data before renaming the volume.

Setting Up a Volume to Store Non-DOS Files (Console)

Warning Do not load the Macintosh*, OS/2*, or UNIX® name spaces (.NAM files) on the server. These NLMs are not included in the NetWare Enhanced Security configuration. DOS is the only name space supported by the server.

Repairing Volumes (Console)

Warning Do not load VREPAIR name space modules. DOS is the only name space supported by the server.

Warning Because VREPAIR may delete corrupted TCB configuration or data files, you should use the (default) option to save deleted files. For more information, see “VREPAIR” description in *Utilities Reference*. After you run VREPAIR, do not remount the volume until you have determined that no TCB files were deleted.

Using a CD-ROM as a NetWare Volume (Console)

Warning Do not use the /MAC or /NFS options with the CD MOUNT or CD CHANGE commands. The Macintosh and NFS* name spaces are not included in the NetWare Enhanced Security configuration.

Managing Server Hard Disks

This section addresses the "Managing Server Hard Disks" section in Chapter 7 of *Supervising the Network*.

Checking Available Disk Space with NDIR (Client)

For more information on the NDIR utility, see the client vendor's documentation.

Using File Compression (Client)

For more information on the FLAG, FILER, and NetWare Administrator utilities, see the client vendor's documentation.

Setting Compression for a File or Directory (Client)

For more information on the FLAG, FILER, and NetWare Administrator utilities, see the client vendor's documentation.

Purging Files from a Disk (Client, Console)

Before manually purging deleted files, see the client vendor's documentation for more information on the PURGE, FILER, and NetWare Administrator utilities.

Adding Optical Storage for File Migration (Console)

Warning HCSS.NLM is not included in the NetWare Enhanced Security server configuration. For more information, see *NetWare Enhanced Security Server*.

Adding a Hard Disk to the NetWare Server (Console)

Warning Before beginning installation of a hard disk drive or controller, see *NetWare Enhanced Security Server* for instructions on determining whether the device is included in the NetWare Enhanced Security configuration.

Loading Disk Drivers (Console)

Warning

For instructions on determining whether a disk driver is included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Deleting NetWare Disk Partitions (Console)

Warning

Other than the DOS partition used for booting the system, you should not have any other non-NetWare operating systems (OS/2, UNIX, XENIX*) loaded on a server disk drive. If such operating systems are booted, they could damage data stored on NetWare partitions.

Disaster Prevention and Recovery

This section addresses the "Disaster Prevention and Recovery" section in Chapter 7 of *Supervising the Network.*

Securing the Server Console (Console)

Warning

The console security features provided by the SECURE CONSOLE command are recommended, but not required, for secure operation because the NetWare Enhanced Security network must provide physical protection for the server console.

Preventing Virus Infection (Console)

Warning

The Execute-Only file attribute cannot be counted on to protect executables from modification. You must also configure file trustees to prevent files from unauthorized modification.

Warning

The bindery SUPERVISOR account must never be used in the NetWare Enhanced Security configuration. Each administrator must have his or here own account for server administration. Failure to follow this policy will result in a lack of accountability for administrative actions.

Preventing Packet Forgery (Console, Client)

Warning

The NCP Packet Signature mechanism protects against forgery of NCP messages. Because the NetWare Enhanced Security architecture (a) provides mechanisms to prevent “spoofing” of IPX addresses by untrusted software and (b) requires physical or cryptographic protection of the network media, the packet signature mechanism is not required in a NetWare Enhanced Security facility.

Warning

The Packet Signature only protects against the forgery of NCP messages. It does *not* protect other non-NCP protocols, for example, the SPX$^{\text{TM}}$-based print and backup protocols. Packet Signature also does not provide any additional assurance that the server's NetWare Enhanced Security software works properly. It is of use only when the underlying assumption of physically or cryptographically protected network media does not hold.

For more information about setting the client-side packet signature configuration, see your client vendor’s documentation.

Activating UPS Monitoring (Console)

Warning

UPS.NLM, UPS_AIO, AIOCOMX, and DCB.DSK are not included in the server's NetWare Enhanced Security configuration. Consequently, you should not use UPS.NLM to configure UPS monitoring. For more information on the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Using Remote Console to Manage a Server

Warning

The remote console NLM program (REMOTE.NLM) is not part of the server component's NetWare Enhanced Security configuration, and you should not load it on the server. Consequently, you should disregard the entire description of using a remote console to manage a server.

Administering Accounting

This section addresses the “Administering Accounting” section in Chapter 7 of *Supervising the Network.*

Accounting is not a NetWare Enhanced Security issue, but the server *does* provide accounting mechanisms and workstation clients may provide administrative utilities to manage the accounting data.

Setting Up Accounting (Client)

NetWare Administrator and NETADMIN are client utilities. For more information on their availability and use, see your client trusted facility manual.

Viewing Accounting Totals (Client)

ATOTAL is a client utility. For more information on its availability and use, see your client trusted facility manual.

chapter 11 Security Supplement to Maintaining NetWare SMP

This chapter contains supplementary NetWare® Enhanced Security facility information for Chapter 8, “Maintaining NetWare SMP,” of *Supervising the Network*.

Warning NetWare SMP is not included in the server’s NetWare Enhanced Security configuration and should be disregarded for purposes of running a NetWare Enhanced Security facility. For a description of the server’s NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

chapter 12 Security Supplement to Backing Up and Restoring Data

This chapter contains supplementary NetWare® Enhanced Security facility information for Chapter 9, “Backing Up and Restoring Data,” of *Supervising the Network*. That chapter describes the use of NetWare Storage Management Services^TM^ (SMS^TM^) software and the SBACKUP utility to back up and restore NetWare 4.11 NDS^TM^ and file system data.

Understanding Storage Management Services (SMS)

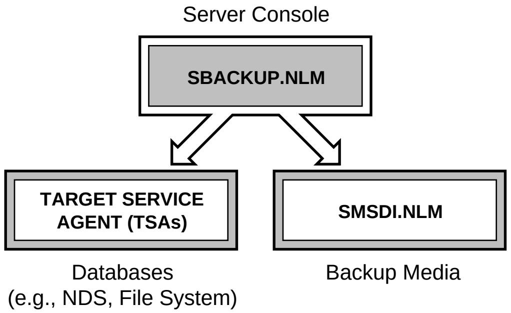
The SMS architecture, shown in Figure 12-1, provides capabilities for backing up and restoring network data.

Backups are controlled by a Storage Management Engine (SME)—in this case, SBACKUP.NLM.

During backups, the SME moves data from various storage targets (NDS or file system) on the network to a Storage Device Interface (SMSDI.NLM) on the local server.

During restoration, the SME moves data from the storage media to the appropriate target NLM^TM^ program.

Figure 12-1
SMS Architecture


Server Console
SBACKUP.NLM
TARGET SERVICE AGENT (TSAs)
SMSDI.NLM
Databases (e.g., NDS, File System)
Backup Media

By loading the appropriate Target Service Agent (TSA), it is possible for SMS to back up a variety of different databases on the local server, remote servers, or even on network clients.

The following table identifies the NLM programs that are included as part of the server's evaluated configuration.

Table 12-1

NLM	Description
SBACKUP.NLM	SBACKUP is the SME that manages the backup/restore function for a NetWare Enhanced Security network. It is loaded and run from the server console.
TSA410.NLM	TSA410 backs up and restores NetWare 4.11 file systems. It may be loaded automatically at boot time, but is usually loaded manually at the console just before performing backups.
TSANDS.NLM	TSANDS backs up and restores NetWare Directory databases. It must be loaded in order to back up NDS.
SMSDI.NLM	SMSDI provides a device-independent storage interface for SMS. It is loaded automatically by SBACKUP.
SMDR.NLM	SMDR contains remote procedure code that is used when SBACKUP backs up a TSA on a different server.

Table 12-1

NLM	Description
Drivers	SMS requires device drivers for the attached backup media. The drivers that are permitted in the evaluated configuration are defined in *NetWare Enhanced Security Server*.

Warning

Only the NLM programs listed in the table are included in the evaluated SMS configuration. In particular, the NetWare Enhanced Security server does not include the TSAs necessary to back up client workstations. Even if a workstation contains SMS software, the server will not be able to back it up.

The NetWare Enhanced Security server also does not include TSAs for backing up SQL databases or other application data not supported by the NetWare Enhanced Security server.

However, SMS is an open architecture that permits a variety of backup products. While third-party SMEs may provide additional capabilities (such as backing up client file systems) and alternate administrative interfaces, they cannot be used in the evaluated configuration.

For a complete list of evaluated NLM programs, see *NetWare Enhanced Security Server*.

The SMS protocol provides a means for untrusted client software to access TSANDS or TSA410 and, thus, to read or write the resources that can be accessed by the TSA. The server protects these resources as follows:

1. Each TSA collects the user password and acts as a proxy to log the remote user into the server using that password. The server operating system performs the same authentication calculations as if the user had logged directly into the operating system. If authentication is not successful, the TSA will not permit further access to the target.

2. Subsequent accesses performed by the TSA, on behalf of the user, are mediated by the server operating system using the authenticated identity of the user and the server's DAC policy.

Consequently, it is not possible for a user to bypass the server's TCB using the SMS protocol.

Understanding Target Service Agents (TSAs)

The server evaluated configuration does not include the NLM programs (such as TSADOS or TSAPROXY) necessary to back up client-based TSAs. Consequently, it is not possible to back up clients to a server archive using SMS. For information on how to perform backups on the client component, see your client manuals.

Understanding Supported Storage Devices and Drivers

For information on identifying the storage devices and device drivers that you can use in a NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Using SBACKUP

The TSAs act as a proxy for the administrator that is running SBACKUP. The server makes access decisions based on the identity of the administrator. If you do not have access to all data on the target, you cannot back up that target.

Consequently, *Supervising the Network* recommends logging in to SBACKUP (and thus to the target) as ADMIN or as another user who is security equivalent to ADMIN (who has all rights).

The evaluated configuration does not include FTAM, Macintosh*, NFS*, and OS/2* name spaces. For further information about the evaluated configuration, see *NetWare Enhanced Security Server*.

TSAs for earlier server file systems (such as TSA220, TSA311, or TSA400) are not included in the evaluated configuration. Thus, you can only back up NetWare 4.11 file systems in a NetWare Enhanced Security network. For more information, see *NetWare Enhanced Security Server*.

Backup Types

HPFS drives and non-DOS name spaces (such as FTAM, Macintosh, NFS, and OS/2) are not supported in the evaluated configuration. For more information, see *NetWare Enhanced Security Server*.

Understanding Backup for the NetWare Directory Database

Warning

Supervising the Network warns against using SBACKUP to restore NDS, unless all replicas have been corrupted. This is because a restored replica will be out of sync with other active replicas of the same data.

Warning

TSANDS.NLM does not back up container audit files or audit preselection flags for users. For more information about backing up NDS audit data, see *Auditing the Network*.

Warning

TSANDS.NLM does not back up extensions to the NDS schema. If you rely on schema extensions, you should have other measures in place to back them up.

Warning

When NDS objects are backed up by TSANDS, RSA private keys associated with the objects are encrypted to provide added protection against wiretappers. This additional encryption is not used to meet any C2 requirement.

Backup Software

The NetWare Enhanced Security configuration does not include any third-party backup applications. For information on the backup software that you can use, refer to Table 12-1 on page 166and to *NetWare Enhanced Security Server*.

Understanding Backup for the File System

TSA410.NLM does not back up audit preselection flags (for files and directories) or any audit files. For more information about backing up volume audit data, see *Auditing the Network*.

Warning

SMS does not back up files that are in use (that is, opened by a NetWare client). Consequently, you should perform backups only when the server is not in use.

SMS backs up the associated access control information when an object is written to media and restores the access control information when the object is restored from media.

UNIX® files and files with extended attributes are not supported by the evaluated configuration. For more information, see *NetWare Enhanced Security Server*.

Loading Drivers, TSAs, and Backup Software

The server evaluated configuration does not include the NLM programs (such as TSADOS or TSAPROXY) necessary to back up client-based TSAs. Consequently, it is not possible to back up clients to a server archive using SMS.

For information on how to perform backups on the client component, see your client manuals.

Loading Controller and Storage Device Drivers on the Server

Warning

For information about the specific storage devices and device drivers included in the evaluated configuration, see *NetWare Enhanced Security Server*. The devices and drivers listed in *Supervising the Network* may or may not be approved for use in a NetWare Enhanced Security facility.

Warning

The TSA400, TSA312, TSA311, and TSA220 NLM programs are not included in the evaluated configuration. Consequently, you cannot back up or restore previous versions of NetWare file systems.

The NetWare Enhanced Security server does not include the TSAs (TSADOS, TSAPROXY) necessary to backup DOS, OS/2, UNIX, Windows 95*, or Macintosh workstations.

Backing Up Data

Warning

After you perform a backup, the removable media that you used (such as tape cartridges) will probably contain sensitive user or TCB data. The server cannot protect the data on these removable devices, so you must physically protect the media itself.

Provide at least the same level of physical protection for the media as you provide for the server itself. However, to prevent losing everything in case of fire, flood, or other disasters, you should keep the backup media in a different location than the (physically protected) server room.

Warning Used backup media contain residual user or TCB data. Because the server cannot protect removable media, you must ensure that no one can gain access to residual data on these devices.

For example, do not release used backup tapes back into a common pool of tapes available for general reuse. Destroy any data stored on a backup tape before you discard the tape.

Use procedures appropriate for the sensitivity of the data, for example, bulk erasure or physical destruction. In particular, do not simply erase a media header, since the medium will still contain the archived data.

The NetWare Enhanced Security server does not include the TSAs necessary to backup client workstations. Refer to your workstation trusted facility documentation for information on how to backup data on your workstation.

SBACKUP requests a password for the target in order for the TSA to access the data on the target.

Custom NDS Backup

Warning TSANDS.NLM does not back up container audit files or audit preselection flags for users. For more information about backing up NDS audit data, see *Auditing the Network*.

Warning TSANDS.NLM does not back up extensions to the NDS schema. If you rely on schema extensions, you should have other measures in place in order to back them up.

Warning When NDS objects are backed up by TSANDS, RSA private keys associated with the objects are encrypted to provide added protection against wiretappers. This additional encryption is not used to meet any C2 requirement.

Custom File System or Workstation Backup

TSA410.NLM does not back up audit preselection flags (for files and directories) or any audit files. For more information about backing up volume audit data, see *Auditing the Network.*

Warning SMS does not back up files that are in use (that is, opened by a NetWare client). Consequently, you should perform backups only when the server is not in use by network users.

SMS backs up the associated access control information when an object is written to media and restores the access control information when the object is restored from media.

The RTDM and HCSS products are not included in the server's evaluated configuration. For more information, see *NetWare Enhanced Security Server*.

Loading Software for Backing Up Workstations

The server evaluated configuration does not include the NLM programs (such as TSADOS or TSAPROXY) necessary to back up client-based TSAs. Consequently, it is not possible to back up clients to a server archive using SMS.

For information on how to perform backups on the client component, see your client manuals.

Loading SMS Software for Backing Up SFT III Servers

The NetWare SFT III^{TM} product is not included in the evaluated configuration. For more information, see *NetWare Enhanced Security Server*.

Understanding Restoring Using SMS

Understanding Restore Issues with NetWare Directory Services

Warning *Supervising the Network* warns against using SBACKUP to restore NDS, unless all replicas have been corrupted. This is because a restored replica will be out of sync with other active replicas of the same data.

Warning Audit trails and configuration data are not backed up by SMS and, consequently, cannot be restored when you restore from media. For information on backing up and restoring audit data, see *Auditing the Network*.

Restoring Data

The server's evaluated configuration does not include the TSAs (TSADOS, TSAPROXY) necessary to support backups and restores of DOS and OS/2 client file systems.

SBACKUP requests a password for the target in order for the TSA to restore the target data.

The TSAs act as a proxy for the administrator that is running SBACKUP. The server makes access decisions based on the identity of the administrator. If you do not have access to all data on the target, you cannot back up that target.

Consequently, *Supervising the Network* recommends logging in to SBACKUP (and thus to the target) as ADMIN or as another user who is security equivalent to ADMIN (who has all rights).

Warning

HCSS is not included in the server's evaluated configuration. For more information, see *NetWare Enhanced Security Server*.

Warning

The server's evaluated configuration does not include the TSAs (TSADOS, TSAPROXY) necessary to support backups and restores of DOS and OS/2 client file systems.

Warning

The TSA400, TSA312, TSA311, and TSA220 NLM programs are not included in the evaluated configuration. Consequently, you cannot back up or restore previous versions of NetWare file systems.

Beginning Procedures for Restoring NDS

Warning

Supervising the Network warns against using SBACKUP to restore NDS, unless all replicas have been corrupted. This is because a restored replica will be out of sync with other active replicas of the same data.

Perform Custom File System Restore

The server's evaluated configuration does not include the TSAs (TSADOS, TSAPROXY) necessary to support backups and restores of DOS and OS/2 client file systems.

Warning

HPFS drives and OS/2 name spaces are not included in the evaluated configuration. For more information, see *NetWare Enhanced Security Server*.

Complete the Restore of the Entire Tree

Refer to your workstation documents to determine if the following utilities are available in your workstation evaluated configuration: PARTMGR, NDS Manager, RIGHTS, NDIR and other client utilities.

Restore File or Directory to File System

The evaluated configuration does not include FTAM, Macintosh*, NFS*, and OS/2* name spaces. For further information about the evaluated configuration, see *NetWare Enhanced Security Server*.

TSAs for earlier server file systems (such as TSA220, TSA311, or TSA400) are not included in the evaluated configuration. Thus, you can only back up NetWare 4.11 file systems in a NetWare Enhanced Security network. For more information, see *NetWare Enhanced Security Server*.

Unloading SMS Files

The NetWare Enhanced Security server configuration does not include WSMAN, TSADOS, or TSAPROXY. For information on the NetWare Enhanced Security NLM programs, see *NetWare Enhanced Security Server*.

Viewing Backup Log or Error Files

Because the evaluated configuration does not support UNIX files and files with extended attributes, it is not possible to view backup log or error files associated with UNIX files. For more information, see *NetWare Enhanced Security Server*.

Managing Storage Media

Warning After you perform a backup, the removable media that you used (such as tape cartridges) will probably contain sensitive user or TCB data. The server cannot protect the data on these removable devices, so you must physically protect the media itself.

Provide at least the same level of physical protection for the media as you provide for the server itself. However, to prevent losing everything in case of fire, flood, or other disasters, you should keep the backup media in a different location than the (physically protected) server room.

Enhancing SBACKUP Performance

TSAs for earlier server file systems (TSA220, TSA311, or TSA400) are not included in the evaluated configuration. Thus, you can only back up NetWare 4.11 file systems in a NetWare Enhanced Security network. For more information, see *NetWare Enhanced Security Server*.

The server evaluated configuration does not include the NLM programs (such as TSADOS or TSAPROXY) necessary to back up client-based TSAs. Consequently, it is not possible to back up clients to a server archive using SMS. For information on how to perform backups on the client component, see your client manuals.

Troubleshooting

Warning You cannot back up data on DOS or OS/2 workstations because the necessary NLM programs are not included in the server's evaluated configuration. These NLM programs include TSADOS, TSASMS, TSAOS2, and TSAPROXY.

chapter 13

Security Supplement to Managing NetWare Licensing Services

NetWare® Enhanced Security information for Chapter 10, “Managing NetWare Licensing Services,” of *Supervising the Network* can be found in the Technical Support area of the Novell, Inc. World Wide Web site (http://www.novell.com).

chapter 14 Security Supplement to Troubleshooting the Network

This chapter contains supplementary NetWare® Enhanced Security facility information for Appendix A, "Troubleshooting the Network," of *Supervising the Network*.

The appendix describes the troubleshooting procedures recommended for resolving network, server hardware, and server software problems.

Troubleshooting Hardware and Network Problems

For information on troubleshooting workstation memory problems, see your client vendor's documentation.

Warning Make sure that the server is not processing actual user data when you are diagnosing server hardware or network problems. Either run the tests while users are not accessing the server, or construct a private test LAN to perform your tests.

Troubleshooting the NetWare Server

Warning Do not run unevaluated disk and network device drivers. For a description of the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

FILER and NetWare Administrator are client utilities. To determine whether these are available in your client NetWare Enhanced Security configuration, see your client documentation.

Troubleshooting Communications Problems

ARCnet* and token ring networks cannot be used with NetWare Enhanced Security servers.

Troubleshooting Workstations

For information on troubleshooting workstations, see your client vendor’s documentation.

chapter 15 Security Supplement to Managing NetWare Server for OS/2

This chapter contains supplementary NetWare® Enhanced Security facility information for Appendix B, "Managing NetWare Server for OS/2," of *Supervising the Network*.

Warning NetWare Server for OS/2* is not included in the server's NetWare Enhanced Security configuration and should be disregarded for purposes of running a NetWare Enhanced Security facility. For a description of the server's NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

chapter 16 Security Supplement to SFT III Management Tips

This chapter contains supplementary NetWare® Enhanced Security facility information for Appendix C, "SFT III Management Tips," of *Supervising the Network*.

Warning

NetWare SFT III™ is not included in the server's NetWare Enhanced Security configuration and should be disregarded for purposes of running a NetWare Enhanced Security facility. For a description of the server's NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

chapter 17 Security Supplement to Creating Menus

This chapter contains supplementary NetWare® Enhanced Security information for Appendix D, “Creating Menus,” of *Supervising the Network*.

Menu administration is not a NetWare Enhanced Security concern for the server component. Menus are created and executed at the client, using the NMENU.BAT utility.

If menus are used for administration of client components, the client documentation must address the use of those menus within the NetWare Enhanced Security configuration.

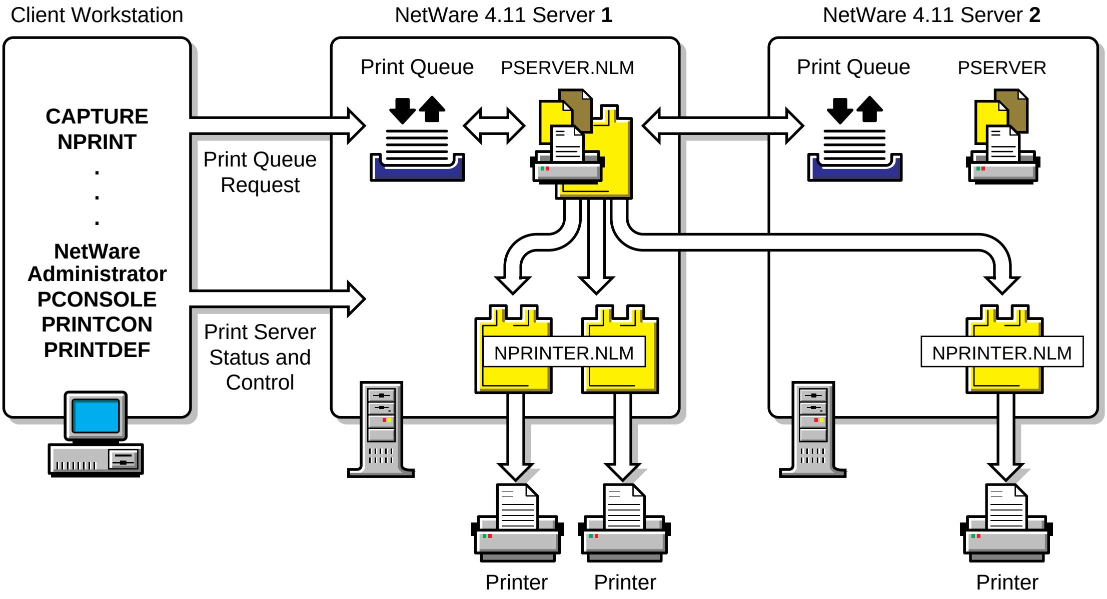
chapter **18**

Security Supplement to Print Services

This chapter contains supplementary NetWare® Enhanced Security information for *Print Services*.

Printing in a NetWare Enhanced Security environment is distributed among clients, NetWare Queue Management Services (QMS) running on each NetWare server, print servers (PSERVER.NLM) running on configured servers, and printer port drivers (NPRINTER.NLM) running on other configured servers.

Figure 18-1
NetWare Enhanced Security Print Architecture



The printing architecture permits, for example, a client program to send a print job to a queue on Server 1, the queue to be serviced by a PSERVER on Server 2, and the print output to be directed through the NPRINTER.NLM on Server 2.

NetWare Enhanced Security printing is NetWare Directory Services™-based. That is, the configurations for queues, print servers, and printers are defined as NDS™ object properties for the corresponding NDS objects that represent the physical resources. NetWare 3.*x* printing is *not* supported in NetWare Enhanced Security environments.

The evaluated server described in this manual does not include workstation-based print servers or port drivers or network print servers or port drivers. Rather it includes only print servers running a NetWare servers (PSERVER.NLM) and port driver running on NetWare servers (NPRINTER.NLM).

The NetWare Enhanced Security distributed print architecture involves the following security mechanisms, which must be configured properly in order to protect print jobs and the network.

Print Server login	PSERVER.NLM may be configured to service print queues on different servers. In order for PSERVER to access a queue on a remote server, PSERVER must first log in to the remote server that holds the queue. Thus, the Print Server NDS object must be configured with a login password and PSERVER must be run with the password in order to log in to the remote server.
IPX address restrictions	When a printer port driver (NPRINTER) attaches to a print server, PSERVER checks the IPX™ network address associated with the connection request and does not permit the connection if the printer's IPX address does not match the list of valid IPX addresses for known printers.

Warning

Print Services describes print configurations for DOS, OS/2*, Windows*, and UNIX® clients. Evaluated versions of these clients may or may not exist for NetWare Enhanced Security. You must use only evaluated client tools to administer the NetWare print system. Such tools may include NetWare Administrator and/or PCONSOLE.

For instructions on which print administration tools are included in the NetWare Enhanced Security configuration, see your client workstation's trusted facility manual.

Introduction to NetWare Print Services

Overview of Network Printing

Figure 1-1 of Print Services shows a print configuration with a printer connected directly to a workstation. This print configuration is outside the scope of NetWare Enhanced Security printing.

As shown in Figure 18-1, NetWare Enhanced Security printing is limited to the following print configurations:

- The only print server used is PSERVER.NLM, which runs on a NetWare Enhanced Security server.

- The only printer driver used is NPRINTER.NLM, which runs on a NetWare Enhanced Security server.

- Printers are physically connected to NetWare Enhanced Security servers.

Refer to your workstation's trusted facility documentation to determine if you are permitted to

- Attach a printer to your workstation

- Use a workstation-based print server (PSERVER.EXE)

- Use a workstation-based port driver (NPRINTER.EXE)

If you intend to use a third-party network-attached printer (with a print server and printer driver), the printer must be evaluated with respect to the network security architecture.

The printing services mentioned in this network printing overview (such as NPRINT and CAPTURE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Using the NetWare Printing Utilities

Note that the client printing utilities (Graphical, Command Line, and Menu) listed in Table 1-1 of *Print Services* may not necessarily be provided by your trusted client workstation.

Warning PUPGRADE.NLM is not included in the server's NetWare Enhanced Security configuration. Only those NLM^TM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

Planning and Setting Up NetWare Print Services

Planning Your NetWare 4 Printing Setup

The administration utilities (such as NetWare Administrator) and client print service utilities mentioned in this paragraph (such as PCONSOLE, PRINTCON, PRINTDEF, CAPTURE, and NPRINT) may not necessarily be provided by your trusted client workstation. To determine how and whether to use these client utilities, see your client documentation.

Warning NetWare Enhanced Security includes only NetWare 4^TM print servers. It does not permit mixed NetWare 3.1 and NetWare 4.1*x* print servers and print configurations.

Warning Because NetWare Enhanced Security does not include NetWare 3^TM servers, the NetSync management utility is not included as part of the server's NetWare Enhanced Security configuration. For a list of NLM programs in the server's NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

NetWare Enhanced Security printing is server-based and does not include workstation- or network-based printers. If you have workstation or network printers, see your trusted facility documentation for instructions for using these types of printers.

Setting Up NetWare Print Services

Note that PCONSOLE or NetWare Administrator may not necessarily be provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Warning The setup procedures describe the use of a workstation-connected printer (“PR_Near”). To determine whether your workstation NetWare Enhanced Security configuration permits network printers connected directly to the workstation, see your workstation documentation. If it does not, then connecting a network printer to the workstation will invalidate the workstation component rating.

Printing Task List

Note that the client utilities (such as NetWare Administrator, PCONSOLE, PSC, PRINTCON, PRINTDEF, CAPTURE, NETUSER, NPRINT, and NPRINTER.EXE) listed in Table 2-1 of *Print Services* may not be provided by your client. To determine how and whether to use these features in the NetWare Enhanced Security configuration, see your client documentation.

Warning PUPGRADE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

Printing from Applications Not Designed for Network Printing

Note that the client printing utilities mentioned (such as NetWare Administrator, PCONSOLE, PRINTCON, PRINTDEF, CAPTURE, NETUSER, and NPRINT) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Additional Information

Note that the client printing utilities mentioned (such as NetWare Administrator, PRINTDEF, and PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Configuring Printing in the NetWare Enhanced Security Environment

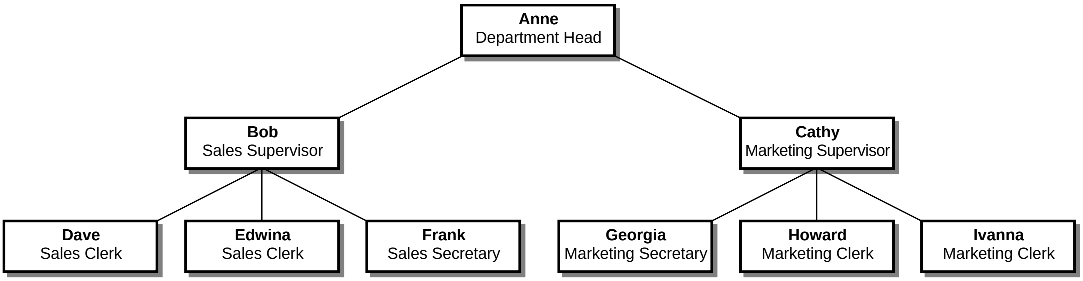
In the NetWare Enhanced Security environment, you must use the NetWare features that allow you to configure your printers and print queues so that only authorized users can generate printouts.

That is, you must set up the list of users of each print queue to include only authorized users, rather than making all print queues accessible to all users. In addition, there are additional requirements imposed when you change the print queue configuration.

This section describes the rules for print queue configuration.

NetWare Enhanced Security Configuration Example

Figure 18-2
Sample Organization

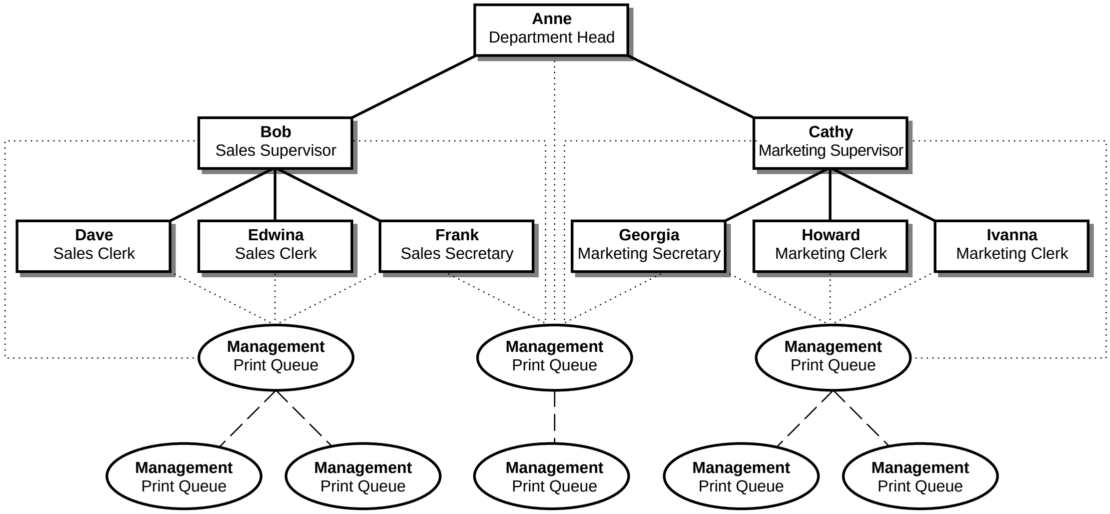


In this organization, there might be several print queues:

- A “Sales” print queue and associated printer(s), used for printing information sensitive to sales
- A “Marketing” print queue and associated printer(s), used for printing information sensitive to marketing
- A “Management” print queue and associated printer(s), used for printing personnel-sensitive information (such as salaries).

Figure 18-3 shows which users can use which print queues and printers. Dotted lines show users who can access print queues, while dashed lines show the relationship of print queues to printers.

Figure 18-3
Printer Configuration for Sample Organization



Each printer would be placed so only the people who should use the print queue that the printer services can gain physical access to the printer. The administrator would also configure the print queues so that only the authorized people can submit jobs to the appropriate print queue. That is:

- Only people working for Bob would be users of the “Sales” print queue and could get physical access to the “Sales” printers.

- Only people working for Cathy would be users of the “Marketing” print queue and could get physical access to the “Marketing” printers.

- Only Alice, Bob, Cathy, Frank, and Georgia would be users of the “Management” print queue and could get physical access to the “Management” printer.

Some users will have access to (and be able to submit jobs to) multiple queues and their corresponding printers. For example, Cathy can submit jobs to the “Marketing” or “Management” print queues, and hence could receive her printouts from the “Management Printer,” “Marketing Printer 1,” or “Marketing Printer 2.”

Security Features User Guide explains that users must select where to spool their output based on what other individuals are users of the print queue and have physical access to the printers.

Warning The abililty to submit a print job to a printing device implies the potential ability to read (by printing to paper) residual data in the printer memory and to modify the printer configuration (by storing print commands in the printer memory) for subsequent print jobs.

Within the NetWare architecture, programmable printers (such as, but not limited to, PostScript*) execute printer programs (print jobs) created by untrusted client software. For example, an authorized user might create a print job for a PostScript printer that saved itself in the printer memory and subsequently reprinted copies of print job submitted by other users.

For this reason, you should restrict the list of authorized users for the printer to those who have a genuine need to use it. Further, when you remove a user from access to the printer, you must reset the printer to its initial configuration. Consult your vendor’s documentation for information on how to reset the printer to a known configuration. For more information, see Step 5 of “Removing Users from Print Queue Access” on page 195.

Warning Although print jobs typically have cover pages, it is entirely up to the workstation application whether there will be banner pages and what the banner pages will say. Therefore, you must not rely on the banner page as a way of determining who a given printout belongs to.

When organizing print queues and printers, you must remember that sending a job to a print queue (and thereby to a printer) is equivalent to giving all authorized users of the print queue the ability to read the information being printed.

Therefore, if you have special information that should only be accessible to some users in the organization, you must set up separate print queues and printers for those users, *in addition to* physically controlling access to the printer.

The following procedures should be performed using utilities in your client’s evaluated configuration. To find those utilities that may be used for print configuration, see your client vendor’s documentation.

Removing Users from Print Queue Access

When you change a print queue configuration to *remove* someone from the list of authorized users, you must use the following procedure (using the PCONSOLE and / or NetWare Administrator utility).

You can use the PCONSOLE and / or NetWare Administrator utility to perform these tasks.

- For more information on using NetWare Administrator, see “Print Queue Options” in Chapter 3 of *Print Services.*

- For more information on using PCONSOLE, see Chapter 4, “Managing Print Services Using PCONSOLE,” in *Print Services*.

Procedure

1. **Stop the print server(s) that process jobs from the print queue from processing already queued jobs.**

   To do so, set the “Allow Service by Current Print Servers” flag to “No” (see “Assigning Queue Operator Flags” in *Print Services*).

2. **Stop the print queue from accepting any new jobs.**

   To do so, set the “Allow Users to Submit Print Jobs” flag to “No” (see “Assigning Queue Operator Flags” in *Print Services*).

3. **Wait for each printer serviced by the print queue to stop printing.**

4. **Review the list of print jobs in the print queue, and remove any that belong to the individual(s) being removed from the list of authorized users.**

   For instructions on using NetWare Administrator to view and modify the list of queued print jobs (by selecting a print job and pressing <Delete>), see “Viewing Details of Print Jobs” in *Print Services.*

If you are using PCONSOLE, complete the following steps:

4a. Select “Print Queues” from the main menu.

4b. Select the print queue that you want to delete the print job from.

4c. Select “Print Jobs.”

4d. To delete a queue entry, press <Delete>**.**

5. Reset the printer to its initial configuration.

Refer to vendor documentation for the printer to determine how to reset the printer. In some cases, power cycling the printer will suffice to clear any residual data that may be left by previous users.

However, for printers that provide nonvolatile storage (such as battery-backed memory or disk drives) you must follow the vendor’s procedures to ensure removal of any residual data from previous print jobs.

6. Remove the user from the list of authorized users of the print queue.

For instructions on using NetWare Administrator to remove users or other NDS objects as queue users, see “Viewing or Changing the List of Users for a Print Queue” in *Print Services*.

If you are using PCONSOLE, complete the following steps:

6a. Select “Print Queues” from the main menu.

6b. Select the print queue that you want to delete the object from.

6c. Select “Users.”

6d. Select the user (or other NDS object) to be deleted.

6e. Press <Delete>**.**

7. Allow print server(s) that process jobs from the print queue to resume processing queued jobs.

To do so, set the “Allow Service by Current Print Servers” flag to “Yes” (see “Assigning Queue Operator Flags” in *Print Services*).

8. **Allow the print queue to resume accepting print jobs.**

   To do so, set the “Allow Users to Submit Print Jobs” flag to “Yes” (see “Assigning Queue Operator Flags” in *Print Services*).

Note that these steps apply even if you indirectly change the list of authorized users. For example, if you have a NetWare group that is identified as users of a print queue and someone is removed from the group, you must follow the same steps.

Similarly, if an NDS container is identified as users of a print queue, then removing a user from the container requires following the above steps.

In the organization described above, if Howard leaves Cathy’s group, then you must follow these steps for the “Marketing” print queue (and printers).

These steps must be followed whether Howard is explicitly listed as a user of the print queue or is a member of a group (or other NDS object) that is listed as a user of the print queue.

Adding Users to Print Queue Access

Procedure

To change a print queue configuration by adding someone to the list of authorized users, use the following steps:

1. **Inform all other authorized users of the additional individual(s) now authorized to use their print queue and printer(s).**

2. **Add the individual(s) to the list of authorized users of the print queue using either PCONSOLE or NetWare Administrator.**

In the organization described above, if Howard joins Bob’s group, then you must follow these steps for the “Sales” print queue (and printers). Note that you do *not* need to reset the “Sales” print queue (and printers) when you add Howard as an authorized user.

These steps must be followed whether Howard is explicitly added as a user of the print queue is added to a group that is listed as a user of the print queue.

If a container is listed as an authorized user of a print queue, then creating a new NDS user object in that container (or any subcontainer) requires following the above steps, since the new user would be implicitly authorized to use the print queue.

Using NetWare Administrator

Chapter 3 in *Print Services* provides instructions on how to use NetWare Administrator to add a user to a print queue:

For instructions on adding users or other NDS objects as queue users, see “Viewing or Changing the List of Users for a Print Queue” in *Print Services*. (See also Step 6 under “Removing Users from Print Queue Access” on page 195).

Using PCONSOLE

Procedure

To use PCONSOLE to change the list of users of a queue:

1. **Select “Print Queues” from the main menu.**

2. **Select “Users” from the print queue of interest.**

3. **Insert a user (or other NDS object) by pressing** <Insert>**.**

4. **Select the desired user by using the NDS browser.**

Managing Print Services with the NetWare Administrator Utility (Client)

Note that the NetWare Administrator utility may not necessarily be available on your trusted client workstation. To determine whether to use this utility, see your client documentation.

Chapter 3, “Managing Print Services with the NetWare Administrator Utility,” of *Print Services* refers in numerous places to the PCONSOLE utility as an alternate means of managing the print configuration. For information about the PCONSOLE utility, see “Managing Print Services Using PCONSOLE (Client)” on page 206.

Overview

No additional security information.

Requirements

No additional security information.

Printing Tasks Handled through NetWare Administrator

No additional security information.

Using the Browser

No additional security information.

Using the Printing Object Dialogs

No additional security information.

Setting Up Print Services with NetWare Administrator

Warning

To determine whether your trusted workstation permits network printers connected directly to workstations, see your workstation trusted facility manual. If it does not, then connecting a network printer to the workstation will invalidate the workstation component rating.

Further, the configuration of the server to permit an unauthorized printer to access print queues invalidates the server component security rating.

Creating Print Queues

No additional security information.

Creating Printers

Warning

You must specify the printer's "Network Address Restriction" property when you create a new printer object in the NetWare Enhanced Security configuration.

The "Network Address Restriction" property must be identical to the IPX network and node addresses of the NTCB partition (normally a server) where the NPRINTER port driver runs. Do not specify a wildcard network address ("FFFFFFFF") or node address ("FFFFFFFFFFFF").

If you do not specify the network address for every printer, then a user may be able to spoof a legitimate printer (for example, by running NPRINTER.EXE on an untrusted workstation session) and thus gain access to print jobs directed to that printer.

Step 4 under "Creating Printers" in *Print Services* indicates that you may optionally define additional properties for the printer. However, because you must specify the address restriction for the printer, replace Steps 4 and 5 of the *Print Services* "Creating Printers" procedure with the following.

Procedure

1. **Mark the “Define Additional Properties” box.**

   This allows you to define additional information about this printer immediately after you create it. One of these properties is the printer’s “Network Address Restriction” property. You must set this property immediately after creating the object.

2. **Select “Create.”**

   The object dialog for Printer P1 appears, similar to that shown in Figure 3-7 of *Print Services*.

3. **Define the printer’s “Network Address Restriction” property.**

   From the printer “Identification” Page, select the “Configuration” menu, then select “Set” for the “Network Address Restriction” property. (Do *not* confuse the “Network Address Restriction” property with the “Network Address” field in the “Identification” menu.)

   When the IPX/SPX^{TM} menu appears, enter the four-byte network number and the six-byte node address for the machine where the printer is connected. After you specify the address restriction, select “OK” to save the “Network Address Restriction” property.

4. **(Optional) Define any additional properties for the printer.**

   When you finish, choose “OK” to save the network configuration.

Assigning Print Queues to Printers

No additional security information.

Creating Print Servers

When you create a new Print Server object, you must specify a password for the Print Server to log in to NDS. You must specify this password even if the print server will never log in to a remote server.

If you do not set a password for the print server object, a user on the network could log in to the network as the print server and spoof PSERVER’s actions.

In addition to the “Creating Print Servers” procedure in *Print Services*, you must perform the following steps when you create a print server.

Procedure

Procedure

1. **Set the print server's password.**

   From the print server "Identification" Page, select the "Identification" menu and choose "Change Password." Enter the new password, reenter the new password, and choose "OK" to save the password as a print server object property.

   Warning

   The server does not enforce any password strength mechanisms for print server passwords. Consequently, you can set a password as short as one character, you can reuse passwords, and you can set a password the same as the name of the Print Server object.

   It is your responsibility, as network supervisor, to set a sufficiently strong password for the print server and to protect that password from unauthorized users. You should select a password that is at least eight characters long.

2. **Define operators for the print server.**

   Select the "Operator" menu, then choose "Add" to bring up a browser. Select the desired operators, then choose "OK" to save the configuration. Operators must be trusted individuals, such as administrators, that are permitted to manipulate print jobs for multiple users.

3. **Define users for the print server.**

   Follow the same procedures as in Step 2 to define users for the print server. A user is permitted to manipulate his or her own jobs, but is not allowed to affect other users' jobs. Multiple users may be specified by selecting a security equivalent group.

4. **(Optional) Define any additional properties for the print server.**

   When you finish, press "OK" to save the network configuration.

The print server audit log is not an audit trail in the NetWare Enhanced Security sense. The feature can be used at a network facility to provide additional information about the utilization of print servers and printers, but does not help satisfy NetWare Enhanced Security auditing requirements. For more information, see *Auditing the Network.*

Assigning Printers to Print Servers

No additional security information.

Assigning Printing Objects

No additional security information.

Modifying NetWare Print Services

No additional security information.

Print Queue Options

Assigning Queue Operator Flags

No additional security information.

Viewing or Modifying Print Jobs

No additional security information.

Viewing Details of Print Jobs

No additional security information.

Viewing or Changing the List of Users for a Print Queue

You can have both network supervisors and ordinary users on the list.

Viewing or Changing the List of Operators for a Print Queue

Warning

Assign only trusted users (such as network supervisors) to the operators list. If you add general (nonadministrative) users to this list of operators, those users will be able to modify the processing of other users’ print jobs.

Printer Options

As described in “Creating Printers” on page 200, if you want to operate in accordance with the NetWare Enhanced Security configuration, you must ensure that each network printer is defined with a “Network Address Restriction” property that defines the printer’s IPX network address.

Warning You must use the full network and node address of the printer for authentication, without any wildcards (for example, “FFFFFFFF”).

Do not confuse the “Network Address Restriction” peroperty (“Configuration” menu) with the network address shown in the “Identification” menu. The network address is provided for information only, and is not used by the print server to control access by printers.

Print Server Options

Viewing Your Printing Layout and Status

No additional security information.

Enabling and Viewing the Print Server Auditing Log

The print server audit log is not an audit trail in the NetWare Enhanced Security sense. The feature can be used at a network facility to provide additional information about the utilization of print servers and printers, but does not help satisfy NetWare Enhanced Security auditing requirements.

Adding, Changing, and Removing Print Server Passwords

Warning

As described in “Creating Print Servers” on page 201, you must set a password for each print server in order to prevent users from spoofing the print server. If a password is not specified for the print server, it can log in to other servers without a password; but this would also permit any user on the network to log in to a server as a purported print server, and to perform print server functions after logging in.

Further, the server does not enforce any password strength mechanisms, so you must ensure that the password is sufficiently strong that users cannot guess the password. You should select a password that is at least eight characters long. Finally, you must physically protect the password (for example, don’t write it down next to your workstation) from access by unauthorized users.

Warning

Do not remove a print server’s password.

When you define a password for the print server, the print server will interactively prompt for the password at the server console when the print server attempts to log in to a server. If you do not have procedures for typing in the password when the server boots, the operation of the print system will be disrupted.

Unloading Print Servers

No additional security information.

Working with Print Job Configurations

Note that the printing services mentioned (CAPTURE, NPRINT, NETUSER, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Working with Printer Forms

Note that the printing services mentioned (PRINTDEF, NetWare Administrator, PSC, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Warning

Banner pages can be suppressed or modified by users. Do not rely on the contents of a banner page to indicate who owns or should have access to the data in a printout.

Working with Print Device Definitions

No additional security information.

Working with Print Device Modes

No additional security information.

Referencing Bindery Queues

Bindery queues are *not* supported in NetWare Enhanced Security systems.

Managing Print Services Using PCONSOLE (Client)

Note that the PCONSOLE utility may not necessarily be available on your trusted client workstation. To determine whether to use this client utility, see your client documentation.

Chapter 4, "Managing Print Services Using PCONSOLE," of *Print Services* refers in numerous places to the graphical NetWare Administrator utility as an alternate means of managing the print configuration. For more information about NetWare Administrator, see "Managing Print Services with the NetWare Administrator Utility (Client)" on page 199.

Overview

No additional security information.

New PCONSOLE Features for NetWare 4

Print Services explains that PCONSOLE can be used to configure Macintosh* and UNIX printers. These printers are not included in the server's NetWare Enhanced Security configuration. To determine if such printers are included in the client evaluated configuration, see the client's vendor documentation.

Printing Tasks Handled through PCONSOLE

No additional security information.

Modifying NetWare Print Services

Creating or Modifying Print Queues

This section describes how to use PCONSOLE to create or modify a print queue. For information on setting the operator list and user list for the queue, see “Setting Queue Operators and Users” on page 208.

Note that the printing services mentioned (CAPTURE, NPRINT) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Creating or Modifying Printers

This section describes how to use PCONSOLE to create or modify NetWare Enhanced Security printers. For information on setting the printer’s “Network Address Restriction” property, see “Printer Options” on page 204.

Creating or Modifying Print Servers

This section describes how to use PCONSOLE to create or modify print servers. For information on setting the print server’s login password, see “Adding, Changing, and Removing Print Server Passwords” on page 205.

Print Queue Options

Assigning Queue Operator Flags

No additional security information.

Creating or Manipulating Print Jobs

Note that the printing services mentioned (NPRINT, CAPTURE, NETUSER) may not necessarily be those provided by your client. to determine how and whether to use these client utilities, see your client documentation.

Setting Print Job Parameters

To change or set print job parameters, select “Print Queues” from the “Available Options” menu, select the print queue, then select “Print Jobs” from the “Print Queue Information” menu. You can only set print job parameters for jobs that are in the queue. Select the print job, and PCONSOLE will display the print job parameters listed in Table 4-2 of *Print Services*.

Warning

Banner pages can be suppressed or modified by users. Do not rely on the contents of a banner page to indicate who owns or should have access to the data in the printout.

Note that the printing services mentioned (CAPTURE, NPRINT, PRINTDEF) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Setting Queue Operators and Users

Warning

Access to a print queue is controlled by entries in a queue user list and a queue operator list. Each list contains object names (users, groups, etc.) that are permitted to access the queue. Users listed in the queue user list can submit jobs and perform operations on their own print jobs. You can assign any user, group or other object as a queue user.

Operators can perform operations on any jobs in the queue, even those that belong to other users. Consequently, you should assign only trusted individuals (such as administrators) on the operator list. If you add general (nonadministrative) users to the operator list, those users will be able to affect the processing of other users’ print jobs.

To set the list of users for a queue, select “Users” from the “Print Queue Information” menu. Press <Insert> to bring up an NDS browser that will allow you to select users or groups to be added as queue users.

To set the list of operators for a queue, select "Operators" from the "Print Queue Information" menu. Press <Insert> to bring up an NDS browser that will allow you to select users or groups to be added as queue operators.

Printer Options

Warning

You must specify the printer's "Network Address Restriction" property when you create a new printer object in the NetWare Enhanced Security configuration. The "Network Address Restriction" property must be identical to the IPX network and node addresses of the NTCB partition (normally, a server) where the NPRINTER port driver runs. Do not specify a wildcard network address ("FFFFFFFF") or node address ("FFFFFFFFFFFF").

If you do not specify the network address for every printer, then a user may be able to spoof a legitimate printer (for example, by running NPRINTER.EXE on an untrusted workstation session) and thus gain access to print jobs directed to that printer.

Table 4-3 of *Print Services* shows the printer configuration parameters that you can configure using PCONSOLE. To set a printer's "Network Address Restriction" property, perform the following steps.

Procedure

Procedure

1. **Select "Printers" from the "Available Options" menu.**

2. **Select the specific printer from the printers list.**

3. **Select "Configuration" from the "Printer Configuration" menu.**

4. **Select "Address Restriction" from the "Parallel Printer Specifics" menu. (A similar menu exists for serial printers.)**

5. **Select "Yes" for "Restrict Address of Remote Printer."**

6. **Enter the specific network number and node address of the machine where the printer is connected.**

Configuring Printers

Note that the printing services mentioned (PRINTDEF, PSC, NetWare Administrator) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Viewing or Modifying a Printer's Status

No additional security information.

Changing Printer Type

No additional security information.

Assigning Multiple Print Queues and Printers

No additional security information.

Mounting Printer Forms

No additional security information.

Print Server Options

No additional security information.

Viewing a Print Server's Status

No additional security information.

Changing a Print Queue's Priority

No additional security information.

Designating a New Default Print Queue

No additional security information.

Adding, Changing, and Removing Print Server Passwords

Warning: When you create a new Print Server object, you must specify a password for the print server to log in to NDS. You must specify this password even if the print server will never log in to a remote server. If you do not set a password for the print server, a user on the network could log in to the network as the print server and spoof PSERVER's actions.

Warning: The server does not enforce any password strength mechanisms for print server passwords. Consequently, you can set a password as short as one character, you can reuse passwords, and you can set a password the same as the name of the Print Server object.

It is your responsibility, as administrator, to set a sufficiently strong password for the Print Server object and to protect that password from unauthorized users.

Enabling and Viewing the Print Server Auditing Log

Warning: The print server audit log is an accounting feature and not an audit trail in the NetWare Enhanced Security sense. The feature can be used at a network facility to provide additional information about the utilization of print servers and printers, but does not help satisfy NetWare Enhanced Security auditing requirements.

Unloading Print Servers

No additional security information.

Using PCONSOLE in Bindery Mode

Warning: NetWare Enhanced Security includes only NetWare 4 print servers. It does not permit mixed NetWare 3.1*x* and NetWare 4.1 print servers and print configurations. Do not run NetWare 3.1*x* programs in your configuration, or you will invalidate your network's C2 rating.

Additional Information

No additional security information.

Sending Jobs to Network Printers Using CAPTURE and NPRINT (Client)

Note that the CAPTURE and NPRINT utilities may not necessarily be provided by your client. To determine how and whether to use these client utilities, see your workstation documentation.

Warning

Print Services explains that if you specify a NetWare server that you are not attached to in your CAPTURE command, CAPTURE attaches you as user GUEST unless the GUEST account requires a password.

More precisely, CAPTURE will attach you as user GUEST if the GUEST account exists on the server and does not have a password. If the GUEST account does not exist, or the GUEST account exists but has a password, CAPTURE will prompt for a username and password in order to log the user in to the server using a bindery (NetWare 3.*x*)-style login.

NetWare Enhanced Security servers are not distributed with a GUEST account. Consequently, if you direct your CAPTURE output to a server where you are not logged in, CAPTURE will prompt you for your login name and password. To determine whether the CAPTURE utility is trusted to properly handle your administrative authentication materials, see your workstation's client documentation.

Note that the printing services mentioned (PRINTDEF, NetWare Administrator, PCONSOLE, PRINTCON) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Setting Up and Servicing Print Servers

Overview

Warning

Third-party printers should be connected to the network only if they have been evaluated. Attaching unevaluated print devices to the network will invalidate the network's C2 rating.

Note that NPRINTER.EXE may not necessarily be provided by your client. To determine how and whether to use this client utility, see your client documentation.

New Print Server Features for NetWare 4

For information on the specific printers that are available for use with NetWare Enhanced Security servers, see *NetWare Enhanced Security Server*.

Warning The print server provides a mechanism for checking that each printer that attaches to the print server is connecting from the IPX address specified in the printer object's "Network Address Restriction" property.

As described in "Print Server Options" on page 204, you must define the printer's address restriction when you add a new printer. If you do not define the address restriction for every printer, then the Print Server will allow remote printers to connect from any address.

Warning The print server audit log is not an audit trail in the NetWare Enhanced Security sense. The feature can be used at a network facility to provide additional information about the utilization of print servers and printers, but does not help satisfy NetWare Enhanced Security auditing requirements.

Requirements

Note that the printing services mentioned (NetWare Administrator, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Using PSERVER.NLM

"Adding, Changing, and Removing Print Server Passwords" on page 211 explains that NDS Print Server objects must be created with a password to prevent untrusted users from spoofing a print server by logging in to a server using the null password.

Consequently, when you load PSERVER (either by explicitly typing "LOAD PSERVER" at the system console or by a LOAD command in a configuration file), PSERVER will prompt for its password before it logs in to a server to access its queues. It prompts for a login password even if the queue is on the same server.

Note that the printing services mentioned (NetWare Administrator, PCONSOLE, PSC, PRINTDEF) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Servicing NetWare 4 Clients and Queues with a NetWare 3 Print Server

Warning NetWare 3 print servers are not included in the server's NetWare Enhanced Security configuration. As described in *NetWare Enhanced Security Server*, NetWare Enhanced Security only permits the use of NetWare Enhanced Security NetWare 4 print NLM programs. Use of unevaluated NLM programs on the server violates the assumptions under which the server was evaluated.

Servicing NetWare 3 Clients and Queues with a NetWare 4 Print Server

Warning NetWare 3 queues are not supported by the server's NetWare Enhanced Security configuration.

Warning NetWare 3 clients are permitted only if the client is evaluated with respect to the NetWare Enhanced Security network architecture.

Using Third-Party Network-Direct Print Devices with NetWare 4

Warning Third-party print devices may be used in the NetWare Enhanced Security configuration only if they are themselves evaluated with respect to NetWare Enhanced Security architecture.

Note that PCONSOLE may not necessarily be provided by your client. To determine how and whether to use this client utility, see your client documentation.

Setting Up Printing on a Network Using SFT III

Warning NetWare SFT III^{TM} is not included in the server's NetWare Enhanced Security configuration. For a list of the NLM programs that are included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*. Use of unevaluated software on the server invalidates the server's C2 evaluation.

Troubleshooting Print Server Problems

Note that the printing services mentioned (NetWare Administrator, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Setting Up Printers Attached to Workstations or Servers

Before setting up printers attached to workstations, check the client documentation to determine whether network printers are included in the client evaluated configuration.

Overview

Note that the printing services mentioned (NPRINTER.EXE, NPTWIN95.EXE, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

New NPRINTER Features for NetWare 4

No additional security information.

Requirements

Note that the printing services mentioned (NetWare Administrator, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Using NPRINTER.EXE

Note that NPRINTER.EXE may not necessarily be provided by your client. To determine how and whether to use this client utility, see your client documentation.

Note that the printing services mentioned (NetWare Administrator, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Using NPRINTER (Windows 95)

The NPRINTER Manager (NPTWIN95.EXE) is a client workstation utility. To determine how and whether to use this client utility, see your client documentation.

Warning NPTR95.NLM and NPTDRV95.NLM are not included in the server's NetWare Enhanced Security configuration. You cannot run these NLM programs s on the server without violating the basis of trust in the server. For more information on the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Setting Up Network Printing on a Windows 95 Workstation

No additional security information.

Using NPRINTER.NLM

Note that NPRINTER.EXE may not necessarily be provided by your client. To determine how and whether to use this client utility, see your client documentation.

Using NetWare-Attached Printers

No additional security information.

Troubleshooting Tips for Administering Printer Stations

Note that the printing services mentioned (NPRINTER.EXE, NetWare Administrator, PCONSOLE, CAPTURE, PSC) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

If your printer cannot connect to a print server, it may be because the printer's "Network Address Restriction" value is incorrect. Use NetWare Administrator, PCONSOLE, or another trusted program on your client to review the "Network Address Restriction" property for your printer's NDS object.

Creating and Managing Print Job Configurations

The printing services mentioned (NPRINT, NetWare Administrator, PCONSOLE, CAPTURE, NETUSER, PRINTCON, PRINTDEF) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Warning Banner pages can be suppressed or modified by users. Do not rely on the contents of a banner page to indicate who owns or should have access to the data in the printout.

Working With Print Device Definitions and Printer Forms

The printing services mentioned (NetWare Administrator, PCONSOLE, PSCS, PRINTDEF) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Using NETUSER, PSC, and PUPGRADE

Using NETUSER

NETUSER may not necessarily be provided by your client. To determine how and whether to use this client utility, see your client documentation.

Using PSC

PSC may not necessarily be provided by your client. To determine how and whether to use this client utility, see your client documentation.

Using PUPGRADE.NLM

Warning PUPGRADE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

Setting Up and Servicing Printers

Warning For information on how to select NetWare Enhanced Security printers, see *NetWare Enhanced Security Server*.

Cabling Printers

There are no additional warnings for this chapter.

Optimizing Network Printing Performance

Parallel Versus Serial Ports

Note that NPRINTER.EXE may not necessarily be provided by your client. To determine how and whether to use this client utility, see your client documentation.

Software Version

Warning When downloading software, be sure that the software being updated is part of the TCB and that the version being downloaded has been evaluated. Installing unevaluated patches in an NetWare Enhanced Security system will result in the resulting system not meeting NetWare Enhanced Security requirements.

Printer Configuration

Note that the printing services mentioned (NPRINTER, PCONSOLE, NetWare Administrator) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Network-Direct Print Devices

Note that the printing services mentioned (NetWare Administrator, NPRINTER, PCONSOLE) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Computer Type

Note that the printing services mentioned (NPRINTER, PCONSOLE, NetWare Administrator) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

Troubleshooting Printing Problems

Note that the printing services mentioned (NPRINTER.EXE, PCONSOLE, NetWare Administrator, PRINTCON NPRINT, FILER) may not necessarily be those provided by your client. To determine how and whether to use these client utilities, see your client documentation.

chapter 19 Security Supplement to Concepts

This chapter contains additional NetWare® Enhanced Security facility information supplementing *Concepts*.

The titles in this chapter match those in *Concepts*; for those concepts not listed in this chapter, there is no additional information necessary for the NetWare Enhanced Security configuration.

A

Address Resolution Protocol

Warning ARP is part of both the TCP/IP and AppleTalk* protocol suites. Neither TCP/IP nor AppleTalk are included in the NetWare Enhanced Security configuration.

AFP

Warning AFP is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

AFP Server Object

There are no restrictions on creating AFP Server objects in the NetWare Enhanced Security configuration; however, the server NetWare Enhanced Security configuration does not include any AFP software to support that object.

AppleShare software

To determine whether AppleShare software is included in your client's NetWare Enhanced Security configuration, see your client documentation.

AppleTalk Filing Protocol

Warning

AppleTalk Filing Protocol is not part of the Server NetWare Enhanced Security configuration; do not load it.

AppleTalk Phase 2

Warning

AppleTalk Phase 2 protocols are not part of the NetWare Enhanced Security configuration.

AppleTalk Print Services Module

Warning

The AppleTalk Print Services NLM^{TM} program is not part of the NetWare Enhanced Security configuration. For a list of NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

AppleTalk Protocols

Warning

AppleTalk Protocols are not part of the NetWare Enhanced Security configuration.

ARP

Warning

ARP is part of both the TCP/IP and AppleTalk protocol suites. Neither TCP/IP nor AppleTalk is included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

ATPS

Warning The AppleTalk Print Services NLM program is not part of the NetWare Enhanced Security configuration. For a list of the NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Attributes

Warning File and directory attributes supplement the NetWare file system access control policy. Such attributes are not enforced by the server. They are advisory information to the client component, and may or many not be enforced by the client.

Do not rely on file or directory attributes for protection of sensitive information. Rather, you should use file rights. For example, rather than using the Delete Inhibit (Di) file attribute, you should remove the Delete right from any user who should not be able to delete the file.

Warning The Execute Only (X) attribute is advisory only. It may be implemented by clients. Do not rely on this attribute to prevent reading of files.

Warning The Copy Inhibit (Ci) attribute is advisory only. It may be implemented by clients. Do not rely on this attribute to prevent copying of files.

Audit File object

For information on configuring Audit File objects, see *Auditing the Network*.

Auditing

For information about auditing a NetWare Enhanced Security server, see *Auditing the Network*.

AUTOEXEC.BAT

AUTOEXEC.BAT is a client feature. To determine whether this feature is present, see your client documentation.

AUTOEXEC.NCF

Warning TCP/IP and AppleTalk NLM programs are not included in the server's NetWare Enhanced Security configuration. Therefore, they should not be invoked in your AUTOEXEC.NCF file. For additional commands that must be placed in your AUTOEXEC.NCF file in the NetWare Enhanced Security configuration, see Chapter 3, "Security Supplement to Installation," on page 69.

B

Backup hosts and targets

To determine whether your client supports any client targets, see your client documentation.

Bindery context path

Warning The server's NetWare Enhanced Security configuration does not include NetWare 3TM NLM programs; therefore, they should not be loaded. For a list of NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Bindery object

Warning Upgrade utilities from versions of NetWare that support the bindery are not included in the server's NetWare Enhanced Security configuration. Therefore, these objects should not occur.

Bindery Queue object

Warning Upgrade utilities from versions of NetWare that support the bindery are not included in the server's NetWare Enhanced Security configuration. Therefore, these objects should not occur.

Binding and unbinding

Warning The INETCFG program is not included in the server's NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

BOOTP

Warning BOOTP is part of the TCP/IP protocol suite, and BOOTPFWD.NLM is not included in the server's NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Btrieve

Warning Server-based Btrieve* is not included in the NetWare Enhanced Security configuration. For a list of software included in the server's NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*. To determine whether client-based Btrieve is supported, see your client documentation.

C

Child VLM

Child VLM™ programs are a client facility. To determine whether they are supported, see your client documentation.

Communication protocols

Warning The INETCFG program is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Computer object

Computer objects are not used to make access control decisions. They are for informational purposes only.

Configuration (router)

Warning The INETCFG and FILTCFG programs are not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Warning The TCP/IP and AppleTalk protocol suites are not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Configuration (server)

Warning The TCP/IP and AppleTalk protocols are not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Warning Before installing additional NetWare products, see *NetWare Enhanced Security Server* for a list of software included in the NetWare Enhanced Security configuration.

Container login script

The execution of login scripts is a client function. To determine how container login scripts are processed, see your client documentation.

Copy Inhibit (Ci) attribute

Warning The Copy Inhibit (Ci) attribute is an advisory indicator that may or may not be used by network clients. Do not rely on this attribute to prevent copying of files. To determine whether this attribute is supported by your workstation, see your client documentation.

D

Data migration

Warning Data migration is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

DCDB

Warning DCDB is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Delete Inhibit (Di) attribute

Warning The Delete Inhibit (Di) attribute is an advisory indicator that may or may not be used by network clients. Do not rely on this attribute to prevent copying of files. To determine whether this attribute is supported by your workstation, see your client documentation.

Disk space restrictions

Disk space restrictions may be set with the FILER client utility. If you are using the NetWare Enhanced Security configuration, see your client documentation to determine whether this utility is available.

Placing a directory disk space restriction on \A\B will limit the cumulative disk space used by files in \A\B, \A\B\C, and \A\B\C\D. To assign directory disk space restrictions, the supervisor must have the Supervisor right to the directory. Any user with the Scan rights to a directory may query the restrictions for that directory.

See also “Owner”; “Rights.”

Related utility: “FILER” in *Utilities Reference*.

Distribution List object

Electronic mail (which is the intended use of Distribution List objects) is not part of the NetWare Enhanced Security configuration. There are no restrictions on creating Distribution List objects in the NetWare Enhanced Security configuration.

Drive mapping

Drive mapping is a client feature. To determine whether this feature is supported, see your client documentation.

Dual processing

Warning NetWare SFT III^{TM} is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

E

Effective rights

Warning Group membership does not play a role in computing effective rights. Rather, only security equivalence is used in determining effective rights.

NetWare administrative utilities (NETADMIN, NetWare Administrator) ensure that users are security equivalent to all groups of which they are members, but the calculation is based solely on security equivalence, and not on group membership.

In addition to the sources for rights listed, MWILKENS could gain additional rights from:

- Trustee assignments to the root object that list MWILKENS, SALES PV, [Public], or [Root] (rights are inherited from the object's container).

  Rights must pass through MANAGER's Inherited Rights Filter before becoming effective.

- Trustee assignments to SALES LA that list [Public] or [Root] (rights are inherited from the object's container).

  Rights must pass through MANAGER's Inherited Rights Filter before becoming effective.

- Trustee assignments to MANAGERS that list [Public] or [Root] (rights are explicitly granted).

Warning In computing effective rights, NetWare computes the rights available to each object to which the user is security equivalent (namely, MWILKENS, SALES PV, [Root], [Public]) and unions them together. That is, if SALES PV has certain rights to MANAGERS, and [Public] has some rights to MANAGERS, then MWILKENS's rights to MANAGERS will be the combination of the rights allowed to SALES PV and [Public].

The following descriptions give detailed explanations of how effective rights are calculated for NDS™ objects, NDS object properties, and NetWare files and directories. In addition, they provide examples showing how trustee assignments, inheritance, and Inherited Rights Filters combine to yield a powerful access control facility.

NDS Rights

For a given subject, represented by an NDS object S, the algorithm for calculating the object rights available to an NDS object O may be summarized as follows:

1. Build a list of all NDS objects to which S is security equivalent. If S is unauthenticated, this list consists only of [Public]. If S is authenticated, this includes:
    - The object S
    - [Public], to which all users are security equivalent
    - [Root], to which all users are security equivalent
    - All NDS objects on the path from the root of the NetWare Directory tree to S
    - All NDS objects to which S has explicitly been given security equivalence
2. For each NDS object in the list, create an empty list of NDS object rights.
3. Starting at the root of the NetWare Directory tree, and moving towards O, perform the following steps for each node N:
    a. If N has an object Inherited Rights Filter (IRF), go through each element of the list created in Step 1 and delete all object rights except those listed as being allowed.

    b. For each trustee in N’s trustee list which is also found in the list from Step 1, replace the rights for the entry with the object rights given in N’s trustee list.
4. Take all object rights from the list and bit-wise OR them together (that is, calculate the union of rights granted to S and all objects to which S is security equivalent).

5. If the union includes the Supervisor object right, then grant all object rights.

6. The result is S’s NDS object rights to O.

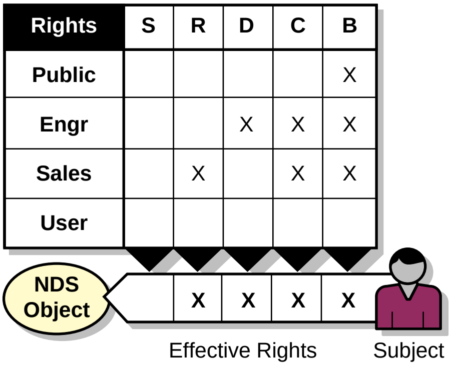
Note that the names of all NDS objects are public. Regardless of the rights settings (including IRFs), any user can present the name of an NDS object and will be told whether or not the object exists.

However, the ability to query what NDS objects exist is controlled by the Browse right. Therefore, you should not give NDS objects sensitive names.

Figure 19-1 provides an example of the calculation of effective rights. In the example, the letters S, R, D, C, and B correspond to the NDS object rights Scan, Rename, Delete, Create, and Browse.

The user’s subject attempts to access an NDS object. The user is assumed to be security equivalent to “Engr” and “Sales”. Thus, the subject’s effective rights to the NDS object are *R*ename, *D*elete, *C*reate and *B*rowse.

Figure 19-1
Calculating Effective Rights



Rights	S	R	D	C	B
Public					X
Engr			X	X	X
Sales		X		X	X
User					

Figure 19-2 shows an example of the computation of effective rights to a leaf object given the existence of an IRF (sometimes called an inheritance mask) on the container object.

In the example, the user's effective rights to the container object include the Rename, Delete, Create and Browse object rights. The IRF permits only the Browse object right to be inherited. Thus, the user's effective object rights for the leaf object is Browse.

The example assumes that there are no object rights explicitly assigned for the leaf object (that is, the leaf object does not have an ACL, but instead it inherits all access information from its container).

Figure 19-2
Calculating Effective Rights with an IRF

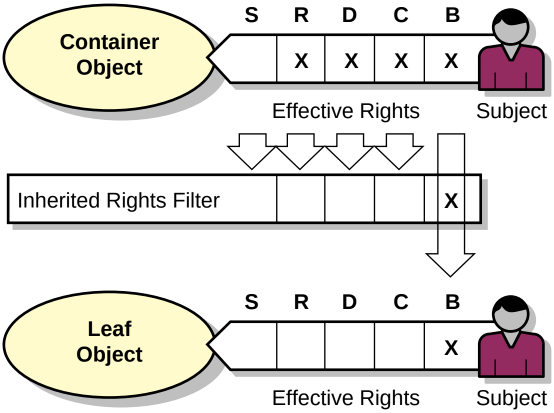
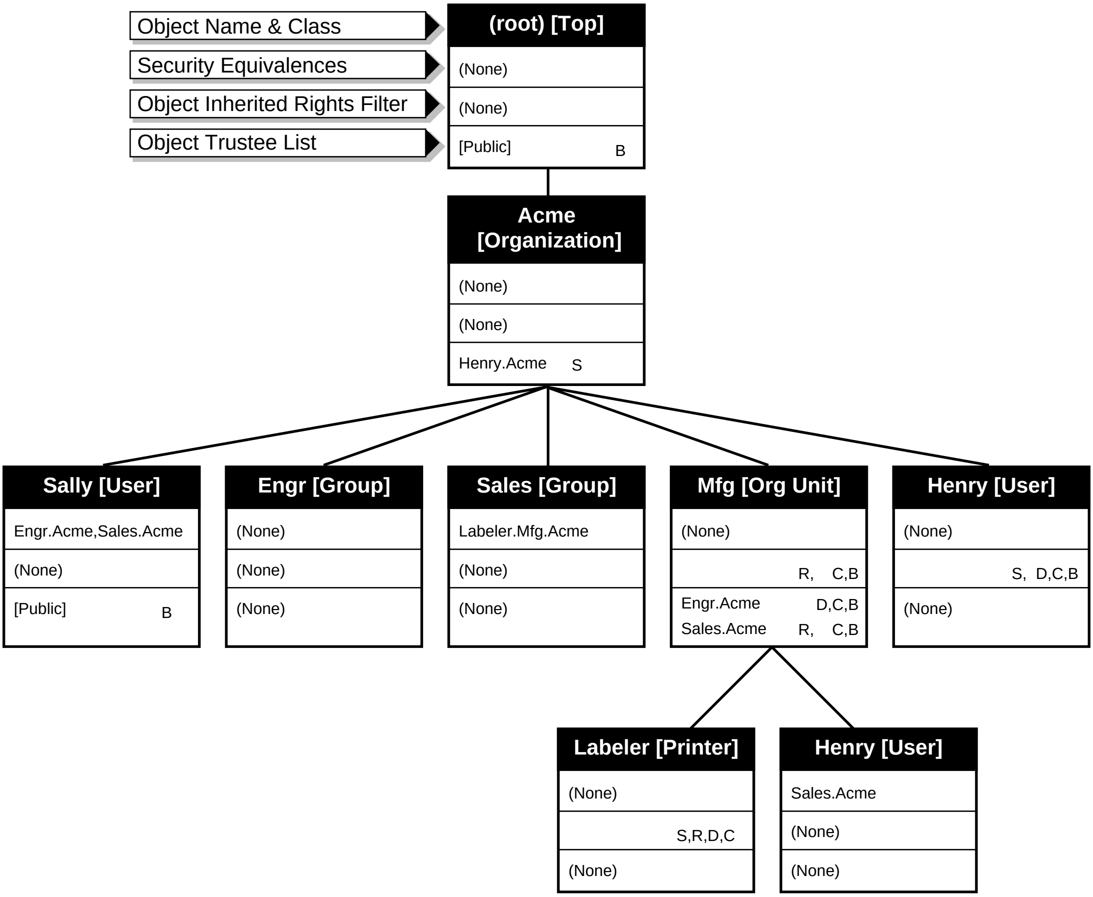


Figure 19-3 shows a sample NDS configuration. Each box represents a node in the NetWare Directory tree:

- The top portion of the box shows the object name and its NDS class.
- The second portion lists those NDS objects to which it is security equivalent.
- The third portion gives the object Inherited Rights Filter.
- The bottom portion is the object trustee list, showing subjects and object rights.

Note that this is not a realistic configuration, and is given for illustrative purposes only.

Figure 19-3
Sample NDS Configuration



There are two users named Henry in this configuration. They can be named independently (Henry.Mfg.Acme and Henry.Acme), and thus can be given rights independently.

Example Calculation 1

Using the algorithm described above, the object rights calculation for user Sally (or more precisely, for NDS object Sally.Acme) to the labeler printer (NDS object Labeler.Mfg.Acme) is as follows:

1. The security equivalence list (using the rules listed above) is:

   a. Sally.Acme

   b. [Public]

   c. [Root]

   d. Acme

   e. Engr.Acme and Sales.Acme

   There are no initial object rights associated with any of them.

Sally.Acme	(None)
[Public]	(None)
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	(None)

2. At the root of the tree, there is no object Inherited Rights Filter to eliminate rights. [Public] gains the Browse object right, so the result is as follows.

Sally.Acme	(None)
[Public]	B
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	B

3. At the Acme node, there is no object Inherited Rights Filter to eliminate rights. There is no change to the object rights set, since Henry.Acme is the only explicitly listed trustee, and Sally.Acme is not security equivalent to Henry.Acme.

4. At the Mfg.Acme node, the object Inherited Rights Filter is R,C, B, so all other object rights (namely, D and S) are removed from all entries. In this case, there is no change.

5. At the Mfg.Acme node, object rights are added for Engr.Acme and Sales.Acme, with the following result.

Sally.Acme	(None)
[Public]	B
[Root]	(None)
Acme	(None)
Engr.Acme	B,C,D
Sales.Acme	B,C,R
(Total)	B,C,D,R

6. At the Labeler.Mfg.Acme node, the object Inherited Rights Filter is S,R,D,C, so all other object rights (namely, B) are removed from all entries, with the following result.

Sally.Acme	(None)
[Public]	(None)
[Root]	(None)
Acme	(None)
Engr.Acme	C,D
Sales.Acme	C,R
(Total)	C,D,R

7. No new object rights are added at the Labeler.Mfg.Acme node, because there are no trustees.

   Thus, the object rights of Sally.Acme to Labeler.Mfg.Acme are Create, Delete, and Rename.

Example Calculation 2

For an unauthenticated user, the object rights calculation to the labeler printer is as follows:

1. The security equivalence list (using the rules listed above) is:

   a. (None)

   b. [Public]

   c. (None)

   d. (None)

   e. (None)

There are no initial object rights associated with any of them.

[Public]	(None)
(Total)	(None)

2. At the root of the tree, there is no object Inherited Rights Filter to eliminate object rights. [Public] gains the Browse object right, so the result is as follows.

[Public]	B
(Total)	B

3. At the Acme node, there is no object Inherited Rights Filter to eliminate object rights. There is no change to the object rights set, since an unauthenticated user is not security equivalent to any of the listed trustees.

4. At the Mfg.Acme node, the object Inherited Rights Filter is R,C,B, so all other object rights (namely, D, S) are removed from all entries. In this case, there is no change.

5. At the Mfg.Acme node, there is no change, since an unauthenticated user is not security equivalent to any of the listed trustees.

6. At the Labeler.Mfg.Acme node, the object Inherited Rights Filter is S,R,D,C, so all other object rights (namely, B) are removed from all entries, with the following result.

[Public]	(Total)
(None)	(None)

7. No new rights are added at the Labeler.Mfg.Acme node, because there are no trustees.

   Thus, an unauthenticated user has no rights to the Labeler.Mfg.Acme node.

Example Calculation 3

The object rights of Henry.Mfg.Acme to Henry.Acme can be calculated as follows.

1. The security equivalence list (using the rules listed above) is:

   a. Henry.Mfg.Acme

   b. [Public]

   c. [Root]

   d. Mfg.Acme and Acme

   e. Sales.Acme

   There are no initial object rights associated with any of them.

Henry.Mfg.Acme	(None)
[Public]	B
[Root]	(None)
Acme	(None)
Mfg.Acme	(None)
Sales.Acme	(None)
(Total)	B

2. At the root of the tree, there is no object Inherited Rights Filter to eliminate object rights. [Public] gains the Browse object right, so the result is as follows.

Henry.Mfg.Acme	(None)
[Public]	B
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	B

3. At the Acme node, there is no object Inherited Rights Filter to eliminate object rights. There is no change to the object rights set, since Henry.Acme is the only explicitly listed trustee, and Henry.Mfg.Acme is not security equivalent to Henry.Acme.

4. At the Henry.Acme node, the object Inherited Rights Filter is S,D,C,B, so all other object rights (namely, R) are removed, which has no effect. No new object rights are added.

   Thus, the object right of Henry.Mfg.Acme to Henry.Acme is Browse.

Example Calculation 4

The object rights of Henry.Acme to Henry.Mfg.Acme can be calculated as follows. Note that this is the converse of the previous calculation.

1. The security equivalence list (using the rules listed above) is

   a. Henry.Acme

   b. [Public]

   c. [Root]

   d. Acme

   e. Sales.Acme

   There are no initial object rights associated with any of them.

Henry.Mfg.Acme	(None)
[Public]	(None)
[Root]	(None)
Acme	(None)
Sales.Acme	(None)
(Total)	(None)

2. At the root of the tree, there is no object Inherited Rights Filter to eliminate object rights. [Public] gains the Browse object right, so the result is as follows.

Henry.Mfg.Acme	(None)
[Public]	B
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	B

3. At the Acme node, there is no object Inherited Rights Filter to eliminate object rights. The explicitly listed trustee is Henry.Acme, which is added.

Henry.Mfg.Acme	S
[Public]	B
[Root]	(None)
Acme	(None)
Sales.Acme	(None)
(Total)	S,B

4. At the Mfg.Acme node, the object Inherited Rights Filter removes the Delete and Supervisor object rights, with the following result.

Henry.Mfg.Acme	(None)
[Public]	B
[Root]	(None)
Acme	(None)
Sales.Acme	(None)
(Total)	B

5. At the Henry.Mfg.Acme node, there is no object Inherited Rights Filter, and no explicit trustees, so no object rights are changed.

   Thus, the object right of Henry.Acme to Henry.Mfg.Acme is Browse.

NDS object property rights

The following describes how to calculate the rights for a subject represented by NDS object S to the P property of the NDS object O.

1. Build a list of all NDS objects to which S is security equivalent. If S is unauthenticated, this list consists only of [Public]. If S is authenticated, this includes:
   - The object S
   - [Public], to which all users are security equivalent
   - [Root], to which all users are security equivalent
   - All NDS objects on the path from the root of the NetWare Directory tree to S
   - All NDS objects to which S has explicitly been given security equivalence
2. For each NDS object in the list, create an empty list of property rights, and an empty list of Supervisor flags.

3. Starting at the root of the NetWare Directory tree, and moving towards O, perform the following steps for each node N:

   a. If N has an property Inherited Rights Filter (IRF) for [All Properties], go through each element of the list created in Step 1 and delete all property rights except those listed as being allowed (thus rights to [All Properties] are filtered).

   b. For each trustee in N’s trustee list which is also found in the list from Step 1 with the property name [All Properties], replace the rights for the entry with the property rights from the triple (thus rights to [All Properties] are inherited).

   c. If N has an object IRF which masks the Supervisor object right, then clear the corresponding entry in the Supervisor flags list.

   d. For each trustee in N’s trustee list which is also found in the list from Step 1, if the trustee has Supervisor object rights, set the corresponding entry in the Supervisor flags list.

4. If O has a property IRF for property P, go through each element of the list created in Step 1 and delete all property rights except those listed as being allowed (thus a property-specific IRF masks out any inherited rights for [All Properties])

5. For each trustee in O’s trustee list which is also found in the list from Step 1:

   - If the property name is P, replace the property rights in the corresponding entry in the list with the property rights from the triple (thus a property-specific set of rights for the trustee replaces any rights granted to [All Properties] for that trustee).

   - If the property name is P and the trustee has Supervisor property rights, then replace the property rights in the corresponding entry in the list with the set of all property rights.

6. Take all rights from the list and bit-wise OR them together (that is, calculate the union of rights granted to S and all objects to which S is security equivalent).

7. If any element in the Supervisor flags list is set, then replace the property rights with the set of all property rights.

8. If P has the DS_PUBLIC_READ or DS_SERVER_READ flag set in the schema, add in the Read and Compare property rights.

9. If P has the DS_READ_ONLY flag set in the schema, remove the Write and Add or Delete Self property rights.

10. The result is S’s property rights to property P of NDS object O.

11. If P has the DS_HIDDEN flag set in the schema, remove all property rights.

Figure 19-4 shows a sample NDS configuration with property rights. Each box represents a node in the NetWare Directory tree.

- The top portion of the box shows the object name and its NDS class.

- The second portion lists those NDS objects to which it is security equivalent.

- The third portion gives the object Inherited Rights Filter.

- The fourth portion is the object trustee list, showing subjects and object rights.

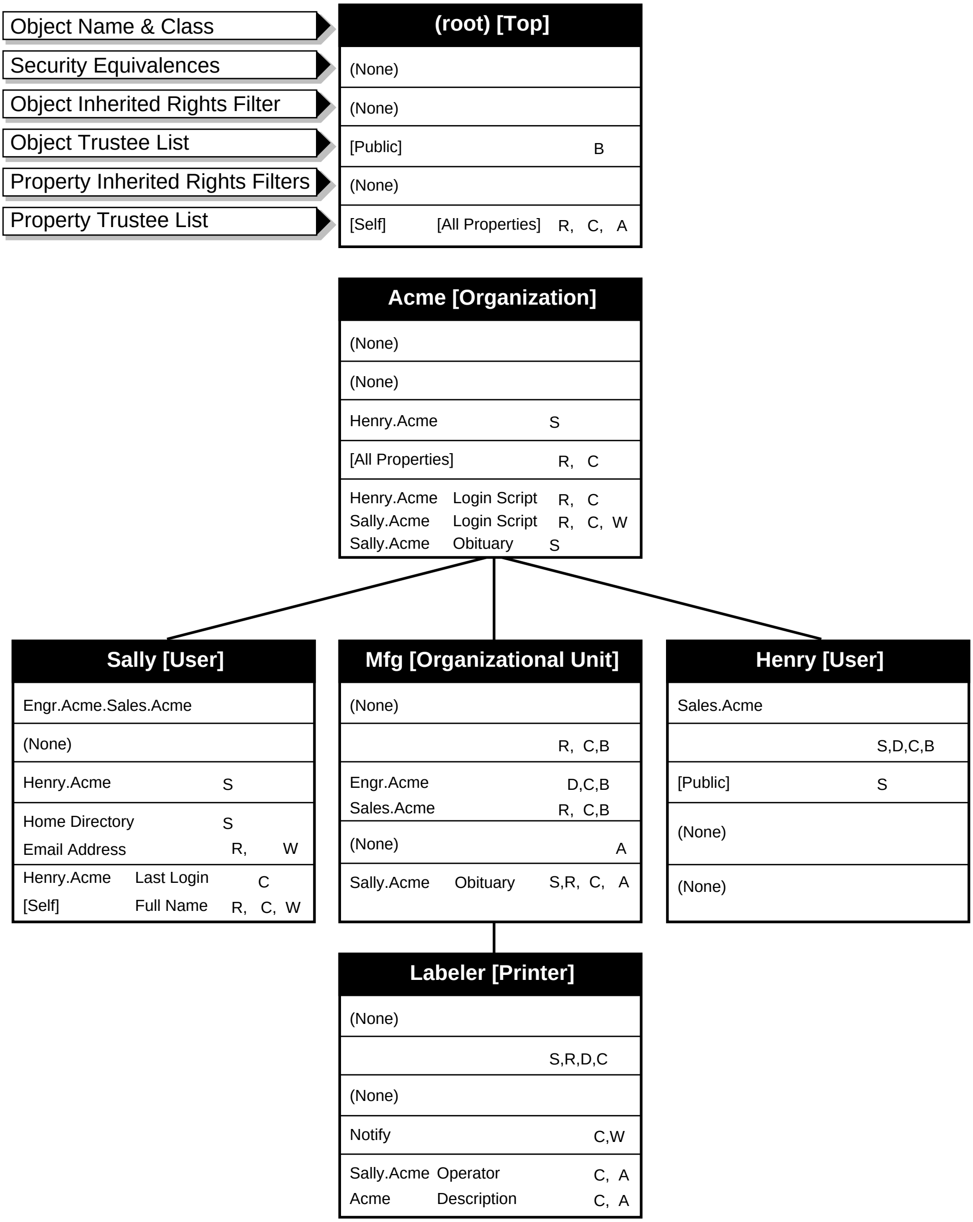
- The fifth portion is the property Inherited Rights Filters (for [All Properties] and specific properties).

- The bottom portion is the property trustee list, showing subjects and property rights.

Note that this is not a realistic configuration, and is given for illustrative purposes only.

Figure 19-4

Sample NDS Configuration with Property Rights



Example Calculation 1

Using the algorithm described above, the property rights calculation for user Sally (or more precisely, for NDS object Sally.Acme) to the Queue, Operator, Description, and Notify properties of the labeler printer (NDS object Labeler.Mfg.Acme) is as follows:

1. The security equivalence list (using the rules listed above) is:

    a. Sally.Acme

    b. [Public]

    c. [Root]

    d. Acme

    e. Engr.Acme and Sales.Acme

    There are no initial property rights associated with any of them, and the list of Supervisor flags is empty.

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	(None)	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	(None)	No

2. At the root of the tree:

    - There is no property IRF for [All Properties], so no rights are removed.
    - The entry in the property trustee list for [Self] rights to [All Properties] causes [Root] to gain the Compare, Read, and Add or Delete Self rights.

- The object IRF filters out all except Supervisor, Rename, Create, and Delete rights. Thus, it would cause Browse rights to be discarded, but because Browse rights were not present, no rights are removed.
- The object trustee list lists [Public] as a trustee, but does not grant Supervisor object rights, so it does not affect the calculation.

The rights are as follows.

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	C,R,A	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	C,R,A	No

3. At the Acme node:
    - The [All Properties] property IRF filters out all except Compare and Read rights (that is, it causes Write, Add or Delete Self, and Supervisor rights to be discarded).
    - There are no entries in the property trustee list for [All Properties].
    - There is no object IRF, so no rights are removed.
    - The object trustee list does not affect any object to which Sally is security equivalent.

The rights are as follows.

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	C,R	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	C,R	No

4. At the Mfg.Acme node:

   - There is no property IRF for [All Properties], so no rights are removed. The filter on the Login Script property does not have any effect.
   - There are no entries in the property trustee list for [All Properties]. Sally’s rights to the Obituary property have no effect.
   - The object IRF filters out all except Rename, Create, and Browse rights (that is, it causes Supervisor and Delete rights to be discarded).
   - The object trustee list does not list Sally as a trustee.

   The rights are thus unchanged.

5. At the Labeler.Mfg.Acme node:

   - There is no property IRF for [All Properties], so no rights are removed.
   - There are no entries in the property trustee list for [All Properties].

- The object IRF filters out all except Supervisor, Rename, Create, and Delete rights. Thus Browse rights can not pass through. Because there were no Browse rights, no rights are removed
- The object trustee list does not list Sally as a trustee.

The rights are thus unchanged.

6. There is no property IRF on Labeler.Mfg.Acme for the Queue, Operator, or Description properties. The property IRF for the Notify property filters out all except Compare and Write rights (that is, it causes the Supervisor, Read, and Add or Delete Self property rights to be deleted from all trustees for that property).

   Thus the rights are as follows.

Table 19-1

Trustee	Queue Property Rights	Operator Property Rights	Description Property Rights	Notify Property Rights	Supervisor Flag
Sally.Acme	(None)	(None)	(None)	(None)	No
[Public]	(None)	(None)	(None)	(None)	No
[Root]	C,R	C,R	C,R	C	No
Acme	(None)	(None)	(None)	(None)	No
Engr.Acme	(None)	(None)	(None)	(None)	No
Sales.Acme	(None)	(None)	(None)	(None)	No
(Total)	C,R	C,R	C,R	C	No

7. There are no specific rights for the Notify or Queue properties. For the Operator property, the property rights for Sally.Acme become Compare and Add or Delete Self. For the Description property, the property rights for Acme become Compare and Add or Delete Self.

Thus the rights are as follows.

Table 19-2

Trustee	Queue Property Rights	Operator Property Rights	Description Property Rights	Notify Property Rights	Supervisor Flag
Sally.Acme	(None)	C,A	(None)	(None)	No
[Public]	(None)	(None)	C,R	(None)	No
[Root]	C,R	C,R	C,R	C	No
Acme	(None)	(None)	C,A	(None)	No
Engr.Acme	(None)	(None)	(None)	(None)	No
Sales.Acme	(None)	(None)	(None)	(None)	No
(Total)	C,R	C,R,A	C,R,A	C	No

8. None of the trustees have Supervisor property rights, so the list of rights is unchanged.

9. The rights corresponding to the individual trustees are removed, leaving only the total rights.

Rights	(Total)
Queue Property rights	C,R
Operator Property rights	C,R,A
Description Property rights	C,R,A
Notify Property rights	C

10. The Operator property has the DS_PUBLIC_READ flag set, so the Read and Compare rights are added (which has no effect, since they are already there). The Queue, Description, and Notify property rights are unchanged.

11. None of the properties have the DS_READ_ONLY or DS_HIDDEN flags set.

12. Thus, the property rights for Sally.Acme are as follows.

Rights	(Total)
Queue Property rights	C,R
Operator Property rights	C,R,A
Description Property rights	C,R,A
Notify Property rights	C

Example Calculation 2

The property rights calculation for Sally.Acme to the Login Script, Obituary, Postal Code, and Revision properties of the Acme object is as follows:

1. The security equivalence list (using the rules listed above) is:
   a. Sally.Acme
   b. [Public]
   c. [Root]
   d. Acme
   e. Engr.Acme and Sales.Acme

There are no initial property rights associated with any of them, and the list of Supervisor flags is empty.

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	(None)	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	(None)	No

2. At the root of the tree:

   - There is no property IRF for [All Properties], so no rights are removed.
   - The entry in the property trustee list for [Self] rights to [All Properties] causes [Root] to gain the Compare, Read, and Add or Delete Self rights.
   - There is no object IRF, so no rights are removed.
   - The object trustee list lists [Public] as a trustee, but does not grant Supervisor object rights, so it does not affect the calculation.

The rights are thus:

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	C,R,A	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	C,R,A	No

3. At the Acme node:

- The [All Properties] property IRF filters out all except Compare and Read rights (that is, the Write, Add or Delete Self, and Supervisor rights are removed).
- There are no entries in the property trustee list for [All Properties].
- There is no object IRF, so no rights are removed.
- The object trustee list does not affect any object to which Sally is security equivalent.

The rights are as follows.

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	C,R	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	C,R	No

4. The Acme node has no property-specific IRFs.

5. The property trustee list assigns Sally.Acme the Compare, Read, and Write property rights to the Login Script property and the Supervisor property right to the Obituary property. Because Sally.Acme has the Supervisor property right to the Obituary property, she gets all property rights.

Thus the rights are as follows.

Table 19-3

Trustee	Login Script Property Rights	Obituary Property Rights	Postal Code Property Rights	Revision Property Rights	Supervisor Flag
Sally.Acme	C,R	S,C,R,W,A	(None)	(None)	No
[Public]	(None)	(None)	(None)	(None)	No
[Root]	C,R	C,R	C,R	C,R	No
Acme	(None)	(None)	(None)	(None)	No
Engr.Acme	(None)	(None)	(None)	(None)	No
Sales.Acme	(None)	(None)	(None)	(None)	No
(Total)	C,R	S,C,R,W,A	C,R	C,R	No

6. The rights corresponding to the individual trustees are removed, leaving only the total rights as follows.

Rights	(Total)
Login Script Property rights	C,R
Obituary Property rights	S,C,R,W,A
Postal Code Property rights	C,R
Revision Property rights	C, R

7. The Revision property has the DS_PUBLIC_READ flag set, so the Read and Compare rights are added. The Login Script, Obituary, and Postal Code property rights are unchanged.

Rights	(Total)
Login Script Property rights	C,R
Obituary Property rights	S,C,R,W,A
Postal Code Property rights	C,R
Revision Property rights	C,R

8. The Obituary and Revision property has the DS_READ_ONLY flag set, so the Write and Add or Delete Self property rights are removed. The Login Script and Postal Code property rights are unaffected.

Rights	(Total)
Login Script Property rights	C,R
Obituary Property rights	S,C,R
Postal Code Property rights	C,R
Revision Property rights	C,R

9. The Obituary property has the DS_HIDDEN flag set, so all rights are removed. The Revision, Login Script, and Postal Code property rights are unaffected.

Thus, the property rights for Sally.Acme are as follows.

Rights	(Total)
Login Script Property rights	C,R
Obituary Property rights	(None)
Postal Code Property rights	C,R
Revision Property rights	C,R

Example Calculation 3

The property rights calculation for Sally.Acme to the Network Address and Private Key properties of the Henry.Acme object is as follows:

1. The security equivalence list (using the rules listed above) is: (a) Sally.Acme, (b) [Public], (c) [Root], (d) Acme, and (e) Engr.Acme and Sales.Acme. There are no initial property rights associated with any of them, and the list of Supervisor flags is empty:

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	(None)	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	(None)	No

2. At the root of the tree:

   - There is no property IRF for [All Properties], so no rights are removed.
   - The entry in the property trustee list for [Self] rights to [All Properties] causes [Root] to gain the Compare, Read, and Add or Delete Self rights.
   - There is no object IRF, so no rights are removed.
   - The object trustee list lists [Public] as a trustee, but does not grant Supervisor object rights, so it does not affect the calculation.

   The rights are thus:

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	C,R,A	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	C,R,A	No

3. At the Acme node:

   - The [All Properties] property IRF filters out all except Compare and Read rights (that is, the Write, Add or Delete Self, and Supervisor rights are removed).
   - There are no entries in the property trustee list for [All Properties].
   - There is no object IRF, so no rights are removed.
   - The object trustee list does not affect any object to which Sally is security equivalent.

   The rights are thus:

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	No
[Public]	(None)	No
[Root]	C,R	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	C,R	No

4. At the Henry.Acme node:

   - There is no property IRF for [All Properties], so no rights are removed.
   - There are no entries in the property trustee list for [All Properties].
   - There is no object IRF, so no rights are removed.
   - The object trustee list shows Sally.Acme as having Supervisor rights, so the Supervisor flag is set.

The rights are thus:

Trustee	Property Rights	Supervisor Flag
Sally.Acme	(None)	Yes
[Public]	(None)	No
[Root]	C,R	No
Acme	(None)	No
Engr.Acme	(None)	No
Sales.Acme	(None)	No
(Total)	C,R	No

5. The Henry.Acme node has no property-specific IRFs, so the rights are unchanged.

6. There are no properties listed in Henry.Acme's trustee list, so the rights are unchanged.

7. The rights corresponding to the individual trustees are removed, leaving only the total rights:

Rights	(Total)
Network Address Property rights	C,R
Private Key Property rights	C,R

8. Because the Supervisor flag is set, all property rights are granted, thus yielding:

Rights	(Total)
Network Address Property rights	S,C,R,W,A
Private Key Property rights	S,C,R,W,A

9. Neither the Network Address nor Private Key property has the DS_PUBLIC_READ, DS_SERVER_READ, or DS_READ_ONLY flag set.

10. The Private Key property has the DS_HIDDEN flag set, so all property rights are removed, this yielding:

Rights	(Total)
Network Address Property rights	S,C,R,W,A
Private Key Property rights	(None)

File and directory rights

For a given subject, represented by an NDS object S, the rights of that subject to a file system object O are the union of the *standard rights* assigned through trustees with the set of *exceptional rights*. The following algorithm describes the calculation of standard rights assigned through trustees:

1. Build a list of all NDS objects to which S is security equivalent. If S is unauthenticated, this list consists only of [Public]. If S is authenticated, this includes:
   - The object S
   - [Public], to which all users are security equivalent
   - [Root], to which all users are security equivalent

- All NDS objects on the path from the root of the NetWare Directory tree to S
- All NDS objects to which S has explicitly been given security equivalence

2. If the connection is unlicensed (which includes unauthenticated):
   - If O refers to anything outside the SYS:LOGIN directory, then no rights are granted (and skip the remainder of the algorithm).
   - The rights available are Read and File Scan (and skip the remainder of the algorithm).

3. If any element in the list created in Step 1 has Supervisor rights to the NDS Server object containing the file system object, or has Write rights to the ACL of the NDS Server object, then all rights are granted, and you should skip the remaining steps.

4. For each NDS object in the list created in Step 1, create an empty list of file system access rights.

5. Starting at the root of the file system tree, and moving towards O, perform the following steps for each node N:

   a. If N has an Inherited Rights Filter (IRF), go through each element of the list created in Step 1 and delete all rights except Supervisor and those listed as being allowed.

   b. For each trustee in N’s trustee list which is also found in the list from Step 1, replace the rights for the entry with the rights given in N’s trustee list, unless the existing entry already includes Supervisor. In that case the trustee assignment is ignored.

6. Take all rights from the list and bit-wise OR them together (that is, calculate the union of rights granted to S and all objects to which S is security equivalent).

7. If the resulting list includes the Supervisor right, then add in all other rights.

8. The result is S’s file system rights to O.

The exceptional rights for a file are the union of each of the following:

- If there is a path O' of which O is a substring, and which some NDS objects listed in Step 1 has any rights, then the exceptional rights include the File Scan right. For example, if a user has the Read right to MEMOS\JANUARY\SUMMARY.TXT, this rule would give that user the File Scan right to directories MEMOS and MEMOS\JANUARY.

  This is a limited File Scan right that only applies to directories along the path to the destination, and cannot be inherited. This feature allows users to change their current directory to a location along a path to a file to which they have access, even if they have no access rights to the intermediate directory.

- If S has the auditor flag set for the volume that contains O (that is, S has sufficient rights for the Audit File object for the volume that contains O and has used a utility such as AUDITCON to initialize auditor access), then the exceptional rights include the File Scan right and the right to modify the per-file audit flag.

- If S is the owner of the file, then (depending on the particular request), the exceptional rights may include the File Scan and Modify rights.

- If O is in the SYS:LOGIN directory, then add Read and File Scan as exceptional rights.

To summarize, the rights calculation for file system objects is the same as for NDS objects, with the following exceptions:

- The Supervisor right cannot be blocked with an Inherited Rights Filter or an explicit trustee assignment.

- Unlicensed connections may Read and Scan the SYS:LOGIN directory, but can never gain any other rights, even if they are assigned to the [Public] trustee.

- The file system provides certain exceptional rights as described above, but there are no exceptional rights in NDS.

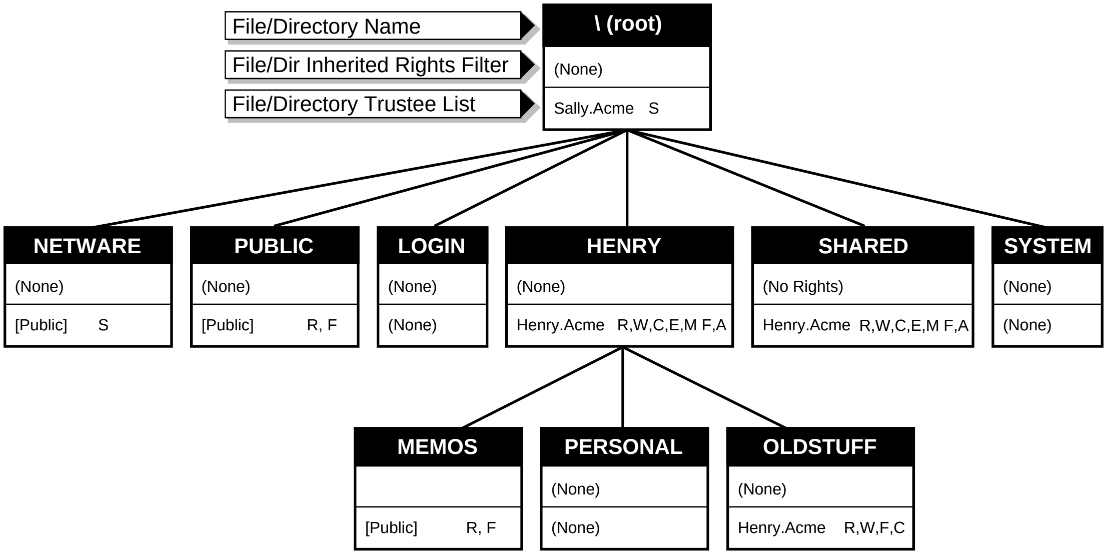
Figure 19-5 shows a sample file system configuration for a portion of a volume. Each box represents a file or directory in the file system.

- The top portion of the box shows the file system object name.
- The middle portion gives the Inherited Rights Filter.
- The bottom portion is the trustee list, showing subjects and object rights.

In the box labeled “SHARED,” note that the term “(No rights)” indicates that an IRF is present, but it does not allow any rights to pass through. Note that this is not a realistic configuration, and is given for illustrative purposes only.

For the purposes of the following examples, the NetWare tree shown in Figure 19-5 is used for security equivalences.

Figure 19-5
Sample File System Configuration



Example Calculation 1

Using the algorithm described above, the file system rights calculation for user Sally (or more precisely, for NDS object Sally.Acme) to the file system object \HENRY\MEMOS is as follows:

1. The security equivalence list is:

   a. Sally.Acme

   b. [Public]

   c. [Root]

   d. Acme

   e. Engr.Acme and Sales.Acme

   There are no initial file system rights associated with any of them.

Sally.Acme	(None)
[Public]	(None)
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	(None)

2. At the root of the volume, there is no Inherited Rights Filter to eliminate rights.

Sally.Acme gains the Supervisor object right, so the result is as follows.

Sally.Acme	S
[Public]	(None)
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	S

Note that granting Sally the Supervisor rights to the root of the volume is almost the same as granting her the Supervisor right to the NDS Server object that the volume is on.

However, if Sally has Supervisor rights to the NDS Server object, then she will have file system Supervisor rights to all volumes on the server, while granting her Supervisor right at the root of the volume gives her rights to the particular volume only.

3. The file is not in SYS:LOGIN, so the special cases do not apply.

4. At the HENRY directory, there is no Inherited Rights Filter to eliminate rights. There is no change to the object rights set, since Henry.Acme is the only explicitly listed trustee, and Sally.Acme is not security equivalent to Henry.Acme.

5. At the HENRY\MEMOS directory, the Inherited Rights Filter is R,F, so all other object rights except S (that is, W, C, E, M, and A) are removed from all entries. In this case, there is no change.

Thus, Sally.Acme has the Supervisor file system rights to \HENRY\MEMOS. Note that Henry was unable to prevent Sally from seeing his MEMOS directory, even using an IRF, because the Supervisor right cannot be stopped with an IRF.

Example Calculation 2

Using the algorithm described above, the file system rights calculation for user Henry (or more precisely, for NDS object Henry.Acme) to a file in the directory SHARED is as follows:

1. The security equivalence list is:

   a. Henry.Acme

   b. [Public]

   c. [Root]

   d. Acme

   e. Engr.Acme and Sales.Acme

   There are no initial file system rights associated with any of them.

Henry.Acme	(None)
[Public]	(None)
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	(None)

2. At the root of the volume, there is no Inherited Rights Filter to eliminate rights. There are no trustees to which Henry.Acme is security equivalent, so he does not gain any new rights.

3. At the SHARED directory, there is no Inherited Rights Filter to block rights.

4. At the SHARED directory, Henry.Acme is an explicit trustee, so the new rights are as follows.

Henry.Acme	RWCEMF
[Public]	(None)
[Root]	(None)
Acme	(None)
Engr.Acme	(None)
Sales.Acme	(None)
(Total)	RWCEMF

Therefore, Henry will have Read, Write, Create, Erase, Modify, and File Scan to any file in the SHARED directory (unless the file has an IRF or other explicit trustee assignment that would override this setting).

Example Calculation 3

Using the algorithm described above, the file system rights calculation for an unauthenticated or unlicensed user to the file system object \HENRY\MEMOS is as follows:

The connection is unlicensed. Therefore, because the \HENRY\MEMOS is not in the LOGIN directory, no rights are granted.

Thus, an unauthenticated user has no rights to \HENRY\MEMOS, despite the fact that [Public] is a trustee with Read and File Scan rights.

Example Calculation 4

Using the algorithm described above, the file system rights calculation for user Henry (when acting as an auditor) to the \SYSTEM directory can be summarized follows:

- Henry is not an explicit trustee of SYSTEM, nor is he security equivalent to any object that is. Therefore, he gets no direct rights.

- Because Henry is an auditor of the volume holding the SYSTEM directory, he will have File Scan rights, as well as the right to set or clear the per-file audit flag.

EGP

Warning

EGP is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Entry rights

A synonym for "object rights."

Execute Only (X) attribute

Warning

The Execute Only (X) attribute is an advisory indicator that may or may not be used by network clients. Do not rely on this attribute to prevent execution of files at the client. To determine whether this attribute is supported by your workstation, see your client documentation.

Extended AppleTalk network

Warning

The AppleTalk protocol suite is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Exterior Gateway Protocol

Warning

Exterior Gateway Protocol is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

External Entity object

Electronic mail (which is the intended use of External Entity objects) is not part of the NetWare Enhanced Security configuration. There are no restrictions on creating External Entity objects in the NetWare Enhanced Security configuration.

Warning

NetWare Message Handling Service is not part of the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

F

Fake root

Fake roots are a client feature. To determine whether fake roots are supported, see your client documentation.

Warning

Fake roots do not protect your files. Do not rely on them for access controls.

File owner

Note

This concept is new to this manual, and does not correspond to an entry in *Concepts*.

The owner of a file or directory in a NetWare volume. See “Owner.”

File Transfer Protocol

Warning

File Transfer Protocol is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration.

Foreign E-mail address

Warning Electronic mail is not part of the NetWare Enhanced Security configuration.

Foreign E-mail alias

Warning Electronic mail is not part of the NetWare Enhanced Security configuration.

FTP

Warning File Transfer Protocol is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

G

Group object

Warning Electronic mail is not part of the NetWare Enhanced Security configuration.

Warning Group membership does not confer trustee rights. Only security equivalence confers trustee rights. Group, Organizational Role, and other NDS objects can be used to simplify assignment of trustee rights using security equivalence.

H

HCSS

Warning High Capacity Storage System is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Hidden (H) Attribute

Warning

The Hidden attribute is a client facility, and is not part of the access control enforced by NetWare. Do not rely on this attribute to protect your data.

High Capacity Storage System

Warning

High Capacity Storage System is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

I

ICMP

Warning

Internet Control Message Protocol is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

“I’m Alive” packet

Warning

NetWare SFT III is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Inherited Rights Filter

The term “object” in this definition means “NDS object.” IRFs apply to files, directories, NDS objects, and NDS object properties. To change the IRF for an NDS object or all NDS object properties, you must have at least the Write property right to the ACL property of that object.

Input/Output Engine

Warning

NetWare SFT III is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

International use of NetWare 4

Warning

LANGUAGE.NLM and KEYB.NLM are not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Internet Control Message Protocol

Warning

Internet Control Message Protocol is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Internet Protocol

Warning

Internet Protocol is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

IOEngine

Warning

NetWare SFT III is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

IP tunneling

Warning

IP tunneling requires the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

L

LAN driver

Warning For information on the specific LAN drivers that are permitted in the server's NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*. LAN drivers are also used in the various trusted network client components; for a description of the drivers that are permitted there, see the client documentation.

Large Internet Packet

The server supports Large Internet Packet (LIP) communications. The determination of packet size is made by the client.

License Certificate object

Warning The server's NetWare Enhanced Security configuration does not include any NetWare Licensing Services (NLS) NLM programs, so this object will not be created by NLS. If the object is created by some other means, it will not be used for NLS purposes.

License Service Provider

Warning The server's NetWare Enhanced Security configuration does not include any License Service Provider (LSP) NLM programs. Loading NLM programs for NetWare Licensing Services (NLS) violates the basis of trust for the NetWare Enhanced Security server. For a list of the NLM programs included in the Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Licensed Product object

Warning The server's NetWare Enhanced Security configuration does not include any NetWare Licensing Services (NLS) NLM programs, so this object will not be created by NLS. If the object is created by some other means, it will not be used for NLS purposes.

Link Support Layer

Warning

The NetWare NetWare Enhanced Security server supports only the IPX^{TM} protocol stack. Other protocols, such as AFP and TCP/IP, require NLM programs that are not part of the NetWare Enhanced Security configuration.

Loadable module

Warning

The server's NetWare Enhanced Security configuration includes only those NLM programs identified in the *NetWare Enhanced Security Server*. Other NLM programs are not permitted in an NetWare Enhanced Security configuration. To determine whether specific VLM programs are permitted for a client, see the vendor's client documentation.

Local drive

Specific NetWare Enhanced Security workstations may or may not support local disk drives. For more information, see your vendor's client documentation.

Login

Login is a protocol-based mechanism for performing Identification and Authentication (I&A) of network users. The server supports two types of logins for network users:

NetWare 4^{TM} login	With NetWare 4, authentication is a two-step process. First, the user logs in (enters a login name and password) once to NDS. Subsequently, the client software performs background authentication to give access to various protected resources, such as other servers.
NetWare 3 login	With NetWare 3, the user must log in individually to each server that the user wishes to access.

The NetWare NetWare Enhanced Security server supports both types of logins. Login involves client and server mechanisms, as well as NCP^{TM} messages to transfer the user's I&A input from the client to the server.

Warning

A user typically logs in to the server by running the LOGIN program from the SYS:LOGIN directory on the server. However, the programs and procedures for logging in to the server may vary from one client workstation to another. For more information, see your client vendor documentation.

For both NetWare 3 and NetWare 4 logins, the server component validates the purported user identity by comparing an encrypted hash of the entered password with the corresponding value for that user maintained by NDS, which is also an encrypted hash.

A successful login changes the user’s connection from an Attached state to an Authenticated state, which gives the user access to the server’s protected resources based upon the user’s authenticated identity.

LOGIN directory

Warning

The contents of the SYS:LOGIN directory (and its subdirectories) can be publicly read by network users before the user logs in to the server. Consequently, you should not store any programs or files in the SYS:LOGIN directory that require protection by the server’s access control mechanisms.

Login restrictions

Warning

Most of the login restrictions (time restrictions, account limits, disk space limits, number of connections) are configurable, depending upon your facility requirements. However, as described in Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91, you must configure user accounts to require a password and to have a minimum password length of eight characters.

NETADMIN and NetWare Administrator are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Login scripts

Login scripts execute on the client, immediately after the user logs in. The login script is stored by the server as an NDS object property. For more information on login scripts, see Chapter 6, “Security Supplement to Creating Login Scripts,” on page 137.

Warning

If you use a client workstation to administer the server component, you must: (a) ensure that your login script does not include any non-TCB client commands and (b) protect your login script and profile properties so that they cannot be modified by nonadministrative users.

Logout

LOGOUT, NETADMIN, and NetWare Administrator are client utilities. For more information on the applicability of these utilities to your workstation, see your vendor's client documentation.

Long machine type

The long machine type, such as IBM_PC or COMPAQ, is used at the client to map a drive to the proper version of DOS on the server file system. For more information, see your vendor's client documentation.

LSL

Warning

The NetWare Enhanced Security server supports only the IPX protocol stack. Other protocols, such as AFP and TCP/IP, require NLM programs that are not part of the NetWare Enhanced Security configuration.

LSP Server object

Warning

The server's NetWare Enhanced Security configuration does not include any NetWare Licensing Services (NLS) NLM programs, so this object will not be created by NLS. If the object is created by some other means, it will not be used for NLS purposes.

M

Macintosh client

Warning

The Macintosh* name space NLM program is not included in the server's NetWare Enhanced Security configuration; consequently, Macintosh clients (if they exist) cannot store files in Macintosh format on the server. For more information on the server configuration, see *NetWare Enhanced Security Server*.

Macintosh files

Warning The Macintosh name space NLM program is not included in the server’s NetWare Enhanced Security configuration; consequently, Macintosh clients (if they exist) cannot store files in Macintosh format on the server. For more information on the server configuration, see *NetWare Enhanced Security Server*.

MAIL directory

Warning Electronic mail is not part of the NetWare Enhanced Security configuration.

Mailbox ID

Warning Electronic mail is not part of the NetWare Enhanced Security configuration.

Mailbox location

Warning Electronic mail is not part of the NetWare Enhanced Security configuration.

Management Information Base

Warning The server’s NetWare Enhanced Security configuration does not support SNMP.

Map

MAP is a client utility. To determine the applicability of this command, see your client documentation.

Memory

This description addresses the memory configuration for DOS client workstations. For more information on the use of memory on your workstation client, see your vendor documentation.

Memory allocation

This description addresses memory configurations for DOS workstations (for example, RAM disks) and for NetWare 4 servers (for example, use of a single memory pool). For more information on the use of memory on your workstation client, see your vendor documentation.

Message Routing Group object

Warning

This object is used by the server to administer electronic mail. However, electronic mail is not part of the NetWare Enhanced Security configuration.

Messaging Server object

Warning

This object is used by the server to administer electronic mail. However, electronic mail is not part of the NetWare Enhanced Security configuration.

MIB

Warning

The server’s NetWare Enhanced Security configuration does not support SNMP.

Migrated (M) attribute

Warning

Data migration is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Migration (operating system)

Warning

Server operating system upgrades are permitted only from one NetWare Enhanced Security version to another. There is no mechanism for upgrading an untrusted (such as NetWare 2.*x*, 3.*x*, or unevaluated 4.*x*) server to an NetWare Enhanced Security configuration.

Migration (protocol)

Warning

NLSP^{TM}, TCP/IP, and OSPF are not supported by the NetWare Enhanced Security server component.

Mirrored Server Engine

Warning NetWare SFT III is not included in the server NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Mirrored server link

Warning NetWare SFT III is not included in the server NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Modify bit

Warning Do not confuse the “Modify bit” (Archive Needed attribute) with the Modify file and directory right. The Archive Needed attribute is used to select files for backup, while the Modify file right is used to determine who can change the file attributes.

MS Windows client

MS Windows* is a client windowing system. To determine whether your client supports MS Windows, see your client vendor documentation.

MSEngine

Warning NetWare SFT III is not included in the server NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

MSL

Warning NetWare SFT III product is not included in the server NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Multiserver network

Warning The NetWare Enhanced Security architecture requires all servers to be NetWare Enhanced Security. Consequently, you should not install unevaluated NetWare 2.*x*, 3.*x*, or 4.*x* servers in a NetWare Enhanced Security facility.

N

Name space support

Warning

Macintosh, OS/2*, Windows 95*, Windows NT*, FTAM, and NFS* name spaces are not included in the server's NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Named pipes

Warning

Named pipes are implemented on top of SPX™. The server provides named pipes as part of its standard IPC* mechanism. However, the NetWare Enhanced Security configuration does not include the Microsoft* SQL Server, Microsoft Comm Server products, or any other server products that use named pipes.

NCP Packet Signature

Warning

The NCP Packet Signature mechanism protects against forgery of NCP messages. Because the NetWare Enhanced Security architecture requires physical or cryptographic protection of the network media, the packet signature mechanism is not required in an NetWare Enhanced Security network facility.

Warning

The NCP Packet Signature only protects against the forgery of NCP messages. It does not protect other non-NCP protocols, for example, the SPX-based print and backup protocols.

NCP Packet Signature also does not provide any additional assurance that the server's NetWare Enhanced Security software works properly. It is of use only when the underlying assumption of physically protected network media does not hold.

NetBIOS

Warning

NetBIOS is a client peer-to-peer protocol. The NetWare Enhanced Security network security architecture prohibits use of direct client-to-client communications.

NETINFO.CFG

Warning

NETINFO.CFG is a server configuration file; however, the INETCFG NLM program is not included in the server's NetWare Enhanced Security configuration.

NetSync cluster

Warning The NetWare Enhanced Security architecture does not permit use of any unevaluated (for example, NetWare 3.1*x*) servers.

NetWare 4.11 Symmetric MultiProcessing

Warning The server's NetWare Enhanced Security configuration does not include any NLM programs for Symmetric MultiProcessing (SMP). Loading these NLM programs violates the basis of trust for the NetWare Enhanced Security server. For a list of the NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

NetWare Client for DOS and Windows

The NetWare Client is client communications software. For a description of the software (such as VLM programs) and the protocols it provides, see your vendor's client documentation. Note that the server component does not support TCP/IP protocols.

NetWare Client for OS/2

NetWare Client for OS/2 is client communications software. For information on NetWare Enhanced Security OS/2 client configurations, see your vendor's client documentation.

Warning The NetWare Enhanced Security architecture does not permit direct client-to-client communications, nor does it permit application servers (applications running on dedicated nonserver hardware platforms). The NetWare Enhanced Security server component does not provide any SQL applications. Note also that the server component does not provide OS/2 name space support.

NetWare Core Protocol

NCP is the standard service protocol for NetWare. While it is commonly used with DOS or OS/2 workstation clients, it is possible for any client to generate NCP messages to the server.

NetWare Directory replica

NDS Manager and PARTMGR are client administrative utilities. For a description of trusted utilities you can use to manage synchronization of replicas, see your vendor's client documentation.

NetWare Directory Services

Note that within this description, the term "object" refers to NDS objects and does not include other named objects (such as files and directories) protected by the server.

NetWare DOS Requester

For information on the client communications software, see your vendor's client documentation.

Warning The NetWare Enhanced Security architecture (a) requires physically or cryptographically protected communications media and (b) precludes connection of untrusted devices. Consequently, the client's RSA encryption is not used to meet any NetWare Enhanced Security rating requirements.

NetWare Licensing Services

Warning The server's NetWare Enhanced Security configuration does not include any NetWare Licensing Services (NLS) NLM programs. Loading these NLM programs violates the basis of trust for the NetWare Enhanced Security server. For a list of the NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server.*

NetWare Licensing Services clients

Warning The server's NetWare Enhanced Security configuration does not include any NetWare Licensing Services (NLS) NLM programs. Consequently, NLS is not available to network clients. For a list of the NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

NetWare Link Services Protocol

Warning The NetWare Enhanced Security server component does not support the NetWare Link Services Protocol™. For information on the server's NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

NetWare Loadable Module

Warning Do not load unevaluated NLM programs into server memory. For information on the server's NetWare Enhanced Security NLM programs, see *NetWare Enhanced Security Server*.

NetWare Management Agent

Warning NetWare Management Agent™ is not included in the server's evaluated configuration. For more information, see *NetWare Enhanced Security Server*.

NetWare MHS Services

Warning The MHS electronic mail system is not included in the NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

NetWare Name Service

Warning NetWare Name Service® is not included in the server's NetWare Enhanced Security configuration.

NetWare Networked File System

Warning NetWare NFS is not included in the server's NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

NetWare NFS

Warning NetWare NFS is not included in the server's NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

NetWare protocols and transports

Warning

The NetWare Enhanced Security server component does not support the ARP, BOOTP, ICMP, IP, RARP, SNA, SNMP, TCP, UDP, and XNS* protocols. For a description of the protocols used by your client workstations, see your vendor's client documentation.

Also, note that the NetWare Enhanced Security architecture does not permit the use of client peer-to-peer protocols such as NetBIOS.

NetWare Runtime

Warning

The NetWare Enhanced Security server component does not include NetWare Runtime^{TM} NLM programs.

NetWare server

Warning

The server's NetWare Enhanced Security configuration does not include the NetWare Server for OS/2 product, or AppleTalk protocol support. For information on the specific network and storage hardware included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

NetWare Server for OS/2

Warning

NetWare Server for OS/2 is not included in the server's NetWare Enhanced Security configuration.

NetWare user tools

Warning

For information on the trusted utilities provided by your client workstation, see your vendor's client documentation. Do not use untrusted client utilities for administration of the server component.

Network communications

Warning

The NetWare Enhanced Security architecture does not permit direct peer-to-peer communications between network clients.

Network direct printer

Warning Network direct printers are permitted in the NetWare Enhanced Security architecture, but the printer interfaces must be controlled by TCB software.

Network node

Warning The NetWare Enhanced Security architecture permits servers, workstations, routers, bridges, and repeaters. Both servers and workstations may provide printers.

Network supervisor

“Network supervisor” is another term for administrator or network administrator.

NETX

For more information on client communications programs and their capabilities, see your vendor’s client documentation.

NFS

Warning Macintosh, OS/2, FTAM, and NFS name spaces are not included in the server’s NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

NLSP

Warning The NetWare Enhanced Security server component does not support the NetWare Link Services Protocol. For information on the server’s NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

NNS

Warning NetWare Name Service is not included in the server’s NetWare Enhanced Security configuration.

Nonextended AppleTalk network

Warning

The AppleTalk protocol suite is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

O

Object

Note that within this description, the term “object” refers to NDS objects and does not include other named objects (such as files and directories) protected by the server.

Warning

The server’s NetWare Enhanced Security configuration does not include any NLM programs for NLS, AFP, or MHS. Consequently, the associated NLS objects, AFP object, and MHS objects are not used by the NetWare Enhanced Security server. If you create any of these objects, they are not used by the NetWare Enhanced Security server.

ODINSUP

Warning

ODINSUP is client protocol software. NDIS* is not supported by the NetWare Enhanced Security server. For more information, see your vendor’s client documentation.

Open Shortest Path First

Warning

OSPF is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Optical disk

Warning

The High Capacity Storage System is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration, or for information on the NetWare Enhanced Security storage hardware and device drivers, see *NetWare Enhanced Security Server*.

OS/2 client

NetWare Client for OS/2 is client communications software. For information on NetWare Enhanced Security OS/2 client configurations, see your vendor's client documentation.

Warning The NetWare Enhanced Security architecture does not permit direct client-to-client communications, nor does it permit application servers (applications running on dedicated nonserver hardware platforms). The NetWare Enhanced Security server component does not provide any SQL applications. Note also that the server component does not provide OS/2 name space support.

OS/2 Requester

The OS/2 Requester is client software. For information on NetWare Enhanced Security OS/2 client configurations, see your vendor's client documentation.

OSPF

Warning OSPF is part of the TCP/IP protocol suite and is not included in the NetWare Enhanced Security configuration. For a list of the items included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Owner

To change the owner of a file or directory, you must have the Supervisor right, or you must have the Write right to the ACL of the NDS User objects corresponding to both the current file owner and the desired new file owner.

Ordinarily, file ownership does not convey any special rights in NetWare. However, for a few specific NCP requests, the owner of a file obtains certain rights beyond what is available based on an effective rights calculation.

For example, for some NCPs, ownership is equivalent to having File Scan rights. In other cases, ownership can permit a user to modify certain file attributes.

See also "Disk space restrictions"; "Rights."

P

Parent VLM

Virtual Loadable Module^{TM} (VLM) programs are client communications programs. For information on NetWare Enhanced Security client configurations, see your vendor's client documentation.

Partition management

NDS Manager and PARTMGR are client administrative utilities. For a description of trusted utilities you can use to manage synchronization of replicas, see your vendor's client documentation.

Password

Warning

The security of the server NTCB partition depends upon the proper configuration of certain password attributes in the user's NDS object. These include "Password Required" and a "Minimum Password Length" of eight characters.

For more information on user account administration procedures, see Chapter 4, "Security Supplement to Managing NetWare Directory Services Objects," on page 91.

The server does not actually manipulate the user password string. When a password is set or changed for a user, the client component hashes the user password string and a salt value into a 16-byte value that is transferred to the server and stored in the user's NDS object.

The server depends on the client to properly specify the length of the new password. At login, the client hashes the password string and salt into a 16-byte value that is transferred to the server and compared with the value stored in the NetWare Directory for that user.

PMMON

Warning

NetWare Server for OS/2 is not included in the server's NetWare Enhanced Security configuration. For more information, see *NetWare Enhanced Security Server*.

Postmaster

Warning The MHS messaging system is not included in the server's NetWare Enhanced Security configuration. For more information on the NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Postmaster General

Warning The MHS messaging system is not included in the server's NetWare Enhanced Security configuration. For more information on the NLM programs included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Primary server

Warning NetWare SFT III is not included in the server's NetWare Enhanced Security configuration.

Print device definition

NetWare Administrator, PRINTDEF, PRINTCON, NPRINT, CAPTURE, and PCONSOLE are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Print header and print tail

PRINTDEF is a client utility. To determine whether this utility is available for your component, see your client documentation.

Print job

Warning If you have multiple users sharing a printer, you must ensure that the printer output is administratively controlled once it is printed.

Print job configuration

PRINTCON is a client utility. Refer to your client documentation to determine whether this utility is available for your component.

Print queue

NetWare Administrator and PCONSOLE are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Print queue operator

Warning The print queue operator must be a trusted administrator within the context of the users serviced by the queue. If the queue is potentially accessed by all users on the network, then the print queue operator must be a network supervisor. If the queue is limited to a specific organization or workgroup, then the print queue operator must be trusted by that organization but need not be a network supervisor.

Print server

PSERVER.EXE is a print server for DOS-based client workstations. To determine whether your trusted client workstation supports client-based print servers, see your client documentation.

Print Server Status and Control Protocol (PSSCP)

Note This concept is new to this manual, and does not correspond to an entry in *Concepts*.

The Print Server Status and Control Protocol (PSSCP) is an SPX-based communications protocol that is available for network clients to request certain services from the print server (PSERVER.NLM).

Network users and operators (referred to as "administrators") can perform services such as requesting the status of print jobs, deleting print jobs, changing forms, etc. A user can only access his or her own job; while an operator can access any print job.

Print tail

PRINTDEF is a client utility. To determine whether this utility is available for your component, see your client documentation.

Printer

NPRINTER.EXE is a print driver for a DOS-based workstation client. To determine whether your trusted client workstation supports client-based print servers, see your client documentation.

NetWare Administrator and PCONSOLE are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Printer form

NPRINT, CAPTURE, NetWare Administrator, PCONSOLE, and PRINTDEF are client utilities. To determine whether your trusted client workstation supports client-based print servers, see your client documentation.

Printer mode

NetWare Administrator and PRINTDEF are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Property

NETADMIN and NetWare Administrator are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Proxy ARP

Warning

The Address Resolution Protocol (ARP) is used by Internet Protocol (IP) and AppleTalk components. The NetWare Enhanced Security server does not support either protocol.

Pseudo hop count

Warning

NetWare SFT III product is not included in the server's NetWare Enhanced Security configuration.

Public trustee

The [Public] trustee does not exist as an NDS object. It is a means for defining the default rights for all users on the network to NDS objects, files, or directories. Assigning [Public] as a trustee tells the server to give the associated rights to all users.

The interpretation of the [Public] trustee is different for file system objects (files and directories) and NDS objects, as follows:

File system objects	A [Public] trustee assignment to a file or directory gives any authenticated and licensed user the associated rights to that object. For example, if the [Public] trustee has File Scan rights to a directory, any authenticated and licensed user can list the files and subdirectories in that directory. Unauthenticated, or authenticated but unlicensed, users do not gain any rights assigned to the [Public] trustee. They are restricted to the LOGIN directory.
NDS objects	A [Public] trustee assignment to an NDS object gives unauthenticated users the associated rights to the object. For example, a [Public] Browse assignment to the NDS [Root] object permits users to read names from the NetWare Directory tree.

Warning

Do not give the [Public] object any rights to the NDS [Root] object. Because of inheritance, a [Public] assignment to [Root] gives unauthenticated users those rights throughout the Directory before the user logs in.

Purge (P) attribute

Warning

The Purge (P) attribute is used by the server to manage storage of deleted file space. This is not addressed by the NetWare file system access control policy, and you should not rely on it for protection of sensitive information.

Q

Queue server mode

Warning Network direct printers are permitted in the NetWare Enhanced Security architecture, but the printer interfaces must be controlled by TCB software.

R

RARP

Warning The NetWare Enhanced Security server component does not support the RARP protocol.

Read Only (Ro) attribute

Warning The Read Only (Ro) attribute supplements the NetWare file system access control policy. Do not rely on this attribute for protection of sensitive information. Instead, use the Write file system right to control who can write the file.

Remote console

Warning The server's NetWare Enhanced Security configuration does not include support for remote consoles.

Remote printer mode

Warning Remote printers operate as client components within the network architecture. All printer interfaces must be controlled by TCB software at the remote printer component.

Remote Reset

DOSGEN is a client utility. To determine whether this utility is available for your component, see your client documentation.

Warning

The contents of the SYS:LOGIN directory may be readable by unauthenticated users. Do not put any data in this directory that you do not wish to be publicly visible to anyone who physical access to a workstation on the network.

As mentioned in “Planning Directory Structures” on page 129, if you assign an explicit trustee to a file in the SYS:LOGIN directory, only logged-in users will have access to the file.

Rename Inhibit (Ri) attribute

Warning

The Rename Inhibit (Ri) attribute supplements the NetWare file system access control policy. Do not rely on this attribute for protection of sensitive information. Instead, use the Modify file system right to control who can modify the file or directory name.

Resource fork

Warning

The NetWare Enhanced Security server does not provide the Macintosh name space NLM program. Consequently, Macintosh files are not stored on the server component.

Resynchronization

Warning

NetWare SFT III is not included in the server’s NetWare Enhanced Security configuration.

Reverse Address Resolution Protocol

Warning

The NetWare Enhanced Security server component does not support the RARP protocol.

Rights

Throughout this discussion, the term “object” is used to refer to NDS objects. Further, NDS objects also represent active entities (“subjects” in computer security terminology), and the term “object” is also used to refer to the entity that is accessing another object.

Warning

If you give a user NDS Supervisor right to a server object, that user gets Supervisor file system rights to all files on the server.

NETADMIN, NetWare Administrator, and RIGHTS are client utilities. To determine whether these utilities are available for your component, see your client documentation.

RIP (TCP/IP)

Warning

The NetWare Enhanced Security server component does not support TCP/IP.

RIP II (TCP/IP)

Warning

The NetWare Enhanced Security server component does not support TCP/IP.

Router

Warning

The NetWare Enhanced Security server configuration does not include TCP/IP and AppleTalk protocols. INETCFG.NLM is also not included in the NetWare Enhanced Security configuration.

Router Information Protocol

Warning

The INETCFG and FILTCFG NLM programs are not included in the server's NetWare Enhanced Security configuration.

S

Salvageable files

FILER is a client utility. To determine whether this utility is available for your component, see your client documentation.

The complete list of flags associated with each property can be found in the *NetWare Directory Services Schema Specification*, which is part of the NetWare server SDK.

Each built-in object class has a default ACL which is assigned to newly created objects of that class. For the default ACL definitions for built in object classes, see Table 4-1 on page 92.

Creating a new type of NDS object (for example, Appliance) is not the same as creating an instance of that object (for example, Fred’s Toaster). The former modifies the schema, while the latter simply creates an object in a container.

Warning Novell does not provide any client or server utilities to extend the schema beyond its base definition. Under certain conditions you may extend the schema using third-party utilities.

If you extend the schema using third-party utilities or client applications you write yourself, you must ensure that

- If any new object classes are created and they have the Public Key and Private Key attributes, there are procedural or other means to ensure that the passwords selected for objects of the class are at least as strong as the passwords required for objects of the User class as described in “User Account Administration (Client)” on page 116.

  In addition, there must be procedural or other means to ensure that objects of the new class cannot be created with null passwords. It is best not to create new classes with the Public Key and Private Key attributes, because they can be used to log into the system. You should verify that there is an valid reason for adding such classes.

- For existing attributes added to existing or new object classes, the rights available to nonadministrative users are restricted to those described in Table 4-2 on page 98.

- If any new attributes are created, nonadministrative users should not be granted any rights to those attributes.

A newly created object class can be used for any purpose that a built-in class is used for. It can be a trustee of NDS or file system objects, and other objects can be security equivalent to it. There is no fundamental difference between object classes in the base schema and those added, other than

- Base object classes cannot be removed from the schema
- Added object classes do not have default ACLs beyond those inherited from the Top class and other superclasses, and
- The AUDITCON utility does not allow selection of nonbase classes for volume auditing of “User and File” or “User or File” events.

See also “Inherited Rights Filter”; “Object”; “Rights.”

Search modes

This describes the algorithms used by workstation clients to search for program to execute. It does not pertain to the server component.

FLAG is a client utility. To determine whether this utility is available for your component, see your client documentation.

Secondary server

Warning

NetWare SFT III is not included in the server’s NetWare Enhanced Security configuration.

Security

Warning The security of the server NTCB partition depends upon the proper configuration of certain password attributes in the user’s NDS object. These include Password Required and a Minimum Password Length of eight characters.

For more information on user account administration procedures, see Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.

FLAG, FILER, RIGHTS, NETADMIN, and NetWare Administrator are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Warning Do not give the [Public] object any rights to the NDS [Root] object. Because of inheritance, a [Public] assignment to [Root] gives unauthenticated users those rights throughout the Directory before the user logs in.

Warning File and directory attributes supplement the NetWare file system access control policy. Do not rely on them for protection of sensitive information. Instead, you should use file rights. For example, rather than using the Delete Inhibit (Di) file attribute, you should remove the Delete right from any user who should not be able to delete the file.

Server console

Warning The NetWare server must be physically protected, such that the server console (keyboard and screen) can be accessed only by trusted administrative personnel. This requirement can be met by placing the server in a locked room, with keys to the room distributed only to the supervisor(s) that are trusted to properly install, configure, and administer the server.

(Note that use of the SECURE CONSOLE command, on a physically unprotected server, does not meet the NetWare Enhanced Security requirements for server protection.)

Warning The server’s NetWare Enhanced Security configuration does not include support for remote consoles. Consequently, the client remote console utility, RCONSOLE.EXE, will not work with the NetWare Enhanced Security server component.

Server mirroring

Warning NetWare SFT III is not included in the server’s NetWare Enhanced Security configuration.

Service Advertising Protocol

Warning INETCFG.NLM is not included in the server's NetWare Enhanced Security configuration.

Shareable (Sh) attribute

Warning The Shareable (Sh) attribute supplements the NetWare file system access control policy by permitting simultaneous accesses to files. Do not use this attribute to control access to files.

Short machine type

The short machine type is used at the client to map a drive to the proper version of DOS on the server file system. For more information, see your vendor's client documentation.

Simple Network Management Protocol

Warning The server's NetWare Enhanced Security configuration does not support SNMP, TCP/IP, or NMS software. Any third-party software, including SNMP management consoles, must first be supported by NetWare Enhanced Security (as described in the *NetWare Enhanced Security Server*) before it can be safely loaded on the server.

SNA

Warning The NetWare Enhanced Security server does not support the IBM* SNA network protocols.

SNMP

Warning The server's NetWare Enhanced Security configuration does not support SNMP.

Source Routing

Warning ROUTE.NLM is not included in the server's NetWare Enhanced Security configuration.

Sparse file

NCOPY is a DOS client utility. For information on the availability and use of the NCOPY command, see your client documentation.

SPX

SPX is a communications protocol that provides connection-oriented services to network clients. SPX provides the underlying connection mechanism for the Printer Communications Protocol (PCP), the Print Server Status and Control Protocol (PSSCP), and SMS communications.

Storage Management Services

Warning The server’s NetWare Enhanced Security configuration does not include any workstation TSAs (Target Service Agents, such as TSADOS.NLM, TSAOS2.NLM), file system TSAs for previous, unevaluated versions of NetWare (such as TSA311.NLM), or TSAs for non-NetWare Directory databases (such as TSASQL). Consequently, it is not possible for SMS to backup workstations, non-NetWare Enhanced Security server file systems, or Btrieve databases.

For information about the permitted TSAs and also the permitted device drivers included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

STREAMS

Warning The server does not support TCP/IP, SNA, or OSI communications protocols.

Subnetwork mask

Warning The server does not support IP addressing.

SUPERVISOR bindery login

The bindery SUPERVISOR has the Supervisor right to the root directory of all file systems (volumes) on its server. The bindery SUPERVISOR also has the Supervisor right to the NDS container in which the NDS server object is found. However, some NDS utilities may not operate when logged as the bindery SUPERVISOR.

The initial password for the bindery SUPERVISOR is set when the server is installed by copying the initial password for ADMIN. Subsequently, the ADMIN and SUPERVISOR passwords are independent (that is, changing one does not affect the other).

LOGIN is a client utility. To determine whether this utility is available for your component, see your client documentation.

Warning There are no tools included in NetWare 4.*x* for managing the bindery SUPERVISOR login. Therefore, you cannot disable the account, set minimum password length, frequency of password changes, or other user characteristics. It is your responsibility as a supervisor to set the bindery SUPERVISOR password in accordance with those restrictions.

The bindery SUPERVISOR is a valid login whenever there is a bindery context set.

If the bindery SUPERVISOR login becomes disabled (such as through intruder detection) you can use the “Enable login” console command to reenable it.

See also “Bindery context” in *Concepts* and “LOGIN” and “ENABLE LOGIN” in *Utilities Reference*.

Supervisor right

Warning In the file system, the Supervisor right cannot be blocked by an Inherited Rights Filter. In NDS, the Supervisor right can be blocked by an Inherited Rights Filter. Therefore, in NDS you must be careful not to use IRFs that would render portions of the Directory tree unmanageable.

The difference between the file system Access Control and Supervisor rights are as follows:

- The Access Control right can be blocked by an IRF, while the Supervisor right cannot.
- The Supervisor right allows setting and removing disk space restrictions, which the Access Control right does not.
- The Supervisor right allows setting the file owner, which the Access Control right does not.
- The Supervisor right *automatically* grants all other rights (such as Read and Write). With the Access Control right, users can grant themselves any other rights (except Supervisor), but the additional rights are not automatically provided by the NetWare software.
- The Access Control right can be used to grant any right except Supervisor, while the Supervisor right can be used to grant any right.
- The Supervisor right is not lost even if an explicit trustee assignment is made, but the Access Control right can be lost this way.

Supported gateway

Warning The NetWare Enhanced Security server component does not include support for NetWare MHS, SNADS, or X.400 messaging.

System Fault Tolerance

Warning NetWare SFT III is not included in the NetWare Enhanced Security configuration. For a list of software included in the NetWare Enhanced Security configuration see *NetWare Enhanced Security Server*.

System (Sy) attribute

Warning The System attribute supplements the NetWare file system access control policy. Do not rely on it to prevent modification of client programs. Instead, remove the Write and Modify file system rights to control access to client programs.

System Network Architecture

Warning The NetWare Enhanced Security server does not support IBM’s SNA network protocols.

T

Target Service Agent

The NetWare Enhanced Security server does not include any NLM programs to permit backing up client workstations.

Task-switching support software

For information on the use of task-switching software on the client component, see your vendor’s client documentation.

TCP/IP

Warning The NetWare Enhanced Security server component does not support TCP/IP protocols, IP tunneling, or NFS.

Time Synchronization

Warning In the NetWare Enhanced Security configuration, you must use a custom configuration, not SAP.

Transaction Tracking System

The NetWare Enhanced Security server does not support Btrieve.

FILER and FLAG are client utilities. For more information on the use of these utilities, see your client documentation.

Transactional (T) attribute

The Transactional attribute controls nonpolicy aspects of file handling, by ensuring that all or no changes are made when a file is modified multiple times.

Transmission Control Protocol

Warning

The NetWare Enhanced Security server component does not support TCP/IP protocols.

Trustee

Throughout this discussion, the term "object" is used to refer to NDS objects. Further, NDS objects also represent active entities ("subjects" in computer security terminology), and the term "object" is also used to refer to the entity that is accessing another object.

Warning

If you give a user NDS Supervisor right to a server object, that user gets Supervisor file system rights to all files on the server.

FILER, NETADMIN, NetWare Administrator, and RIGHTS are client utilities. To determine whether these utilities are available for your component, see your client documentation.

Warning

Do not give the [Public] object any rights to the NDS [Root] object. Because of inheritance, a [Public] assignment to [Root] gives unauthenticated users those rights throughout the Directory before the user logs in.

U

Universal Naming Convention redirection

Windows, the MS-DOS* NET USE command, and the Windows File and Print Managers are client utilities. To determine how these utilities map to server resources, see your client documentation.

UNIX client

Warning

The NetWare Enhanced Security architecture allows for UNIX clients. However, the server does not provide name space support for UNIX clients, so the client is limited to using the DOS name space. Further, all clients must be single-user workstations.

Unknown object

Warning

As described in Chapter 3, “Security Supplement to Installation,” on page 69, you must not migrate or upgrade unevaluated NetWare servers (such as NetWare 2.*x* or 3.*x*) to a NetWare Enhanced Security component.

Upgrade

Warning

As described in Chapter 3, “Security Supplement to Installation,” on page 69, the upgrade mechanism will be used only to upgrade from one NetWare Enhanced Security version to another.

You must not migrate or upgrade unevaluated NetWare servers (such as NetWare 2.*x* or 3.*x*) to an NetWare Enhanced Security component. You also must not upgrade to an NetWare Enhanced Security server from any other non-NetWare products (such as IBM LAN Server or Microsoft LAN Manager*).

UPS monitoring

Warning

Do not install non-NetWare Enhanced Security hardware (that is, hardware not identified in *NetWare Enhanced Security Server*) in the server component. Installation of non-NetWare Enhanced Security hardware in the server, even a board for monitoring a UPS device, violates the basis of trust provided by the server evaluation. Even one non-NetWare Enhanced Security hardware component will invalidate your server’s rating.

User Datagram Protocol

Warning The NetWare Enhanced Security server does not provide UDP or any of the other TCP/IP protocols.

User object

Warning User names are public information that can be determined by all users. If the [Public] trustee has Browse rights to the [Root] object, a user can read other user names from NDS before logging in. If the Browse right is disabled, unauthenticated users can still query NDS to determine names of existing users. Regardless, names of all NDS objects, including users, are public information, and you should not give names that convey sensitive information.

Login scripts are stored on the server, but execute on network clients. For more information on login scripts, see Chapter 6, “Security Supplement to Creating Login Scripts,” on page 137.

Warning All of the User Account Restrictions that are described in this portion of *Concepts* are available for you to control who can log in, when, and from what workstation.

However, the security of the server NTCB partition depends upon the proper configuration of certain password attributes in the user’s NDS object. These include Password Required and a Minimum Password Length of eight characters.

For more information on user account administration procedures, see Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.

NETADMIN and NetWare Administrator are client utilities. To determine whether these utilities are available for your component, see your client documentation.

User template

Warning

Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91 describes use of a USER_TEMPLATE object to configure security characteristics that must apply to all User objects created within a container. These include Password Required and a Minimum Password Length of eight characters.

For more information on user account administration procedures, see Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91.

Utilities

Warning

The NetWare Enhanced Security configuration does not include the NetWare Server for OS/2 product or any specific console commands for that product.

DOS, Windows, OS/2, and the OS/2 Presentation Manager* are client programs. For more information on the use of this software by your client component, see your client documentation.

V

Value-added process

Warning

VAP refers to a NetWare 2 capability. Because the NetWare Enhanced Security server does not include NetWare 2, this does not pertain to the NetWare Enhanced Security server component.

Virtual Loadable Module

VLM programs are client software that run on DOS workstations. For more information on your client’s software architecture, see your client documentation.

Volume

NetWare Administrator, NETADMIN, FILER, MAP, and VOLINFO are client administrative utilities. For a description of trusted utilities you can use to manage synchronization of replicas, see your vendor’s client documentation.

chapter 20

Security Supplement to Utilities Reference

This chapter contains additional NetWare® Enhanced Security information supplementing *Utilities Reference*. The titles in this chapter match those in *Utilities Reference*; for those utilities not listed in this chapter, there is no additional information necessary for the NetWare Enhanced Security configuration.

Command Syntax

There are no additional security warnings for this chapter.

Utilities

ACTIVATE SERVER (Console)

Warning

This console command is used to manage NetWare SFT III^{TM}, and is not included in the NetWare Enhanced Security configuration. Only those NLM^{TM} programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs that are not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

ADD NAME SPACE (Console)

Warning

Support for name spaces other than DOS is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

ADDICON (Client)

ADDICON is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

AFP (Server)

Warning AFP.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

AFPCON (Server)

Warning AFPCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

ATCON (Console)

Warning ATCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

ATCONFIG (Server)

Warning ATCONFIG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

ATOTAL (Client)

ATOTAL is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

ATPS (Server)

Warning

ATPS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

ATPSCON (Console)

Warning

ATPSCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

ATXPR (Server)

Warning

ATXPR.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

AUDITCON (Client)

AUDITCON is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Auditors are only partially independent of network administrators. For more information on the independent auditor concept, see *Auditing the Network*.

BRGCON (Console)

Warning

BRGCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

BROADCAST (Console)

Warning

Because you cannot tell whether a user is physically at their client computer, use this command only for broadcasting nonsensitive information (for example, the server is going down for backups).

CAPTURE (Client)

CAPTURE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

CD (Console)

When you mount a CD for use with CDROM.NLM, NetWare builds an index of all the files and directories on the CD. This index is stored in SYS:\CDROM$$.ROM, unless you use the "/V=" option when you load the CDROM.NLM. In that case, it is in the volume you specified.

The index file is also used to store trustee assignments, files logically deleted from the CD-ROM, and files logically copied to the CD-ROM. The index file can be destroyed with the CD PURGE command or by mounting the CD-ROM with the "/R" (rebuild index) option.

When using the CD GROUP command, the group name supplied is not verified until you use it with the CD MOUNT or CD CHANGE commands. The group name specified must be an NDS Group object in the bindery context of the server. (See the "Bindery Context" parameter under "SET" in *Utilities Reference*.)

If the group name is not an NDS Group object, you will get an error when you use the CD MOUNT or CD CHANGE commands, and only users with the Supervisor right to the NDS server object representing the server will be able to access the volume.

If you do not have an EVERYONE group in the server's bindery context, by default no groups will have access to mounted CD-ROMs.

When using the CD MOUNT and CD CHANGE commands, if you specify a group with the "/G=" option or use the default group of EVERYONE, a trustee entry is created at the root of the CD volume for that group, granting Read and File Scan rights to the CD-ROM volume.

You can add additional trustees, subject to the normal file system access controls. The trustee lists are retained after the CD-ROM is dismounted and recovered the next time the volume is remounted. Using the CD Purge command eliminates the cache of trustees for the volume.

Warning

Do not use the /MAC or /NFS options with the CD MOUNT or CD CHANGE commands. The Macintosh* and NFS* name spaces are not included in the NetWare Enhanced Security configuration.

CDROM (Console)

Warning

If you use the "/V" option, ensure that the CDROM$$.ROM directory in the specified volume is protected in the same way as the CDROM$$.ROM directory in the SYS: volume. Nonadministrative users must *not* have any access to CDROM$$.ROM.

Warning

HFSLF.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in NetWare Enhanced Security Server are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security Configuration will invalidate your server's C2 rating.

CLIB (Console)

Warning

Third-party NLM programs are not included in the NetWare Enhanced Security configuration. Disregard the portion of this command that describes how to load third-party NLM programs using CLIB.

COLORPAL (Client)

COLORPAL is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

CONLOG (Console)

Warning CONLOG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

CX (Client)

CX is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

DHCPCFG (Server)

Warning DHCPCFG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

DISABLE LOGIN (Console)

Warning This command disables future logins and background authentication. It does not affect users who are already logged in. You can terminate connections that are already established with the CLEAR STATION console command or the MONITOR console utility.

DSMIGRATE (Client)

DSMIGRATE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

DOSGEN (Client)

DOSGEN is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning

RPL.NLM, which is required to use DOSGEN, is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

EDIT (Console)

Warning

EDIT.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

ENABLE LOGIN (Console)

Warning

This command unlocks the SUPERVISOR bindery account, not the administrator's account as stated in *Utilities Reference*.

FILER (Client)

FILER is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

FILTCFG (Console)

Warning

FILTCFG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

FLAG (Client)

FLAG is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning

File and directory attributes supplement the NetWare file system access control policy. Do not rely on them for protection of sensitive information. Rather, you should use file rights. For example, rather than using the Delete Inhibit (Di) file attribute, you should remove the Delete right from any user who should not be able to delete the file.

Warning

The Execute Only (X) attribute is advisory only. It may be implemented by clients. Do not rely on this attribute to prevent reading of files.

Warning

The Copy Inhibit (Ci) attribute is advisory only. It may be implemented by clients. Do not rely on this attribute to prevent copying of files.

HALT (Console)

Warning

This console command is used to shut down NetWare SFT III, and is not included in the NetWare Enhanced Security configuration.

HCSS (Console)

Warning

HCSS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

HFSCD (Server)

Warning

HFSCD.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

HSFCDCON (Console)

Warning

HSFCDCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

INETCFG (Console)

Warning INETCFG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

IPXCON (Console)

Warning IPXCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

IPXPING (Console)

Warning IPXPING.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

IPXS (Console)

Warning IPXS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

KEYB (Server)

Warning KEYP.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

LOAD (Console)

Warning

Do not use this command to load any NLM programs (Novell® or third-party) that are not part of the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

Warning

The Macintosh name space is not part of the NetWare Enhanced Security configuration. Do not use this command to load the Macintosh name space.

Warning

For instructions on how to determine if a device driver is included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

LOGIN (Client)

LOGIN is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

LOGOUT (Client)

LOGOUT is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

MACFILE (Server)

Warning

MACFILE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

MAP (Client)

MAP is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

MEMORY MAP (Console)

Warning

This console command is used to examine memory usage in SFT III, which is not included in the NetWare Enhanced Security configuration.

MIGPRINT (Client)

MIGPRINT is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

MIGRATE (Client)

MIGRATE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

MIRROR STATUS (Console)

Warning

NetWare SFT III is not part of the NetWare Enhanced Security configuration. Ignore that part of the command description that deals with SFT III.

MONITOR (Console)

Warning

Use of the console lock facility does not replace the requirement for keeping the server console in physically secured facility.

MPDRIVER (Server)

Warning

MPDRIVER.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

MSERVER (Console)

Warning

This console command is used for NetWare SFT III and is not included in the NetWare Enhanced Security configuration.

NCOPY (Client)

NCOPY is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NCUPDATE (Client)

NCUPDATE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NDIR (Client)

NDIR is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning

File and directory attributes supplement the NetWare file system access control policy. Do not rely on them for protection of sensitive information. Instead, you should use file rights. For example, rather than using the Delete Inhibit (Di) file attribute, you should remove the Delete right from any user who should not be able to delete the file.

Warning

The Execute Only (X) attribute is advisory only. It may be implemented by clients. Do not rely on this attribute to prevent reading of files.

Warning

The Copy Inhibit (Ci) attribute is advisory only. It may be implemented by clients. Do not rely on this attribute to prevent copying of files.

NDS MANAGER (Client)

NDS Manager is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NETADMIN (Client)

NETADMIN is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning Before assigning file and directory rights with NETADMIN, see “Making the File System Secure and Accessible (Client)” on page 132 for cautions about rights assignments.

Warning Before assigning NDS rights with NETADMIN, see “Default Objects and Rights for NetWare 4.11” on page 92 for cautions about rights assignments.

Warning Before creating user templates with NETADMIN, see “User Account Administration (Client)” on page 116 for cautions about required user template settings in the NetWare Enhanced Security configuration.

Warning Before creating user objects with NETADMIN, see “User Account Administration (Client)” on page 116 for cautions about required user account settings in the NetWare Enhanced Security configuration.

Warning When you use NETADMIN to create a new User object, it copies the User object USER_TEMPLATE as its template. NETADMIN cannot be used to create Template objects or to create users from Template objects.

Warning Before setting property values with NETADMIN, see “User Account Administration (Client)” on page 116 for cautions about minimum settings in the NetWare Enhanced Security configuration.

NETSYNC3 (Console)

Warning NETSYNC3.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

NETSYNC4 (Console)

Warning NETSYNC4.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

NETUSER (Client)

NETUSER is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning Before using this utility to change a password, see the restrictions on passwords in *Security Features User Guide*.

NetWare Administrator (Client)

NetWare Administrator is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning Before assigning file and directory rights with NetWare Administrator, see "Making the File System Secure and Accessible (Client)" on page 132 for cautions about rights assignments.

Warning Before assigning NDS rights with NetWare Administrator, see "Default Objects and Rights for NetWare 4.11" on page 92 for cautions about rights assignments.

Warning NetWare Administrator uses Template objects as the basis for creating new User objects. It will not examine the USER_TEMPLATE object used by NETADMIN.

Warning Before creating user templates with NetWare Administrator, see "User Account Administration (Client)" on page 116 for cautions about required user template settings in the NetWare Enhanced Security configuration.

Warning Before setting property values with NetWare Administrator, see "User Account Administration (Client)" on page 116 for cautions about minimum settings in the NetWare Enhanced Security configuration.

NetWare Application Launcher (Client)

NetWare Application Launcher is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare Application Manager (Client)

NetWare Application Manager is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare Directory Browser (Client)

NetWare Directory Browser is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare File Migration (Client)

NetWare File Migration is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare Login (Client)

NetWare Login is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare Print Choser (Client)

NetWare Print Choser is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare Tools—OS/2 (Client)

NetWare Tools—OS/2 is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare TSA—OS/2 (Client)

NetWare TSA—OS/2 is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare User Tools (Client)

NetWare User Tools is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NetWare Volume Mounter (Client)

NetWare Volume Mounter is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NLIST (Client)

NLIST is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NLS Manager (Client)

NLS Manager is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NMENU (Client)

NMENU is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NPAMS (Console)

Warning

NPAMS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

NPATH (Client)

NPATH is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NPRINT (Client)

NPRINT is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NPRINTER-OS/2 (Client)

NPRINTER-OS/2 is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NPRINTER-Windows 95 (Client)

NPRINTER-Windows 95 is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NPRINTER.EXE (Client)

NPRINTER.EXE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NPRINTER.NLM (Console)

Warning

When loading NPRINTER.NLM, see the warnings associated with printer configurations in Chapter 18, “Security Supplement to Print Services,” on page 187.

NWSTART (Client)

NWSTART is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NWSTOP (Client)

NWSTOP is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NVER (Client)

NVER is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

NWIPCNFG (Server)

Warning NWIPCNFG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

NWXTRACT (Client)

NWXTRACT is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning Do not use NWXTRACT to extract unevaluated NLM programs from a distribution CD-ROM.

PARTMGR (Client)

PARTMGR is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

PCONSOLE (Client)

PCONSOLE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

PING (Console)

Warning

PING.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

PMMON (Console)

Warning

PMMON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

PRINTCON (Client)

PRINTCON is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

PRINTDEF (Client)

PRINTDEF is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

PSC (Client)

PSC is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

PSERVER (Console)

Warning When loading PSERVER, see the warnings associated with printer configurations in Chapter 18, “Security Supplement to Print Services,” on page 187.

Warning If the print server has been configured to require a password (as is required in the NetWare Enhanced Security configuration), PSERVER.NLM will prompt you for the print server password before continuing. The print server password must therefore be available to console operators so they can provide it when loading the print server.

PUPGRADE (Console)

Warning PUPGRADE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

PURGE (Client)

PURGE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

RCONSOLE (Client)

RCONSOLE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning The RCONSOLE command requires that the REMOTE NLM program be loaded. Because REMOTE is not included in the NetWare Enhanced Security server configuration, this client utility will not operate in the NetWare Enhanced Security configuration.

REMAPID (Console)

Warning

REMAPID.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

REMOTE (Console)

Warning

REMOTE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

Remote Console (Mac OS-Based Workstations) (Client)

Remote Console (Mac-OS-Based Workstations) is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning

The RCONSOLE command requires that the REMOTE NLM program be loaded. Because REMOTE is not included in the NetWare Enhanced Security server configuration, this client utility will not operate in the NetWare Enhanced Security configuration.

REMOVE DOS (Console)

Warning

In the NetWare Enhanced Security configuration, the REMOVE DOS command must be in your AUTOEXEC.NCF file.

RENDIR (Client)

RENDIR is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

RESTART (Console)

Warning This console command is used to manage NetWare SFT III, and is not included in the NetWare Enhanced Security configuration.

RIGHTS (Client)

RIGHTS is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning When using the /I option, be aware that only certain trustees are shown (for example, if you use Organizational Role objects, they will not show up as trustees). To see the complete list of trustees of a file system object, you can use the FILER or NetWare Administrator utilities (if they are part of your client software).

Also, note that the algorithm displayed by this command is not the exact algorithm used for calculating file system rights. In particular, the /I option does not show the replacement of trustee rights closer to the root with rights closer to the leaf. While the calculation shown is incorrect, the effective rights shown are accurate.

ROUTE (Console)

Warning ROUTE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

RPL (Console)

Warning RPL.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

RS232 (Console)

Warning RS232.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

RSPX (Console)

Warning RSPX.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

SCHDELAY (Console)

Warning SCHDELAY.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

SEARCH (Console)

This command is unnecessary in the NetWare Enhanced Security configuration, because all NetWare Enhanced Security NLM programs are in the SYS:SYSTEM directory.

SECURE CONSOLE (Console)

Warning Use of this feature does not replace the requirement for keeping the server console in physically secured facility.

SEND (Console)

Warning Because you cannot tell whether a user is physically at their client computer, use this command only for broadcasting nonsensitive information (for example, that the server is going down for backups).

SEND (Client)

SEND is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

Warning Because you cannot tell whether a user is physically at their client computer, use this command only for broadcasting nonsensitive information (for example, that the server is going down for backups).

Warning Administrators who are responsible for auditing of volumes or containers must not use the /A=P or /A=N options, as these would cause loss of important messages regarding audit overflow.

SERVER (Console)

Warning Do not use the –s, –na, or –ns options except for troubleshooting. These options cause commands in AUTOEXEC.NCF and STARTUP.NCF to be skipped, which can lead to your server not executing commands required in the NetWare Enhanced Security configuration.

SERVMAN (Console)

Warning Do not use SERVMAN to set any options not allowed in the NetWare Enhanced Security configuration.

SET (Console)

Communication Parameters

Warning NetWare SFT III is not part of the NetWare Enhanced Security configuration. Disregard the default values for SFT III systems.

File Caching Parameters

Warning Increasing the “Dirty Disk Cache Delay Time” parameter will result in greater potential loss of audit data. In addition, it will cause greater potential loss of changes to file system trustee lists. Use caution in changing this parameter.

Time Synchronization Parameters

Warning

Use extreme caution in changing the synchronization parameters. Failure to maintain synchronized clocks can cause audit trails to become misleading, due to inaccurate representations of time.

NCP Parameters

Warning

NCP packet signatures may be useful when running networks that are not physically or cryptographically protected (that is, outside the NetWare Enhanced Security configuration). Using NCP packet signatures does not replace the requirement for a physically or cryptographically protected network in the NetWare Enhanced Security configuration.

Warning

The “Reject NCP Packets with Bad Lengths” and “Reject NCP Packets with Bad Components” parameters must be set to ON in the NetWare Enhanced Security configuration.

Miscellaneous Parameters

Warning

The Allow Unencrypted Passwords parameter must be set to OFF in the Enhance d Security configuration.

Warning

The “Automatically Repair Bad Volumes” parameter must be set to ON. Setting this parameter to OFF could allow file system corruption, which could in turn cause incorrect access control decisions. To support this parameter, the VREPAIR.NLM utility must *not* be deleted from the DOS file system after it is automatically put there by the INSTALL utility.

Warning

If you increase the value of the “Maximum Service Processes” parameter and you are performing any auditing on the server, you must recalculate the necessary audit overflow file size and use the AUDITCON utility to set the new value. Failure to do so may result in loss of audit data.

Warning

In the NetWare Enhanced Security configuration, the “Allow Audit Passwords” parameter must be set to OFF in the Enhance d Security configuration. Failure to do so will allow use of passwords instead of the NetWare Enhanced Security access controls for audit trails.

Warning

The ENABLE_SECURE.NCF parameter must be set to ON in the NetWare Enhanced Security configuration.

Warning

MetWare SMP is not part of the NetWare Enhanced Security configuration. Disregard all SMP parameters.

NetWare Directory Services Parameters

Warning

In the NetWare Enhanced Security configuration, the “Check Equivalent To Me parameter” must be set to ON.

The “NDS Trace to Screen” parameter can be used for determining when replicas of an NDS partition have been synchronized. For information on how to use this parameter to determine the synchronization status of a partition, see “Viewing and Managing NDS Synchronization Status (Console)” on page 145.

SFT III Parameters

NetWare SFT III is not part of the NetWare Enhanced Security configuration. Disregard all SFT III parameter settings.

SETPASS (Client)

SETPASS is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

SETTTS (Client)

SETTTS is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

SETUPDOC (Client)

SETUPDOC is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

SPXCONFG (Console)

Warning

SPXCONFG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

SYSTIME (Client)

SYSTIME is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

TCPCON (Console)

Warning

TCPCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

TECHWALK (Server)

Warning

TECHWALK.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

TPING (Console)

Warning

TPING.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server's C2 rating.

UIMPORT (Client)

UIMPORT is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

UPS (Console)

Warning UPS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

UPS_AIO (Server)

Warning UPS_AIO.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

UPS STATUS (Console)

Warning The UPS STATUS command is implemented by the UPS.NLM, which is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

UPS TIME (Console)

Warning The UPS TIME command is implemented by the UPS.NLM, which is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

VIEW (Server)

Warning VIEW.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. Loading NLM programs not in the NetWare Enhanced Security configuration will invalidate your server’s C2 rating.

WHOAMI (Client)

WHOAMI is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

WSUPDATE (Client)

WSUPDATE is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

WSUPGRD (Client)

WSUPGRD is a client utility. To determine how and whether to use this feature in the NetWare Enhanced Security configuration, see your client trusted facility manual.

LAN Driver Statistics

The following warnings and additional information supplement Appendix A, “LAN Driver Statistics,” of *Utilities Reference*.

Monitoring Network Traffic

Common LAN Driver Statistics

Warning Of the TSMs listed, only ETHERTSM is included in the NetWare Enhanced Security configuration. For a complete list of NLM programs in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Warning For instructions on how to determine whether a network board is included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Custom LAN Driver Statistics

Warning For instructions on how to determine whether a network board is included in the NetWare Enhanced Security configuration, see *NetWare Enhanced Security Server*.

Warning

Tables A-3, A-4, and A-5 (under “Common LAN Driver Statistics” in Appendix A of *Utilities Reference*) do not apply to the NetWare Enhanced Security configuration, because the TOKENTSM, RXNETTSM, and FDDITSM are not included in the NetWare Enhanced Security configuration.

Tables A-7 and A-8 (under “Custom LAN Driver Statistics” in *Utilities Reference*) do not apply because token ring and IBM* baseband PCN2L drivers are not included in the NetWare Enhanced Security configuration.

chapter 21 Security Supplement to System Messages

This chapter contains additional NetWare® Enhanced Security information supplementing *System Messages*. The titles in this chapter match those in *System Messages*; for those system messages not listed in this chapter, there is no additional information necessary for NetWare Enhanced Security.

2XUPGRADE

Warning Upgrading from an unevaluated configuration to an NetWare Enhanced Security configuration is not supported.

ADSP

Warning NLM^{TM} programs that support AppleTalk* protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

AFP

Warning NLM programs that support AppleTalk protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Appletalk

Warning

NLM programs that support AppleTalk protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

ATCON

Warning

ATCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

ATOTAL

ATOTAL is client software. To determine whether you will see system messages of this type, see your client documentation.

ATPS

Warning

NLM programs that support AppleTalk protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

ATXRP

Warning

NLM programs that support AppleTalk protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

AUDITCON

AUDITCON is client software. To determine whether you will see system messages of this type, see your client documentation.

AURP

Warning NLM programs that support AppleTalk protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

AUTO

AUTO is client software. To determine whether you will see system messages of this type, see your client documentation.

BIND

BIND is client software. To determine whether you will see system messages of this type, see your client documentation.

BOOTPFWD

Warning NLM programs that support TCP/IP protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

BTRIEVE

Warning BTRIEVE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

CAPTURE

CAPTURE is client software. To determine whether you will see system messages of this type, see your client documentation.

COLORPAL

COLORPAL is client software. To determine whether you will see system messages of this type, see your client documentation.

CONLOG

Warning

CONLOG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

CONN

CONN is client software. To determine whether you will see system messages of this type, see your client documentation.

CX

CX is client software. To determine whether you will see system messages of this type, see your client documentation.

DNWxxxx

DNWxxxx is client software. To determine whether you will see system messages of this type, see your client documentation.

DOMAIN

Warning

DOMAIN.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

DSI

Warning

Message 30: PARTMGR.EXE (DOS text utility), NetWare Administrator (graphical utility), and PMADMIN (OS/2* utility) are client utilities. To determine the utilities to use to find out which server contains the master replica of the container's partition, see your client documentation.

DSKSHARE

Warning

DSKSHARE is part of NetWare for OS/2, which is not part of the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

DSREPAIR

Message 33: FILER is client software. To determine what utility to use to check whether there are any available directory entries on the volume, see your client documentation.

EDIT

Warning

EDIT.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

EXOS-OS2

EXOS-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

FILER

FILER is client software. To determine whether you will see system messages of this type, see your client documentation.

FIO

FIO is client software. To determine whether you will see system messages of this type, see your client documentation.

FLAG

FLAG is client software. To determine whether you will see system messages of this type, see your client documentation.

Messages 300, 325: RIGHTS is client software. To determine which utility to use to check whether there are any available directory entries on the volume, see your client documentation.

FLTSRV

Warning

FLTSRV.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

GENERAL

The messages listed are client software. To determine which utility to use to check whether you will see system messages of this type, see your client documentation.

HCSS.NLM

Warning

HCSS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

HFSCD

Warning HFSCD.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

HFSCDCON

Warning HFSCDCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

INETCFG

Warning INETCFG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

INSTALL

Warning Message 107: BTRIEVE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning Message 109: BTRIEVE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning Message 115: BTRIEVE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning

Message 436: INETCFG.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning

Message 478: MSSTART.NCF and IOSTART.NCF are not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning

Message 480: IOAUTO.NCF and MSAUTO.NCF are not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning

Message 483: ISSLIB.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning

Message 488: ICMD.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IOENGINE (SFT III)

Warning

IOENGINE (SFT III^{TM}) is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IPCONFIG

Warning

IPCONFIG is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IPTUNNEL

Warning

IPTUNNEL is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IPXCON

Warning: IPXCON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IPXFLT

Warning: IPXFLT is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IPXNCP

IPXNCP is client software. To determine whether you will see system messages of this type, see your client documentation.

IPXODI

IPXODI is client software. To determine whether you will see system messages of this type, see your client documentation.

IPXRTR

Warning: IPXRTR is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IPXRTRNM

Warning: IPXRTRNM is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

IPXS

Warning

IPXS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

LANSUP-DOS

LANSUP-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

LANSUP-OS2

LANSUP-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

LANZENET.DOS

LANZENET.DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

LOGIN

LOGIN is client software. To determine whether you will see system messages of this type, see your client documentation.

LOGOUT

LOGOUT is client software. To determine whether you will see system messages of this type, see your client documentation.

MacIPXGW

Warning

MacIPXGW is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

MAP

MAP is client software. To determine whether you will see system messages of this type, see your client documentation.

MHS

Warning

MHS is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

MHSCON

Warning

MHSCON is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

MHSDEINS

Warning

MHSDEINS is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

MHSINS

Warning

MHSINS is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

MIGRATE

MIGRATE is client software. To determine whether you will see system messages of this type, see your client documentation.

MSENGINE (SFT III)

Warning MSENGINE (SFT III) is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

NCOPY

NCOPY is client software. To determine whether you will see system messages of this type, see your client documentation.

NCUPDATE

NCUPDATE is client software. To determine whether you will see system messages of this type, see your client documentation.

NDIR

NDIR is client software. To determine whether you will see system messages of this type, see your client documentation.

NDS

NDS.VLM is client software. To determine whether you will see system messages of this type, see your client documentation.

NE1000-DOS

NE1000-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NW1000-OS2

NW1000-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NE1500T-DOS

NE1500T-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NW1500T-OS2

NW1500T-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NE2_32-DOS

NE2_32-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NW2_32-OS2

NW2_32-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NE2-DOS

NE2-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NE2-OS2

NE2-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NE2000-DOS

NE2000-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NW2000-OS2

NW2000-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NE2000+-DOS

NE2000+-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NW2000+-OS2

NW2000+-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NE2100-DOS

NE2100-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NW2100-OS2

NW2100-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NE3200-DOS

NE3200-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

NW3200-OS2

NW3200-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NETADMIN

NETADMIN is client software. To determine whether you will see system messages of this type, see your client documentation.

NETSYNC

Warning

NETSYNC3.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

NETUSER

NETUSER is client software. To determine whether you will see system messages of this type, see your client documentation.

NETX

NETX is client software. To determine whether you will see system messages of this type, see your client documentation.

NLIST

NLIST is client software. To determine whether you will see system messages of this type, see your client documentation.

NMENU

NMENU is client software. To determine whether you will see system messages of this type, see your client documentation.

NMR

NMR is client software. To determine whether you will see system messages of this type, see your client documentation.

NPATH

NPATH is client software. To determine whether you will see system messages of this type, see your client documentation.

NPRINT

NPRINT is client software. To determine whether you will see system messages of this type, see your client documentation.

NPRINTER-DOS

NPRINTER.EXE is client software. To determine whether you will see system messages of this type, see your client documentation.

NPRINTER.NLM

Warning

AIO.NLM is not included in the NetWare Enhanced Security server configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

NPRINTER-OS2

NPRINTER-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

NVER

NVER is client software. To determine whether you will see system messages of this type, see your client documentation.

NWDRV

NWDRV is client software. To determine whether you will see system messages of this type, see your client documentation.

NWDSBRWS

NWDSBRWS is client software. To determine whether you will see system messages of this type, see your client documentation.

NWP

NWP is client software. To determine whether you will see system messages of this type, see your client documentation.

NWSxxxx

NWSxxxx is client software. To determine whether you will see system messages of this type, see your client documentation.

NWTIL

Warning

NWTIL.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

NWTILR

Warning

NWTILR.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

NWTOOLS

NWTOOLS is client software. To determine whether you will see system messages of this type, see your client documentation.

NWXTRACT

NWXTRACT is client software. To determine whether you will see system messages of this type, see your client documentation.

NetWare Client for OS/2 Install

NetWare Client for OS/2 Install is client software. To determine whether you will see system messages of this type, see your client documentation.

PARTITION

PARTITION is client software. To determine whether you will see system messages of this type, see your client documentation.

PARTMGR

PARTMGR is client software. To determine whether you will see system messages of this type, see your client documentation.

PCN2L-NW

Warning

PCN2L-NW is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

PCN2L-OS2

PCN2L-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

PCONSOLE

PCONSOLE is client software. To determine whether you will see system messages of this type, see your client documentation.

PING

Warning PING.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

PMMON

Warning PMMON.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

PNWxxxx

PNWxxxx is client software. To determine whether you will see system messages of this type, see your client documentation.

PRINTCON

PRINTCON is client software. To determine whether you will see system messages of this type, see your client documentation.

PRINTDEF

PRINTDEF is client software. To determine whether you will see system messages of this type, see your client documentation.

PS2ESDI

PS2ESDI is client software. To determine whether you will see system messages of this type, see your client documentation.

PS2SCSI

PS2SCSI is client software. To determine whether you will see system messages of this type, see your client documentation.

PSC

PSC is client software. To determine whether you will see system messages of this type, see your client documentation.

PSERVER

Message 90: NLIST is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 95: NETADMIN is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 95: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 96: NETADMIN is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 96: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 102: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Messages 127 through 130: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 183: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 217: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 240: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 247: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Message 269: PCONSOLE is client software. To determine what utility to use to perform the necessary action, see your client documentation.

PUPGRADE

Warning

PUPGRADE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

PURGE

PURGE is client software. To determine whether you will see system messages of this type, see your client documentation.

RCONSOLE

Warning

The RCONSOLE command requires that the REMOTE NLM program be loaded. Because REMOTE is not included in the NetWare Enhanced Security server configuration, this client utility will not operate in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Warning

Message 82: The REMOTE, RSPX, and RS232 NLM programs are not included in the NetWare Enhanced Security configuration.

Warning

Message 118: The REMOTE, RSPX, and RS232 NLM programs are not included in the NetWare Enhanced Security configuration.

REDIR

REDIR is client software. To determine whether you will see system messages of this type, see your client documentation.

REMOTE

Warning REMOTE.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

RENDIR

RENDIR is client software. To determine whether you will see system messages of this type, see your client documentation.

REQxxxx

Warning REQxxxx is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

REQINSTALL

Warning REQINSTALL is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

RIGHTS

RIGHTS is client software. To determine whether you will see system messages of this type, see your client documentation.

RS232

Warning RS232.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

RSA

RSA is client software. To determine whether you will see system messages of this type, see your client documentation.

RSPX

Warning

RSPX.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

SALVAGE

SALVAGE is client software. To determine whether you will see system messages of this type, see your client documentation.

SECURITY

Warning

SECURITY.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

SEND

Warning

Message 120: NETADMIN and NetWare Administrator are client software. To determine what utility to use to perform the necessary action, see your client documentation.

Warning

Message 125: NETX is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Warning

Message 140: NETADMIN and NetWare Administrator are client software. To determine what utility to use to perform the necessary action, see your client documentation.

Warning

Message 441: NLIST is client software. To determine what utility to use to perform the necessary action, see your client documentation.

SEND

SEND is client software. To determine whether you will see system messages of this type, see your client documentation.

SERVER

Message 847: AUDITCON is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Warning

Message 932: RTDM.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Message 1251: AUDITCON is client software. To determine what utility to use to perform the necessary action, see your client documentation.

Warning

Messages 1556, 1557: DOMAIN.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Messages 2006 through 2050: SETTTS is client software. Consult your client documentation for the utility to perform the necessary action.

SERVMAN

Warning

Message 171, 172: MSSTART.NCF is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

SETPASS

SETPASS is client software. To determine whether you will see system messages of this type, see your client documentation.

SETTTS

SETTTS is client software. To determine whether you will see system messages of this type, see your client documentation.

SNMP

Warning

NLM programs that support TCP/IP protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

SNMP Client

SNMP Client is client software. To determine whether you will see system messages of this type, see your client documentation.

SNMPLOG

Warning

NLM programs that support TCP/IP protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

SYSTIME

SYSTIME is client software. To determine whether you will see system messages of this type, see your client documentation.

TASKID

TASKID is client software. To determine whether you will see system messages of this type, see your client documentation.

TBM12

TBM12 is client software. To determine whether you will see system messages of this type, see your client documentation.

TCPCON

Warning NLM programs that support TCP/IP protocols are not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

TCP/IP

Warning TCP/IP is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

TEXTUTIL-utility_name

TEXTUTIL-utility_name is client software. To determine whether you will see system messages of this type, see your client documentation.

TOKENDMA-NW

Warning TOKENDMA-NW is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

TOKEN-NW

Warning TOKEN-NW is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

TOKEN-OS2

TOKEN-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

TPING

Warning

TPING.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

TRAN

TRAN is client software. To determine whether you will see system messages of this type, see your client documentation.

TRXNET-DOS

TRXNET-DOS is client software. To determine whether you will see system messages of this type, see your client documentation.

TRXNET-OS2

TRXNET-OS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

TSA400

Warning

TSA400 is replaced by TSA410 in the NetWare Enhanced Security configuration.

TSADOS

Warning

TSADOS is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

TSAOS2

TSAOS2 is client software. To determine whether you will see system messages of this type, see your client documentation.

TSASMS

TSASMS is client software. To determine whether you will see system messages of this type, see your client documentation.

TUI

Warning

TUI is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

UIMPORT

UIMPORT is client software. To determine whether you will see system messages of this type, see your client documentation.

UPS

Warning

UPS.NLM is not included in the NetWare Enhanced Security configuration. Only those NLM programs identified in *NetWare Enhanced Security Server* are included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

VLM

VLM^{TM} programs are client software. To determine whether you will see system messages of this type, see your client documentation.

WHOAMI

WHOAMI is client software. To determine whether you will see system messages of this type, see your client documentation.

WSUPDATE

WSUPDATE is client software. To determine whether you will see system messages of this type, see your client documentation.

WSUPGRD

WSUPGRD is client software. To determine whether you will see system messages of this type, see your client documentation.

Error Codes

Appendix A of *System Messages* contains error codes for the general configuration. These have not been amended to reflect the NetWare Enhanced Security configuration.

MHS Error Reasons, Explanations, and Actions

Warning

MHS is not included in the NetWare Enhanced Security configuration. You should not see system messages of this type in the NetWare Enhanced Security configuration.

Workstation Error Messages

These error messages all relate to client software. To determine whether you will see system messages of this type, see your client documentation.

chapter 22 Summary

Physical Security Considerations

All servers and consoles must be physically protected. This is because there is no login provided at the server console. Therefore, anyone who has physical access to the console has access to the server resources.

The steps taken to physically secure the servers and consoles are dependent on the sensitivity of the information accessible via the servers. In some cases, a locked room is sufficient. In other cases, a guarded area is warranted. In all cases, only trustworthy administrators should be able to enter commands at the server console.

Because there is no identification of users at the console, you should keep a manual log of what users have access to the server console. For information on how to maintain and use this log, see *Auditing the Network*.

In addition to protecting the servers and consoles, the network media (cabling, routers, etc.) must also be either physically or cryptographically protected to prevent wiretapping attacks. An intruder can

- Perform a passive wiretap attack by connecting to the network and reading the information being transmitted

- Perform an active wiretap attack by connecting to the network and writing or modifying packets in transit

NetWare® Enhanced Security uses encryption for various functions within the network, but such encryption should not replace physically protecting network media. Encryption should only be used to add an extra degree of protection over physically protecting the network media.

Personnel Security Considerations

Your organization must provide trustworthy administrators for the server and the network. The server enforces rules set in place by these administrators.

Because of the broad permissions that are necessary for administrators to perform their jobs, an administrator can deliberately or inadvertently make changes to the server that affect the protection of all the data on the server and the network.

Users should also be trustworthy to some degree. However, users without administrative privileges are restricted and their actions (either malicious or unintentional) do not compromise security for all of the data on the server and network, but only to the data to which they have access.

Again, the burden is on the administrator to limit access permissions for certain users and to remove user accounts under certain circumstances. These might include

- Termination of employment
- Violation of specified security procedures by such actions as leaving printed output laying around, writing down their password by their workstation, or leaving their workstation unattended while logged in

Administrative Security Considerations

As an administrator, you must be extremely careful when you are working at the server console or logged in as an administrator at a client workstation. The parameters you set and the NLM^{TM} programs you load directly affect the security provided by the server component.

You must also be extremely careful when you are logged in as an administrator at a network client. This is because your account has permissions to access and modify the access permissions enforced by the server.

Additionally, you should keep the following security considerations in mind:

- You should not run DOS on the server hardware except to boot the server. In addition, booting from a DOS diskette puts the system at risk from virus damage. For this reason, neither you nor anyone else should run DOS on the server hardware, except to boot the server or perform maintenance tasks.
- You should physically protect the licensing diskette.
- The system cannot protect any data that is external to the system, such as printed output and removable media. You must protect your printed output and instruct users to do likewise.

TCB Protection

You need to make sure access rights are set such that nonadministrative users do not have access to TCB directories that contain TCB files and programs.

For information about setting up permissions for NDS^{TM} objects and object properties, see Chapter 4, “Security Supplement to Managing NetWare Directory Services Objects,” on page 91. For information about setting up permissions for TCB files and directories, see Chapter 5, “Security Supplement to Managing Directories, Files, and Applications,” on page 129.

Do not change the permissions for NDS objects and object properties from what is preconfigured. You may modify the permissions of leaf objects as specified in Chapter 4.

Social Engineering

Many security failures are a result of “social engineering”—the use of social means (such as phone requests) rather than technical means to gain access to protected resources. The following is a list of social engineering techniques to be aware of that are commonly used to violate system security.

- **Phone or E-mail requests for password changes.** Before changing any user’s password (especially to a specific value requested by the user), make sure you know that the request is from the authorized user of the account.

  A potential intruder could call up, masquerade as a legitimate user, and ask that his or her password be changed. Once the password is changed, the intruder has control of the account.

- **Emergency access to server consoles.** Security guards and other personnel should be trained not to allow “emergency” access to servers by unauthorized personnel.

  An intruder could come into a facility (especially after hours) and insist that there’s an emergency that necessitates access to the computer facility even though he or she is not on the list of authorized personnel.

  Once the intruder gains access to the room, he or she has access to the information on the server.

- **Requests for current passwords.** Users should be trained not to give their password to anyone unless they know that person to be an authorized administrator.

  An intruder could call a user and masquerade as an administrator, claiming to need the user’s password to solve a problem. Once the intruder has the user’s password, he or she has control of the account.

Do List

- *Do* read the online manuals *before* installing the server software.
- *Do* physically restrict the console to prevent access by nonadministrative users.
- *Do* make and securely store frequent backups of TCB configuration files. Your computer system can be replaced, but it may not be possible to replace the data stored on your system.
- *Do* set the console parameter to disable use of audit passwords (as required for the NetWare Enhanced Security configuration).
- *Do* configure your audit trails properly: only trusted users as Audit Administrators and Audit Viewers, only workstation TCBs as Audit Sources.
- *Do* provide sufficient space for audit data collection.
- *Do* archive audit files on a regular basis.
- *Do* keep a manual record of per-user and per-file audit configuration flags, since they are not backed up by SBACKUP.
- *Do* file reports (User Comment Forms) with Novell if you find any problems with the server programs or documentation.
- *Do* create a separate account (for example, MSMITH-ADM) for administrative work.
- *Do* set up a separate administrative account for each administrator. (*Don't* share administrator accounts.)
- *Do* use a strong password for your administrative accounts.
- *Do* change the password frequently for your administrative accounts.
- *Do* set up a separate administrative account for each administrator (that is, do not share the ADMIN account).
- *Do* configure the server to remove DOS (using REMOVE DOS) after NetWare has booted.

- *Do* configure the IPX^{TM} restriction on all printer objects so that print servers will accept connections only from valid printer drivers.

- *Do* protect SYS:PUBLIC, SYS:SYSTEM, SYS:CDROM$$$, SYS:QUEUES, SYS:DELETED.SAV, SYS:DOC, and SYS:MAIL by defining the appropriate file system rights settings.

- *Do* set up print queues, print servers, and printers such that only trusted users are on the list of operators, only evaluated print servers are on the list of servers, and all users are on the list of users.

- *Do* modify all user template settings before creating any users: set minimum password length to at least eight characters, password required to “yes”, and account disabled to “true.”

- *Do* use a user template when creating new users.

- *Do* develop a site policy for password changes, and enforce it.

- *Do* configure the USER_TEMPLATE and all NDS User objects so that each user can change his or her own password.

- *Do* enable password expiration.

- *Do* configure audit trails to shut off operations when audit trails fill, to avoid audit loss.

- *Do* physically protect the licensing diskette.

- *Do* protect printed output and instruct users to do likewise.

- *Do* protect removable media (such as tapes and floppy disks) and instruct users to do likewise.

- *Do* configure the CMOS settings for your server to boot from drive C:, not drive A:. This will minimize the risk of malicious software (such as viruses) infecting your server if you accidentally leave a floppy diskette in the drive when rebooting.

- *Do* run the system integrity tests referred to in “System Integrity” on page 38 whenever you suspect a hardware failure.

Don’t List

- *Don’t* allow general (nonadministrative) users to have access to the server console.
- *Don’t* type your administrative password at any time other than
  - When running INSTALL to set up the server
  - At the server console SBACKUP prompt, or
  - To the TCB of an evaluated client component.
- *Don’t* specify the optional parameters (–s, –na, –ns) when you boot the server for normal operation. This is because the STARTUP.NCF, AUTOEXEC.NCF, and INITSYS.NCF files help initialize the server’s secure state.
- *Don’t* install arbitrary untrusted NLM executables.
- *Don’t* give the [Public] object any additional rights beyond those available in the standard distribution (that is, “out of the box”). Rights given to the [Public] object are available to all users on the network.
- *Don’t* give sensitive names to what is public information (such as usernames, container names, server names, E-mail addresses, people’s names, etc.).
- *Don’t* add unevaluated peripherals to the server hardware configuration.
- *Don’t* use workstations as queue servers or queue operators, unless the queue server is an evaluated part of a workstation component.
- *Don’t* install name space NLM programs that are not part of the NetWare Enhanced Security configuration. Consequently, only the DOS name space is supported on the server.
- *Don’t* use undocumented console operations, as they may place the server into an unevaluated configuration.

- *Don't* load NLM programs associated with the AppleTalk* Filing Protocol (AFP) or TCP/IP protocol suite.

- *Don't* use undocumented console operations, as they violate the server's NetWare Enhanced Security configuration

- *Don't* believe all telephone calls or email messages you receive. For example, the Computer Emergency Response Team (CERT) has documented cases of messages telling users to temporarily change their passwords to a certain value "for debugging purposes."

Promoting User Security Awareness

An important part of your job as a system administrator is promoting security awareness among your users.

NetWare Enhanced Security provides a *Security Features User Guide* that explains how to use the server's security features and addresses user security responsibilities. Users should be familiar with this document, but you should not fall back on telling them to "read the manual."

appendix W Network Composition Rules

The NetWare® 4.11 server is identified as a C2 IAD Si:Sa:Sn:Sn:Sb:Snp:Sn component. The C2 IAD rating refers to the server's ability to perform C2 Identification and Authentication (I&A, or "I"), Audit ("A"), and Discretionary Access Control (DAC, or "D").

The second part of the rating (Si:Sa:Sn:Sn:Sb:Snp:Sn) is a requirements vector that describes how the server can be installed with other components into a C2 network system. Table W-1 shows the elements of the vector along with the associated requirements.

Table W-1

Server Requirements Vector

Requirements	Vector	Nomenclature
IPX™ Source Address Validity	Si	IPX Accepting Server
RIP/SAP Advertising Validity	Sa	RIP/SAP Accepting Server
Protection of Communications Medium	Sn	Nonencrypting Server
Communication Between Untrusted Subjects	Sn	Nonfiltering Server
Protection of Authentication Materials	Sb	Server with Basic Credential
Object Reuse in Protocol Fields	Snp	Residual Data Nonprotecting Server
Administrative Control	Sp	Nonadministrative Server

The following items explain the general approach to determining if it is possible to add this server to a NetWare Enhanced Security network.

1. Obtain the Trusted Facility Manual (TFM) for each existing component in the network. The TFM contains

    - Each product’s requirements vector

    - Statements of permissible interactions with other components

2. Analyze the interactions between the server and each existing component. If the server will be the first component in the network, then there are no interactions, and the resulting network satisfies the NetWare Enhanced Security architecture. Each successive component must be added in accordance with the guidance provided in that product’s TFM.

3. The analysis involves looking at each of the seven requirements areas listed in Table W-1. Some of these areas focus on the server’s interactions with all other components in the internetwork, while other areas focus on the server’s interactions with all other components on the local network segment.

    A network segment is a collection of one or more LANs, possibly interconnected by bridges or routers, that shares a single IPX network number. Network segments are interconnected either by external router components or by the internal router within NetWare server components.

    The term *internetwork* refers to the global network system, that is, all servers, workstation, interconnection, and media components that make up a NetWare Enhanced Security system.

4. The server must be compatible with the existing configuration for all seven vector elements. If the server is not permitted for any one or more of these areas, then the server cannot be used in the proposed configuration. If the problem exists for a network segment, then the server can possibly be installed on a different network segment.

The following sections provide more specific guidance for the seven requirements areas.

IPX Source Address Validity

IPX source addresses are used by servers to tie a user's actions to a user workstation. However, some workstations do not provide TCB mechanisms to prevent untrusted software on the workstation from generating incorrect IPX addresses. For these workstations, servers and routers must provide mechanisms to check the IPX address generated by the workstation.

The NetWare 4.11 server is characterized as an IPX Accepting Server (Si) with respect to IPX source address validity. Conformance of the server for this requirement is determined as follows:

1. Identify the network segment where you intend to install the server.

2. Acquire the requirements vector and TFM guidance for all components currently installed on the network segment.

3. For each existing component on the local network segment, review the component's TFM guidance to verify that it permits an Si server on the same network segment with that component.

4. Further, determine that each existing component is permitted on the same network segment as the Si server. The first element of each component's vector must be either Wi, Si, Sm, Se, Ri, Rm, or Re.

5. If the server is permitted for each component (Step 3) and each component is permitted for the server (Step 4), then the network segment conforms to the architecture for IPX source address validity.

6. If the server is to be physically connected to multiple network segments (that is, the server will operate as a router between network segments), then the server is an Si server for each of the network segments. Thus, each of the network segments must conform with Steps 1 through 5.

RIP/SAP Advertising Validity

The Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) are used to broadcast network configuration data throughout the network.

Some workstations do not provide TCB mechanisms to prevent untrusted software on the workstation from broadcasting these configuration messages. For these workstations, servers and routers must provide mechanisms to prevent the distribution of these messages to other components.

The NetWare 4.11 server is characterized as a RIP / SAP Accepting Server (Sa) with respect to RIP / SAP Advertising Validity. Conformance of the server for this requirement is determined as follows:

1. Identify the network segment where you intend to install the server.

2. Acquire the requirements vector and TFM guidance for all components currently installed on the network segment.

3. For each existing component on the local network segment, review the component's TFM guidance to verify that it permits an Sa server on the same network segment with that component.

4. Further, determine that each existing component is permitted on the same network segment as the Sa server. The second element of each component's vector must be either Wo, Wio, Sa, Si, Ra, or Ri.

5. If the server is permitted for each component (Step 3) and each component is permitted for the server (Step 4), then the network segment conforms to the architecture for RIP / SAP advertising validity.

6. If the server is to be physically connected to multiple network segments (that is, the server will operate as a router between network segments), then the server is an Sa server for each of the network segments. Thus, each of the network segments must conform with Steps 1 through 5.

Protection of Communications Medium

To prevent passive and active wiretapping of information on network media, NetWare Enhanced Security requires protection of the communications medium using either physical/procedural methods, end-to-end encryption, or link encryption.

The NetWare 4.11 server is characterized as a Nonencrypting Server (Sn) with respect to Protection of Communications Medium. Conformance of the server for this requirement is determined as follows:

1. Identify the network segment where you intend to install the server.

2. Acquire the requirements vector and TFM guidance for all components currently installed on the network segment.

3. For each existing component on the local network segment, review the component's TFM guidance to verify that it permits an Sn server on the same network segment with that component.

4. Further, determine that each existing component is permitted on the same network segment as the Sn server. The third element of each component's vector must be either Wn, Sn, or Rn.

5. If the server is permitted for each component (Step 3) and each component is permitted for the server (Step 4), then the network segment conforms to the architecture for Protection of Communication Medium.

6. If the server is to be physically connected to multiple network segments, then the server is an Sn server for each of the network segments. Thus, each of the network segments must conform with Steps 1 through 5.

Communication Between Untrusted Subjects

The NetWare Enhanced Security architecture does not permit communications between untrusted client workstations. There are a variety of methods for preventing these associations, including router- and server-based based filtering of packets from a workstation on one network segment to a workstation on a different network segment.

The NetWare 4.11 server is characterized as a Non-Filtering Server (Sn) with respect to preventing the flow of packets between workstations. Conformance of the server for this requirement is determined as follows:

1. Identify the network segment or segments where you intend to install the server.

2. Acquire the requirements vector and TFM guidance for all components currently installed on each network segment.

3. If the server is to be installed on a single network segment, then the server is irrelevant with respect to this requirement and no further analysis is required for this requirement.

4. If the server is to act as a router between multiple network segments, then the server may be required to perform filtering of workstation-to-workstation communications. Perform the following analysis for each network segment connected directly to the server:

   a. For each workstation component on the network segment, review that workstation's TFM guidance to verify that the workstation does not depend upon a filtering router to help enforce the requirement. If the workstation requires a RiL router or an SiL server for all routing, then the Sn server cannot be used.

   b. Further, review the existing workstation types on the network segment. The fourth element of each workstation's vector may be any type other than WiR, WoR, or WioR.

   c. If the server is permitted for each workstation on each segment (Step 4a) and each workstation is permitted for the server (Step 4b), then the server can be used as a router between segments.

Protection of Authentication Materials

Protocol stacks that run within untrusted user sessions have access to the user's password and a credential and signature that can be subsequently used for background authentication. NetWare Enhanced Security provides various approaches to protecting these authentication materials.

The NetWare 4.11 server is characterized as a Server with Basic Credential (Sb) with respect to Protection of Authentication Materials. The architecture defines various types of workstations (for example, Wt, We, and Wn) and servers (Sb, Se, Ss, Sbe, Sbs, Ses, and Sbes). Any of these component types are permitted on an internetwork with any other component type. Provided all components are evaluated, no further analysis is required.

Object Reuse in Protocol Fields

Some versions of NetWare server software may not provide object reuse protection for packets generated by the server. That is, the server may send short packets to a workstation that are padded with residual data from another user's session. The architecture provides various methods to ensure that this residual data is not made available to another user at a client workstation.

The NetWare 4.11 server is characterized as a Residual Data Nonprotecting Server (Snp) with respect to this requirement. Conformance of the server for this requirement is determined as follows:

1. Acquire the requirements vector and TFM guidance for all workstations within the internetwork.

2. For each workstation on the internetwork, determine that the workstation provides mechanisms to overwrite any residual data in short packets from the server. That is, the sixth element of each workstation's vector must be type Wp.

3. Further, review each workstation's TFM guidance to verify that the workstation can interoperate with a type Snp server.

4. If each workstation is permitted for the server (Step 2) and the server is permitted for each workstation (Step 3), then the server can be added to the network.

5. If all workstations do not provide the necessary support for the server (Step 4), then acquire the requirements vector and TFM guidance for all routers and servers on the local network segment. These routers and servers may provide mechanisms to overwrite any residual data in short packets.

6. For each router / server on the local network segment that provides routing to another network segment, determine that the router or server overwrites any residual data in server packets. That is, the sixth element of the router or server must be Rp or Sp.

7. Further, review each review each router's or server's TFM guidance to verify that the component can interoperate with a type Snp server.

8. If each router / server is permitted for the Snp server (Step 6) and the server is permitted for each router / server (Step 7), then the Snp server can be added to the network.

Administrative Control

The NetWare 4.11 server is characterized as a Nonadministrative Server (Sn) with respect to the Administrative Control requirement. Conformance of the server for this requirement is determined as follows:

At least one workstation or server component on the internetwork must provide the capability for administrative management of NetWare Enhanced Security server file systems, NDS^{TM} objects, NDS object properties, NDS partitions, auditing, and print servers.

1. Acquire the requirements vector and TFM guidance for all workstation and server components in the internetwork.

2. Determine that at least one component is capable of providing administrative control. That is, the seventh element of at least one other component must be either Wa or Sa.

Trademarks

Novell Trademarks

Internetwork Packet Exchange and IPX are trademarks of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE/2-32 is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NetSync is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Asynchronous Communication Services and NACS are trademarks of Novell, Inc.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Directory Services and NDS are trademarks of Novell, Inc.

NetWare DOS Requester is a trademark of Novell, Inc.

NetWare I/P is a trademark of Novell, Inc.

NetWare Link Services Protocol and NLSP are trademarks of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NetWare Management Agent is a trademark of Novell, Inc.

NetWare MHS is a trademark of Novell, Inc.

NetWare Name Service is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Peripheral Architecture is a trademark of Novell, Inc.

NetWare Runtime is a trademark of Novell, Inc.

NetWare SFT III is a trademark of Novell, Inc.

NetWare SQL is a trademark of Novell, Inc.

NetWare Storage Management Services and NetWare SMS are trademarks of Novell, Inc.

NetWire is a registered service mark of Novell, Inc. in the United States and other countries.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Novell DOS is a trademark of Novell, Inc.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Sequenced Packet Exchange and SPX are trademarks of Novell, Inc.

SFT III is a trademark of Novell, Inc.

Storage Management Services and SMS are trademarks of Novell, Inc.

UNIX is a registered trademark of Novell, Inc. in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Virtual Loadable Module and VLM are trademarks of Novell, Inc.

Third-Party Trademarks

AppleTalk is a registered trademark of Apple Computer, Inc.

ARCnet is a registered trademark of Datapoint Corporation.

Btrieve is a registered trademark of Btrieve Technologies, Inc.

DynaText is a registered trademark of Electronic Book Technolgies, Inc.

IBM is a registered trademark of International Business Machines Corporation.

IPC is a trademark of Sun Microsystems, Inc.

LAN Manager is a trademark of Microsoft Corporation.

Macintosh is a registered trademark of Apple Computer, Inc.

Microsoft is a registered trademark of Microsoft Corporation.

MS-DOS is a registered trademark of Microsoft Corporation.

NDIS is a rademark of PC-Plus Communications LP.

NFS is a registered trademark of Sun Microsystems, Inc.

OS/2 is a registered trademark of International Business Machines Corporation.

PostScript is a registered trademark of Adobe Systems Incorporated.

Presentation Manager is a trademark of International Business Machines Corporation.

SAA is a registered trademark of International Business Machines Corporation.

Windows is a registered trademark of Microsoft Corporation.

Windows 95 is a trademark of Microsoft Corporation.

Windows NT is a trademark of Microsoft Corporation.

XENIX is a registered trademark of Microsoft Corporation.

XNS is a trademark of Xerox Corporation.

User Comments

We want to hear your comments and suggestions about this manual. Please send them to the following address:

Novell, Inc.
Documentation Development
MS C-23-1
122 East 1700 South
Provo, UT 84606
U.S.A.

Fax: (801) 861-3002

NetWare 4.11
NetWare Enhanced Security Administration
Part #100-003611-001 A
September 1996

For technical support issues, contact your local dealer.

Your name and title: ________________________________

Company: ________________________________

Address: ________________________________

____

____

Phone number: ____________________ Fax: ____________________

I use this manual as ❑ an overview ❑ a tutorial ❑ a reference ❑ a guide ❑ ____________

	Excellent	Good	Fair	Poor
Completeness	❑	❑	❑	❑
Readability (style)	❑	❑	❑	❑
Organization/Format	❑	❑	❑	❑
Accuracy	❑	❑	❑	❑
Examples	❑	❑	❑	❑
Illustrations	❑	❑	❑	❑
Usefulness	❑	❑	❑	❑

Please explain any of your ratings: ________________________________

____

____

____

____

In what ways can this manual be improved? ________________________________

____

____

____

____

You may photocopy this comment page as needed so that others can also send in comments.