

Chapter
1

INTRODUCTION

*Get on the
Fast Track!*



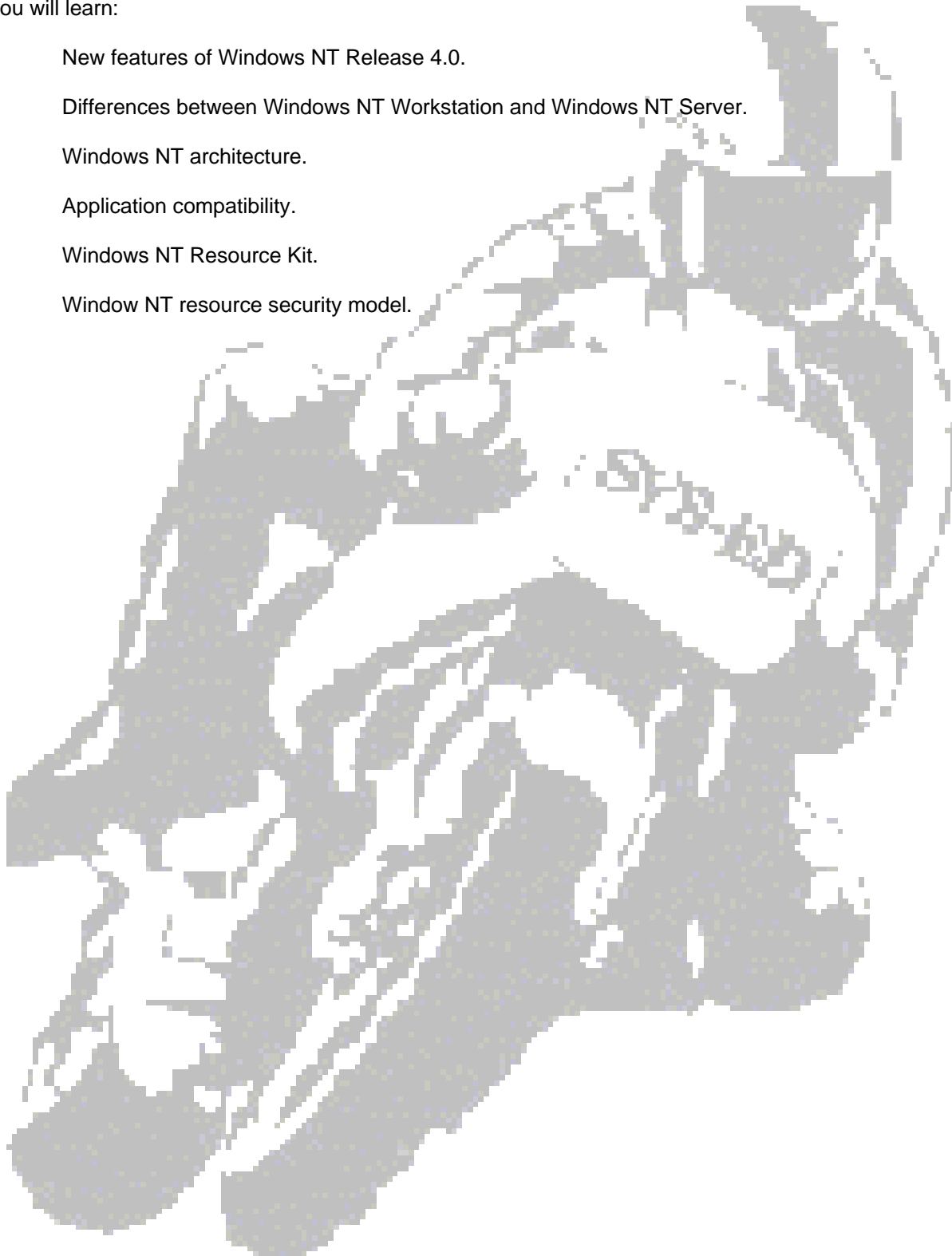
TM

**SYS-ED/
COMPUTER
EDUCATION
TECHNIQUES, INC.**

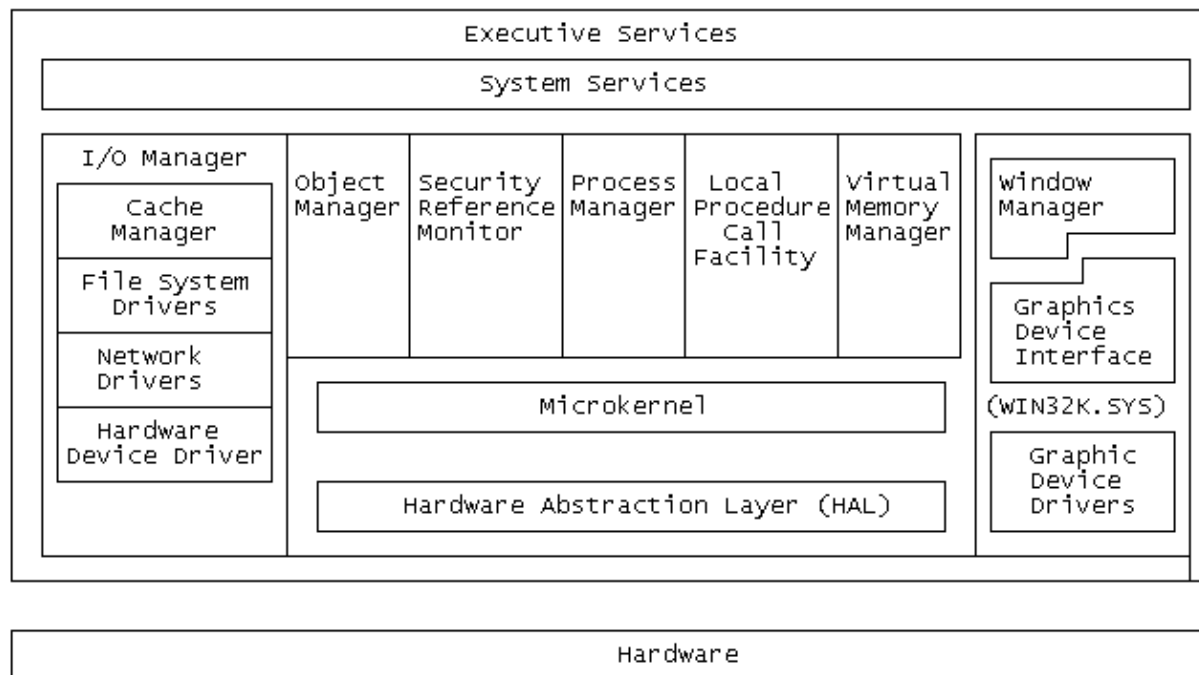
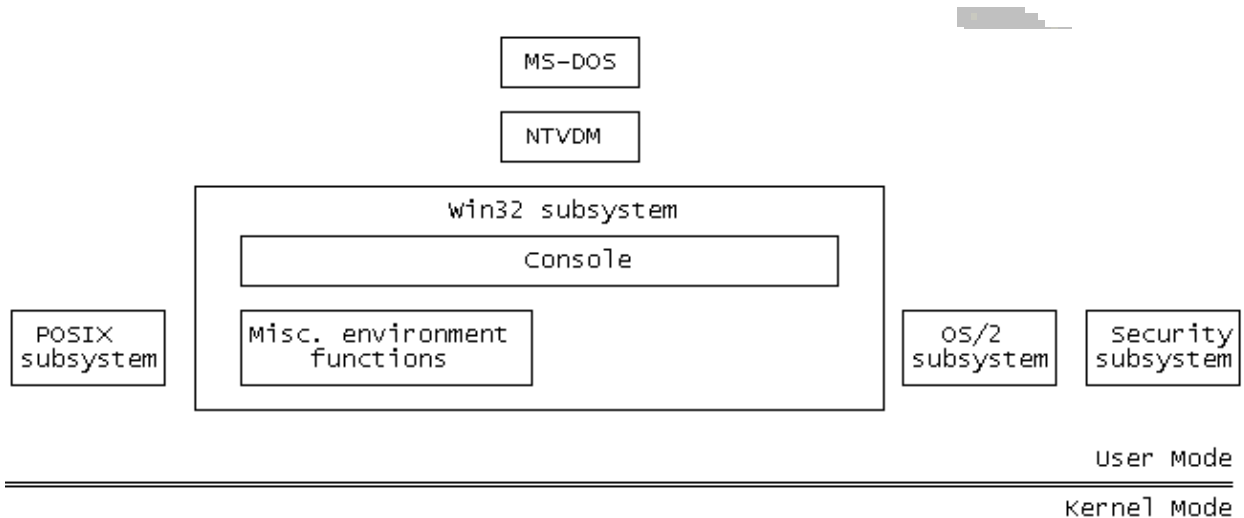
Objectives

You will learn:

- C New features of Windows NT Release 4.0.
- C Differences between Windows NT Workstation and Windows NT Server.
- C Windows NT architecture.
- C Application compatibility.
- C Windows NT Resource Kit.
- C Window NT resource security model.



1 Architecture



2 Workstation versus Server

There are two versions of Windows NT:

Workstation	Windows NT is designed for user workstations, but can also effectively act as a server for relatively small workgroups of up to 25 nodes.
Server	Windows NT Server is optimized to serve large workgroups and domains, and includes additional features not included with Windows NT Workstation, such as the Internet Information Server.

Functionality	Windows NT Server	Windows NT Workstation
Symmetric Multiprocessor Support (SMP)	Four processors supported in the shipping version	Two processors supported in the shipping version
Network Connections Support	No limit on connections	As a server, limit of 10 client connections
Apple Macintosh Services Support	Built-in	Not supported
Disk Fault Tolerance Features	RAID levels 1 and 5	Not supported
Domain Logon Authentication	Built-in	Not supported
Remote Access Services	Up to 256 simultaneous remote connections	Limit of one remote connection
Directory Replication Services	Can act as an importer and exporter	Can only act as an importer
Microsoft BackOffice Server Products Platform	Built-in	Not supported

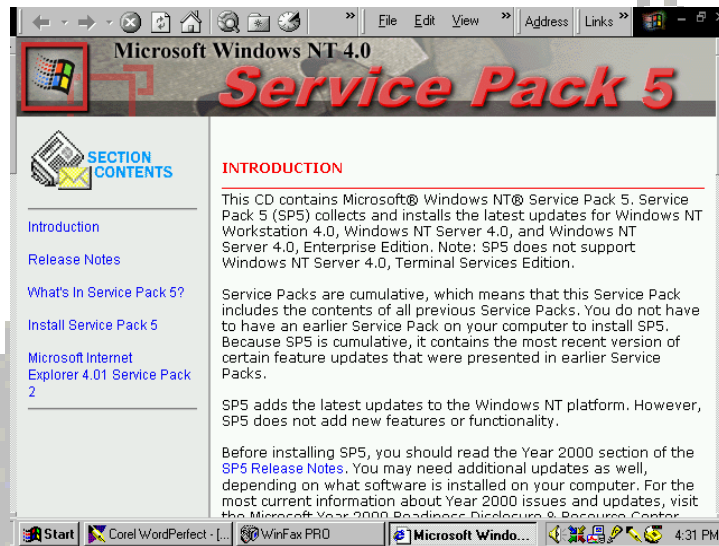
Although you can run the same types of programs under Windows NT Server as can be run under Windows Workstation, the additional overhead in Server can lessen program performance. Using a server as a workstation also limits its performance as a server.

Each product has to be purchased separately.

Service Pack

The current service packs for Microsoft Windows NT Workstation 4.0 and Windows NT Server 4.0 are Service Pack 5 and 6.

The Service Pack changes only those files that were originally set up on the Windows NT Workstation or Windows NT Server system. Service Pack releases are cumulative; they contain all previous fixes and any new fixes made to the system.



```
Volume in drive Z is NT4_SP5
Volume Serial Number is 35E3-13C7
```

```
Directory of Z:\
```

```
04/29/99 12:04p <DIR> .
04/29/99 12:04p <DIR> ..
04/29/99 12:04p <DIR> ALPHA
04/29/99 12:04p 146 AUTORUN.INF
04/29/99 12:04p <DIR> BIN
04/29/99 12:04p 0 DISK1
04/29/99 12:04p <DIR> DRVLIB
04/29/99 12:04p <DIR> GIFS
04/29/99 12:04p <DIR> I386
04/29/99 12:04p <DIR> MSIE401
04/29/99 12:04p <DIR> MSSCE
04/29/99 12:04p 1,178 NT4SP5.PDF
04/29/99 12:04p 230 NTSP.INI
04/29/99 12:04p 8,594 NTSP5.HTM
04/29/99 12:04p 106,676 README.TXT
04/29/99 12:04p 45,275,986 SP5ALPHA.EXE
04/29/99 12:04p 34,548,334 SP5I386.EXE
04/29/99 12:04p 0 SPCDROM.40
04/29/99 12:04p 250 SPSETUP.BAT
04/29/99 12:04p <DIR> SUPPORT
20 File(s) 79,941,394 bytes
0 bytes free
```

Directory PATH listing for volume NT4_SP5
volume serial number is 0012FC94 35E3:13C7
Z:.

```
├──ALPHA
│   └──UPDATE
├──BIN
│   ├──ALPHA
│   └──I386
├──DRVLIB
│   ├──NETCARD
│   │   └──X86
│   │       ├──3C59X
│   │       ├──E100B
│   │       └──NETFLX3
│   ├──PNPISA
│   │   ├──ALPHA
│   │   │   ├──SYMBOLS
│   │   │   └──SYS
│   │   └──X86
│   │       ├──SYMBOLS
│   │       └──SYS
│   ├──STORAGE
│   │   ├──CPQFCALM
│   │   └──I386
│   └──VIDEO
│       └──X86
│           └──S3VIRGE
├──GIFS
├──I386
│   └──UPDATE
├──MSIE401
│   ├──ALPHA
│   └──I386
├──MSSCE
│   ├──ALPHA
│   │   └──SYMBOLS
│   ├──I386
│   │   └──SYMBOLS
├──SUPPORT
│   ├──DEBUG
│   ├──MCIS2.0
│   │   ├──ALPHA
│   │   │   ├──SYMBOLS
│   │   │   └──DLL
│   │   └──I386
│   │       ├──SYMBOLS
│   │       └──DLL
│   ├──MSMQ.95
│   ├──MSMQ.NT
│   │   ├──ALPHA
│   │   └──I386
│   ├──OEMTOOLS
│   │   ├──ALPHA
│   │   └──I386
│   ├──PRINTERS
│   │   ├──ALPHA
│   │   └──I386
│   ├──RRAS
│   │   ├──ALPHA
│   │   └──I386
│   ├──TCP32WFW
│   ├──UTILS
│   │   ├──ALPHA
│   │   └──I386
│   └──WINNT32
│       ├──ALPHA
│       └──I386
```

3 Application Compatibility

Out of necessity to support a large installed base and enhance the appeal of Windows NT, Microsoft built support into Windows NT for DOS and 16-bit Windows programs. Microsoft also added POSIX support to Windows NT, however, support for OS/2 applications has been dropped.

In general, Windows NT can run DOS programs and 16-bit Windows programs written for Windows 3.x (a.k.a. Win16 programs). Many Win16 programs run equally well under Windows NT or Windows 3.x. Some Win16 programs, however, do not run under Windows NT. In particular, Win16 programs that require private virtual device drivers (VxDs) will not run under Windows NT.

Programs that conform to the Windows 95 compatibility logo requirements also run under Windows NT, so most Windows 95/98 programs will run fine under Windows NT.

It is also possible to connect to <http://msdn.microsoft.com/library/winresource/dnwinnt/S85DC.HTM> for additional information on hardware and software compatibility.

4 C-2 Security

The National Computer Security Center (NCSC) is the United States government agency responsible for performing software product security evaluations. These evaluations are carried out against a set of requirements outlined in the NCSC publication Department of Defense Trusted Computer System Evaluation Criteria, which is commonly referred to as the Orange Book. Windows NT has been successfully evaluated by the NCSC at the C2 level as defined in the Orange Book.

Because Windows NT supports C2 Level security, the workstation must be configured appropriately to apply this. Additionally, Windows NT supports security features that are not required to meet C2 Level security. The Windows NT C2 Security System Administrators Guide provides information on how to define and implement security on your system and should be reviewed for more information. Windows NT adheres to many of principles underlying C2-level security.

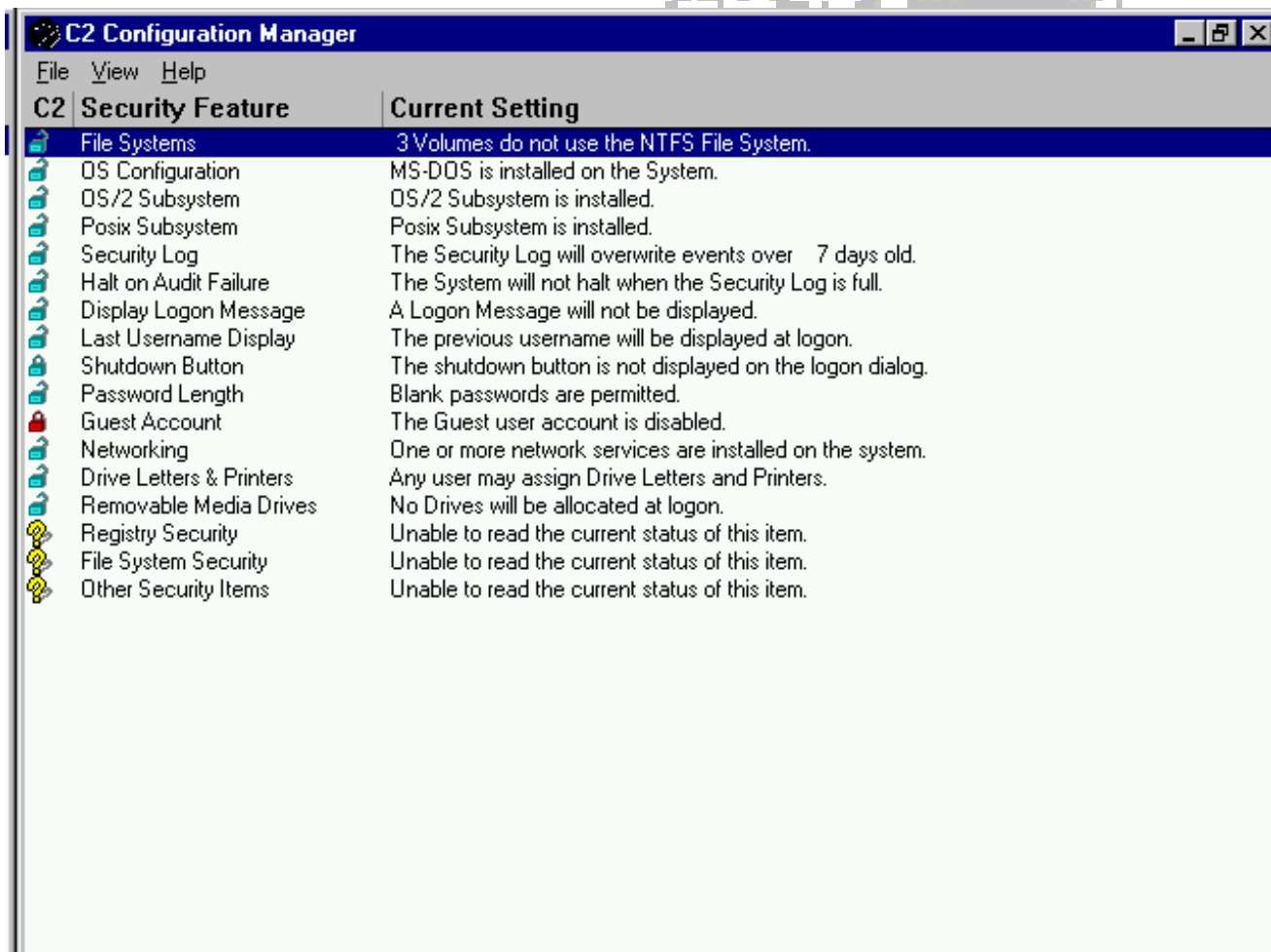
A C2-level system such as Windows NT must support the following security features:

Security Feature	Explanation
Secure Logon	Users must identify themselves with a user name and password to gain access to the system. Unlike Windows for Workgroups and Windows 95, a user must have a logon account and password created on the system by an administrator. A user cannot create his/her own logon on-the-fly.
Discretionary Access Control	The owner of a resource determines which other users, if any, can gain access to the resource. When a user creates a file, the user determines who else can access the file, and what level of access (read, modify, etc.) that others have to the file.
Auditing	The system must track and record events relating to the security of the system and access to resources.
Memory protection	Applications, files, another resources must be protected from one another to prevent unauthorized access across the network.

4.1 Windows NT C2 Configuration Manager

Windows NT C2 Configuration Manager is used to help configure the security of a Windows NT Workstation or Windows NT Server. The C2 Configuration Manager may be used to change one or more security attributes on the system.

Refer to the Windows NT Administration documentation for more information on what the correct settings are for the desired security level as well as for more information on defining and implementing a security policy.

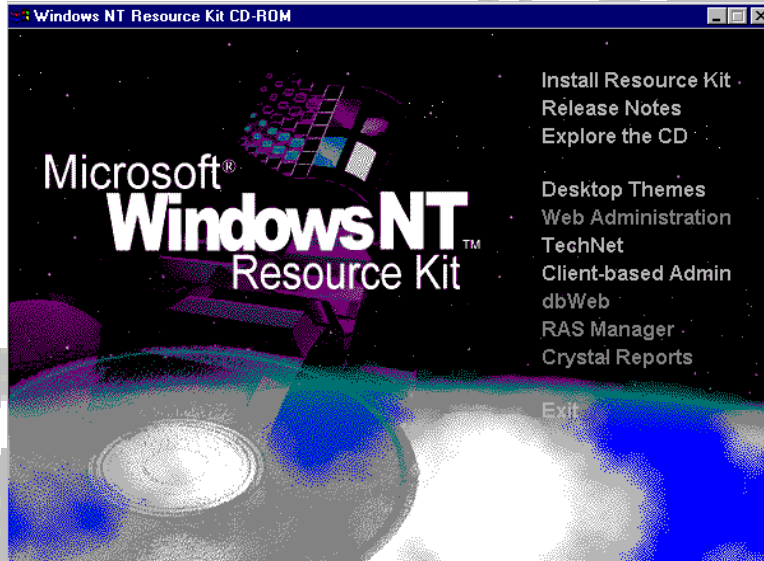


5 Resource Kit

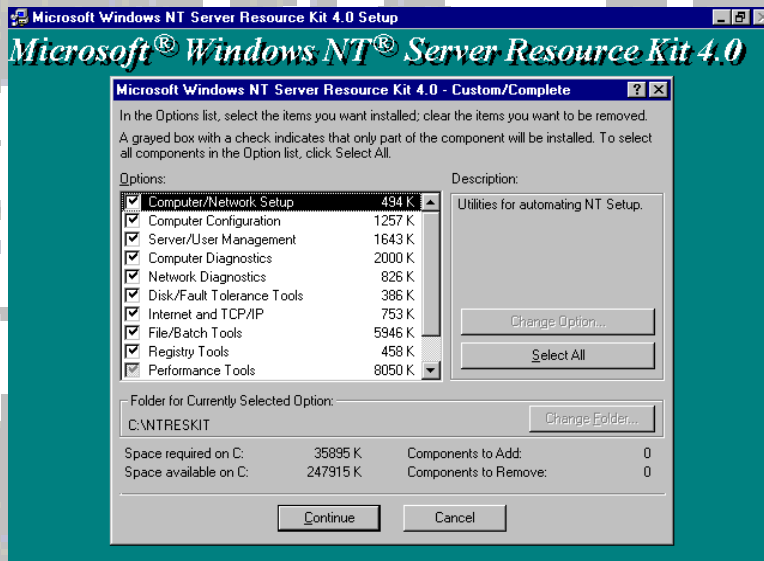
The Windows NT Resource Kit is not distributed as a standard part of the Windows NT Server or Workstation products. It contains a variety of on line documents, updates and utilities.

Separate Microsoft Resource Kits are sold for both Windows NT Workstation and Windows NT Server.

Windows NT Workstation Resource Kit



Windows NT Server Resource Kit



6 Interactive and Remote Logon

Two logon processes can start logon authentication:

- C Interactive Logon
- C Remote Logon

6.1 Interactive Logon Authentication

Interactive logon occurs when the user types information in the Logon Information dialog box displayed by the computer's operating system. In Domain, the user selects either the name of a domain or the name of the computer being logged on to is being defined.

If the computer is a member of a workgroup and not of a domain, the Logon Information dialog box does not have a place for typing in the domain name.

Computer is in	User can logon at	Unique Identifier
Workgroup	Local database	Computername and username
Domain	Local database	Computername and username
	Domain database	Domain name and username
Domain with a trust relationship	Local database	Computername and username
	Home domain database	Domain name and username
	Trusted domain database	Trusted-domain name and username
Domain without a trust relationship	Local database	Computername and username
	Domain database	Untrusting-domain name and username

- C The unique identifier used by Windows NT after logon depends on the location of the database used to log on the user.
- C The third column in this table describes the unique identifier used in each case. Any network connection requests sent elsewhere on the network include this unique identifier.

6.2 Remote Logon

Remote Logon takes place when a user already logged on to a user account makes a network connection to another computer. For example, the user connects to another computer using the MAP NETWORK DRIVE dialog box or the net use command.

A security-access token created at interactive logon is assigned to the initial process created for the user. When the user tries to access a resource on another computer, the remote server authenticates the user again and creates a security access token for the user.

The security-access token is placed in a table stored on the remote server. The server creates a user identifier (UID) for the user and maps it to the user's security -access token. This UID is sent back to the client redirector and is used in all further server-message-block (SMB) communication between the server and client. Subsequently, whenever a request for any resource on that server (and not just in the same share) comes in from the client, the UID identifies the user to the server process. The server checks the table and uses the security access token stored for the UID.

6.3 Logon Caching

If a domain controller for your domain can not be contacted, you will be logged on using cached account information.

Changes to your profile since you last logged on may not be available.

6.4 Net Logon Service and Pass-Through Authentication

The Net Logon function is what allows a user from a trusted domain to log on and validate at a computer belonging to the trusting domain.

When the user logs on at a computer belonging to the trusted domain, the From box on the NT Welcome screen displays not only the trusting domain as a valid domain option, but also any trusted domains that have been set up.

Example:

Domain A trusts Domain B.

Domain A is therefore the trusting domain and Domain B is the trusted domain. UserB is a member of Domain B. When UserB tries to log on to an NT computer that belongs to Domain A, when he selects the From box on the NT Welcome screen, he/she will see a choice for both Domain A and Domain B.

By selecting Domain B, the Net Logon service determines that this account cannot be validated by a domain controller for Domain A. Therefore, the request is passed through the trust to Domain B where it can be validated by a domain controller for that domain. Once UserB is validated, the user's access token information is returned to the computer at which he is logging on.

Once the trust has been established, resource managers in the trusting domain can create ACLs for their resources by adding accounts from their own domain, as well as from the account database on the trusted domain. So if UserB from DomainB needs access to a resource in Domain A, the resource manager for the resource in Domain A can add UserB to the ACL for the Domain A resource by virtue of the trust. In addition, the trust gives UserB the ability to log on to a computer that is a member of Domain A and still access the same set of network resources.

7 Windows NT Resource Security Model

Windows NT protects its resources, including files, printers, and applications by controlling access to them.

There are two basic approaches to resource security.

- C An access code can be associated with each resource.
Any user who knows the code receives access.

- C A user can be associated with each resource.
Any user who is granted permission to the resource receives access.

In Windows NT, users are associated with a resource.

Everything in Windows NT is represented to the operating system as an object. Access to each object is controlled through an Access Control List (ACL).

7.1 Access Control Lists

The ACL contains the user (and group) accounts that have access and permissions to an object.

When a user wants to access an object, the system checks the user's security identifier and group memberships with the ACL to determine whether this user is allowed to complete the request.

7.2 Access Control Entries

Every user of the system must have a user account, which can be added to resource access control lists. This includes applications and services which need to access resources as well as people.

When an administrator grants access to a resource, the user account is added to the ACL for that resource, along with any specific permissions.

These ACL entries are called Access Control Entries (ACEs). Each entry identifies a user or group and the permissions that have been granted or denied for the object. An ACE is added to the ACL for each user or group that is granted or denied access to an object.

Entries that deny access are listed first in the ACL, and entries that permit access are listed next. The only time this order is changed is when an organization has written its own application which edits the ACL of a resource. In this case, the ACE can be placed anywhere in the ACL.

7.3 Mandatory Logon

Windows NT requires each user to provide a unique username and password to log on to a computer. This mandatory logon process cannot be disabled.

The benefits of mandatory logon and using CTRL+ALT+DEL to start the logon process are:

- C The mandatory logon procedure provides a way to identify authorized users and determine whether they are allowed to log on and have access to system resources.
- C Access to user mode programs is suspended during mandatory logon. This makes it impossible for someone to create an application that steals the user's logon name and password.
- C The mandatory logon process permits user to have individual configurations, including desktops, and network connections that are automatically saved and restored each time the user logs on. Two or more people can use the same computer and still retain their own custom setting.

7.4 Logging on and Access Tokens

When a user logs on to Windows NT, the security subsystem creates an access token for the user. The access token includes information such as the user's name and the groups to which the user belongs. Access to the system is allowed after the user has received this access token.

The Process of Receiving an Access Token

1. The Win32 WinLogon process presents a dialog box requesting a username and password. This information is passed to the Security Accounts Manager.
2. The Security Accounts Manager queries the security accounts database to determine whether the specified username and password belong to an authorized system user.
3. If the access is authorized, the security subsystem constructs an access token and passes it back to the Win32 WinLogon process.
4. WinLogon calls the Win32 subsystem to create a new process for the user, passing the access token to the subsystem. Win32 attaches the token to the newly created process.

When a user's process attempts to access any object, Windows NT checks the user ID and list of groups in the access token of the user process against the object's ACL.

This check determines whether the user is granted the requested access to the object. The access token is permanently attached to each of the user's processes and serves as each process's "identify card" whenever it attempts to use system resources.

Access tokens are objects and have attributes and services like any other system object.

Some attributes and services in an access token include:

Attribute	Description
Security ID	The security identification for the user who is logged on.
Group IDs	The groups to which the user belongs.
Privileges	The privileges for this user.

7.5 Security IDs

Windows NT stores user and group identifications in the form of a Security Identifier (SID) and group Security Identifiers (group SIDs).

A SID is a unique identifier used to represent a user, group, or some, type of security authority. SIDs are used within access tokens and ACLs instead of usernames or group names.

A SID is represented as a unique number, such as:

S-1-5-21-76965814-1898335404-322544488-1001

Caveat

The result of identifying users by SIDs is that the same user account name could have been created multiple times on the same computer, but each instance of the account name will have a unique SID.

For example, there is a user account for User-1. If this account is deleted and a new account is created for User-1 using the same name, the new account will not have access to the same resources as the old account. This is because the SID will be different, even when the account name is the same.

User access tokens are regenerated each time a user logs on to the system, and they are not updated after they have completed the logon process.

Therefore, if an administrator adds User-1 to a new group after User-1 has already logged on to the system, User-1 must log off and log on again so that a new access token is generated with the new group membership.

7.6 Checking Permissions

Windows NT compares the information in the access token to the information in the ACL to determine whether access should be granted. When a user attempts to access a resource on the system, the security subsystem compares the user's access token to the ACL to validate or deny the requested permission to the resource.

The security subsystem goes through the following steps:

1. Starting at the top of the ACL, it checks each entry (ACE) to see whether it explicitly denies the user or any of the groups that appear in the user's access token the type of access that is being requested.
2. It checks to see whether the type of access requested has been explicitly granted to the user or any of the groups in the user's access token.
3. It repeats steps 1 and 2 for each entry in the ACL until it either encounters a deny or has accumulated all the necessary permissions to grant the requested access.
4. If a grant does not appear in the ACL for each of the requested permissions, the user is denied access.

7.7 Optimizing Permission Checking

When Windows NT grants access to an object, it is actually giving the user's process a pointer (handle) to the object. A handle is an identifier used internally by the system to identify and access a resource. The system also creates a list of allowed permissions called the list of granted access rights. This information is then stored in the user's process.

An ACE is checked only when the object is initially opened. Subsequent actions performed on an opened object are checked against the list of granted access rights that was stored in the user's process table for that handle.

If a UserID needs to write to the file, the process uses the handle previously granted to check for Write privileges. This is much faster than checking the ACE for every access.

The list of granted access rights reflects the state of the object's ACE at the time a handle to the object is opened. After the granted access rights have been determined, the process retains these rights until it closes the handle to the object.

If an object's ACE is changed while a process has an open handle, the change does not affect the process's access rights until the handle is closed and then reopened.

By default in Windows NT, each time a user presses CTRL+ALT+DEL to bring up the logon dialog box, it displays the username of the last person to log on to the system. If this is undesirable, a Registry parameter can be set to prevent display of the last username that logged on to the system.