NICs
Network Information Connection, a Technical e-Journal

Test Prep: Integrating Netware and Windows NT Exam

by **Steve**Crowley

The Novell test #644 Integrating Netware and Windows NT is the exam that has just replaced the retired #636 test. My experience, and that of our students, has shown that Exam Essentials from http://www.certify.com/ proved very useful. You can download the practice exams with 278 questions for just under $60.00, which is well worth it.

Another resource that has proven useful is a practice exam CD from the Test Out corporation located in Pleasant Grove, Utah. They offer practice exams for all the Novell as well as the Microsoft tests. They also offer a money back guarantee if you don't pass the exam after using their software. They can be found at http://www.testout.com/. Several of our students have also used their software with good success.

Another great resource is from www.cramsession.com. This site provides concise and to the point helps for what to know for the test. I have included the cramsession for this test in the following pages. You should have no trouble passing the test using the aforementioned resources. Good Luck.

Integrating NetWare and Windows NT: Cramsession

Windows NT Workstation 4.0 provides the following features:

1. Supports preemptive multitasking for all applications.
2. Supports multiple processors.
3. Provides local security for files, folders, printers, and other resources if the NTFS file system is used.
4. Supports each application in its own memory address space.
5. Can be used with the Microsoft BackOffice product family.
6. Provides better performance for processor-intensive applications.
7. Minimum hardware requirements are listed below:
   - Intel-based 486 processor or a RISC-based Alpha, MIPS R4X00, or PowerPC TM processor
   - 16 MB of RAM
   - 120 MB of available hard disk space

The Administrator has complete administrative control over the system. Some of the tasks that the Administrator can perform include:

1. Management of security policies.
2. Modification of operating system software.
3. Ability to create and connect to shared directories.

Integrating Netware and Windows NT Exam

Exam Number	#050-644
Exam Status	Available
Passing Score	608
# of Questions	66
Time Allotted	90 minutes
Certifications	NetWare 4.11 CNE

Official Site

http://education.novell.com/testinfo/objectives/555btobj.htm

Institute for Network Professionals

4. Ability to install and connect to printers.
5. Ability to partition and format a disk. The Administrator account can be renamed, but not deleted.

For increased security, you should rename the Administrator account.

Windows NT	
Server	provides an unlimited number of concurrent client connections (inbound and outbound).
	supports up to 256 RAS sessions.
Workstation	supports ten inbound and an unlimited number of outbound connections.

The initial user account is assigned a name during installation and has all administrator rights and privileges. It can be renamed and deleted, but not disabled.

The initial user is not created if the Windows NT Workstation is added to a workgroup or domain during installation.

These default groups are created when Windows NT workstation is installed on a computer:

- Power Users
- Administrators
- Backup Operators
- Users
- Guests
- Replicator

These default groups are created when Windows NT server is installed on a computer:

- Users
- Guests
- Replicator
- Server Operators
- Administrators
- Backup Operators
- Account Operators
- Print Operators

The default accounts that are created when you install NT workstation without network support are:

Administrator Used by the person who administers the computer's configuration

Guest Used by occasional or one-time users to log in with minimal privileges

Initial user (created only if Windows NT Workstation is installed without any networking options) Local user uses this account to manage his or her own computer resources and accounts

User Manager for Domains is used to:

- Manage profile or login scripts
- Manage security policies
- Create and manage user accounts
- Create and manage groups
- Establish tracked events by setting an auditing policy.

The Server Manager utility is used to manage computers and domains. You can use Server Manager when you want to:

- Display a list of users connected to a computer over the network
- Display shared and open resources
- Control directory replication
- Send messages to connected users
- Promote backup domain controllers to primary domain controllers
- Synchronize servers with the primary domain controller
- Add computers to and remove computers from a domain.

Use Network Neighborhood to:

- Connect to other computers on the network
- Establish drive mappings
- Connect to printers
- Browse the network for resources.

With Disk Administrator you can:

- Create and delete partitions
- Create and delete logical drives with an extended partition
- Format and label volumes
- Create and delete volumes
- Obtain information about disks, such as available space and partition size
- Change drive letter assignments
- Create and delete stripe sets.

The Windows NT Registry has these subtrees:

HKEY_LOCAL_MACHINE Contains all configuration data about the computer. Applications, device drivers, and the operating system use the data in this subtree. Some of the data is used during the Windows NT boot process to determine which device drivers to load.

HKEY_USERS Contains security information about all the users in the directory database and the system default settings for each user.

HKEY_CURRENT_USER Holds data about the user currently logged in. A copy of this subtree is stored for every user that has logged in to the machine.

HKEY_CLASSES_ROOT Holds information about softwareconfigurations.

HKEY_CURRENT_CONFIG Holds information about the active hardware profile.

Logon

When you click OK, the WinLogon process passes the username and password to the Local Security Authority (LSA) process.

The LSA queries the Security Accounts Manager (SAM) to verify that the username and password are valid for the local workstation.

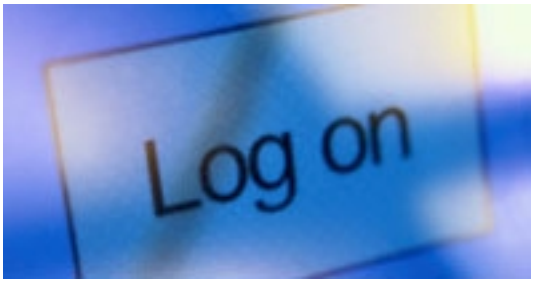
If the SAM verifies that the username and password are valid, the LSA creates an access token that contains information about that user's access rights and passes the token back to the WinLogon process.

The mandatory login process provides three advantages:

1. A user can have more than one account. Each account can allow different activities within the Windows NT security system.

2. Users can have profiles. Profiles include desktops, network connections, and other user-level preferences. Profiles are automatically saved and restored each time the user logs in.

3. Users can secure files on the local computer and prevent other local users from accessing those files, if the computer is configured with NTFS.



Permissions

Permissions are cumulative. If a user is a member of multiple groups and each group has been granted permissions to a specific directory, the user gets permissions from each group.There is an exception to this rule, however. If one of the groups that the user belongs to has been given the No Access permission, the user will not be able to access the directory, regardless of permissions granted through other group memberships.

The share permission hierarchy is as follows:

Full Control - Maximum abilities
Change
Read
No Access - Minimum abilities

The Change directory permission allows users to perform all tasks that the Read permission allows. Additionally, the Change permission gives users the ability to perform these tasks:

- Add files and subdirectories to the shared directory
- Change data in files
- Delete subdirectories and files
- Change file attributes.

Permissions granted on an individual file basis overwrite those granted at the directory. Therefore, the Change permission granted to a file takes precedence.

Users with Add and Read (RWX) (RX) permissions :

- View filenames and subdirectory names(read)
- Make changes to subdirectories in the directory(read)
- View data in files(read)
- Run applications(read)
- Add files and subdirectories to the directory(add).

Users with Change (RWXD) permissions:

- View filenames and subdirectory names
- Make changes to subdirectories in the directory
- View data in files
- Run applications
- Add files and subdirectories to the directory
- Change data in files
- Delete the directory and its files.

Shares are created in Explorer by right-clicking the directory you want to share and entering the appropriate information on the Sharing tab.When you share a directory, you provide all users on the network with access to the directory and all its subdirectories because the group Everyone gets full control by default.

Shares only affect remote users. You must use NTFS directory and file permissions to secure files locally. If the share is on a FAT volume, shares are the only security available. Permissions are set per directory and do not affect directories and files below the share point. Microsoft's recommended method of securing the file system is to give the group Everyone, Full Control permissions and apply NTFS directory and file permissions to limit user access.

Models

In the workgroup model, users share resources that are located on local machines. Each workstation can share files with other workstations. The workgroup model is a peer-to-peer networking arrangement that does not require a central server. Every workstation manages its own user accounts by maintaining a security database locally.

The disadvantages of the workgroup model are:

- Centralized administration cannot be used
- Inefficient for large #'s of workstations/ workstations not in close proximity to each other
- Each member of the workgroup has security responsibilities
- User on each workstation must create/maintain own user account in separate database
- File system backups are complicated and often unreliable.

The advantages of the domain model are:

- Centralized administration of users and security
- Single-point login for members of the domain
- Support for user groups larger than a workgroup.

Global groups facts:

- They are stored on domain controllers
- They contain users within the domain
- They can be used in other trusting domains
- They cannot contain other global or local groups.

System policies are used to control user-definable settings in user profiles and system configuration settings, and to restrict what users can do from the desktop. They are enabled and configured in the System Policy Editor utility. These policies include:

- Remove the Run command on the Start menu
- Disable Registry editing tools
- Show common program groups
- Hide the desktop
- Specify which programs execute automatically via the StartUp group
- Lock and unlock specific program groups
- Allow users to add and remove Print Manager connections
- Force users to wait for the login script to process before running any other applications.

Account policies allow you to set domain-level user security options such as:

- Maximum password age
- Minimum password length
- Minimum password age
- Lockout duration.

Account policies are set using User Manager for Domains.

User Rights Control what the user can do on the network
User Accounts Required to access the network resources
System Policies Control access to specific features in Windows NT User Profiles: Control users' working environments

Guidelines when implementing groups across domains include:

- Use the built-in global and local groups when possible. Determine if an existing group can perform the desired task or grant the desired rights before creating a new group.

• Create new user accounts and global groups on the primary domain controller of the trusted domain. Then assign the appropriate users to global groups for multidomain access.

• Create new local groups on the servers in the trusting domains. Assign the local group the needed user rights and resource permissions.

Trust relationships are established so that users can access resources outside the domain in which they reside. When creating a one-way trust relationship, the domain that contains the resources becomes the trusting domain and the domain that contains the user accounts becomes the trusted domain. The trusting domain is so called, because it trusts the users to access its resources. The trusted domain is so called, because its users are trusted by the trusting domain to access its resources. Trust Relationships are normally illustrated by arrows. Remember that the arrow always points to the trusted domain.

You can establish an unlimited number of outgoing trust (trusting) relationships. You can establish a maximum of 128 incoming (trusted) trust relationships for a Windows NT domain.

The multiple master domain model has the following advantages:

- Network administration can be centralized or decentralized.
- Domains can be configured to reflect a company's departmental organization.
- Users can use one account to log in from anywhere in the network.
- It meets the needs of mobile users by letting them log in from anywhere in the network.

The two main disadvantages of the complete trust model are:

- It requires complex administration of trusts because two way trust must be established between all domains.
- It is difficult to ensure the integrity of global groups used in domains outside of the administrator's control. Central administration of user accounts is not possible in the complete trust model. This can pose a security risk because each domain must rely on other domains not to place inappropriate users into global groups.

The single domain model allows you to manage the entire network as well as its users and resources by managing the master domain. You can also distribute resource management by allowing administrators in the resource domains to manage the resources in their domains. This model is appropriate in a company that has several departments and each department wants to administer its own resources, but user and group account management must be centrally administered.

Windows NT Workstation	Windows NT Server
Applications	Applications
SAMLIB.DLL	SAMLIB.DLL
RPC	RPC
	SAMSRV.DLL from Novell
	Novell Client for Windows NT

Applications needing access to information from the Windows NT domain make requests to SAMLIB.DLL. SAMLIB.DLL communicates with SAMSRV.DLL using remote procedure calls. SAMSRV.DLL accesses the Windows NT Security Accounts Manager (SAM) where the domain database is stored and performs the requested operation.

The Domain objects contains several property pages to manage the domain.

Identification Allows you to enter a description of the domain and specify a default context in which new users created in User Manager are located.

Members Allows you to view, add, or delete user access to the domain. (Does not allow you to move them to another domain)

Intruder Detection Allows you to specify intruder detection limits for the domain.

Replica Advisor Can help you decide how to partition the NDS tree and show you where to place replicas.

NT Tools Gives you access to NT tools from NetWare Administrator.

The Domain User Settings page is used to configure NT-only properties such as:

- Path to the user profile
- Workstations that the user may log on to.

Domain Access is used to:

- add or delete domain, group memberships
- set the user's primary group
- unlock the account when it is locked by intruder detection.

To install NDS for NT:

1. Log in to your Windows NT Server as Administrator
2. Launch WINSETUP.EXE at the server
3. Select the NDS for NT option
4. Accept the license agreement
5. Reboot the Windows NT Server to load Novell Client for Windows NT
6. The Domain Object Wizard will launch automatically to help you complete the rest of the installation.

You can integrate your NT domains in stages, but you must integrate all components in a domain at the same time. That is, if you install NDS for NT on the PDC for a domain, you must install NDS for NT on the BDCs for that domain at the same time.

After integration, you can use native Windows NT tools and utilities to manage NT.

Mailbox Manager for Exchange is a snap-in for NetWare Administrator. It allows you to use NetWare Administrator to create, edit, and delete Exchange mailboxes. Changes made in NetWare Administrator are automatically made on the Exchange server. However, changes made in Microsoft's Exchange Manager must be manually synchronized with NDS.

WINNT user packages contain the policies below:

- Dynamic local user
- NT desktop preferences
- NT User printer
- NT User system policies
- Workstation import policy.

Comments or Suggestions? E-mail webmaster@cramsession.com

Tips and Tricks

Kill Hung Processes When Logging Off

When you tell Windows NT to shut down, it first sends shutdown requests to any running processes. Most 32-bit applications honor these requests and shut down, but older 16-bit apps running in the Virtual DOS Machine often won't.

When this occurs, the operating system prompts you with a dialog box asking if you want to kill the task, wait for the task to die on its own, or cancel the shutdown.

You can automate this process by editing the registry, and force NT to kill all running processes on shutdown by adding a REG_SZ value named HKEY_USER\<SID>\ControlPanel \Desktop\ AutoEndTasks and set the value to 1. You can also add this value to HKEY_USERS \.DEFAULT so that all new accounts will shut down the same way.

Documenting your NetWare Servers

If in the process of troubleshooting a network problem, or in doing routine maintenance of your servers you find that the documentation is insufficient, it can add lengthy delays to the time that it would normally take to accomplish the task. You can avoid those delays for your NetWare Servers by using the console command REGISTER by typing

LOAD REGISTER –C <ENTER>

This will compile information such as

- Server Name
- Memory
- NIC address
- OS & revision
- Network Protocols
- Serial Number
- Volume Settings.

It will then put this information in a text file named *CONFIG.NFO* and put it in SYS:\SYSTEM. You can then use any text editor to view and print the information and put the documentation where it's available.

NICs
Network Information Connection

is published by the
Institute for Network Professionals

Prices Domestic $100/yr ($8.50 each)
Outside US $125/yr ($10.00 each)

Phone US 801 223 9444
Fax 801 223 9486

Address Please send tips, special requests, change of address, subscriptions, fullfillment questions, requests for group subscriptions and other correspondence to:

NICs
1372 South 740 East
University Office Park
Orem, UT 84097-8083

or contact us via Internet E-mail at:
info@inpnet.org

Postmaster Periodicals postage paid in Provo, UT. Send address changes to:

NICs
1372 South 740 East
University Office Park
Orem, UT 84097-8083

Staff

Editor-in-Chief	**Keith**Parsons
Managing Editor	**Darryl**Alder
Testing Editor	**Deni**Berger
Tech Support Editor	**Todd**Hindmarsh
Technical Advisors	**Art**Allen
	SteveCrowley

Back Issues To order back issues, call Customer Relations at 801 223 9444. Back issues cost $8.50 each, $10.00 outside the US. You can pay with MasterCard, Visa, or American Express, or visit our archive at http://www.inpnet.org/nics.

The Institute for Network Professionals, in alliance with technical suppliers and organizations, makes resources accessible to network professionals worldwide by providing products, training, publications and events.