

Microsoft

# Server 2003 Network Environment

(70-290)

Microsoft Certified  
Systems Engineer (MCSE)



**Smarter  
Training**

This LearnSmart exam manual prepares candidates for the Server 2003 Network Environment exam (70-290) by providing in-depth information about the following exam-related content:

- Managing and Maintaining Physical and Logical Devices
- Managing Users, Computers and Groups
- Managing and Maintaining Access to Resources
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

# Windows Server 2003 Network Environment (70-290) LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC  
Product ID: 10011  
Production Date: July 12, 2011  
Total Questions: 25

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

## Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

## Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

**1-800-418-6789**  
[solutions@learnsmartsystems.com](mailto:solutions@learnsmartsystems.com)

## International Contact Information

**International:** +1 (813) 769-0920

**United Kingdom:** (0) 20 8816 8036

**Table of Contents**

Abstract .....	4
What to Know .....	4
Tips .....	4
Resources:.....	4
<b>Managing and Maintaining Physical and Logical Devices .....</b>	<b>6</b>
Managing Basic and Dynamic Disks .....	6
<i>Converting Basic Disks to Dynamic Disks</i> .....	7
Monitoring Server Hardware .....	8
<i>Device Manager</i> .....	8
<i>Hardware Troubleshooting Wizard</i> .....	10
Optimizing Server Disk Performance .....	10
<i>Implementing a RAID Solution</i> .....	10
<i>Defragment Volumes and Partitions</i> .....	11
Installing and Configuring Server Hardware Devices .....	12
<i>Configuring Driver Signing Options</i> .....	13
<i>Configuring Resource Settings for a Device</i> .....	14
<i>Configuring Device Properties and Settings</i> .....	14
Managing Users, Computers and Groups .....	15
<i>Managing Local, Roaming, and Mandatory Profiles</i> .....	16
Creating and Managing Computer Accounts in an Active Directory Environment .....	18
Creating and Managing Groups .....	20
Group Types.....	20
<i>Group Scope</i> .....	21
<i>Creating Groups</i> .....	21
Creating and Managing User Accounts .....	22
<i>Other Managing Users, Computer, and Groups Topics</i> .....	23
<b>Managing and Maintaining Access to Resources .....</b>	<b>24</b>
Configuring Access to Shared Folders .....	24
Troubleshooting Terminal Services .....	27
<i>Configuring Data Compression</i> .....	28
Configuring File System Permissions .....	28
<i>Encrypting File System (EFS)</i> .....	29
<i>Copying and Moving files encrypted with EFS</i> .....	30

---

<b>Managing and Maintaining a Server Environment</b> .....	<b>31</b>
Monitoring and Analyzing Events .....	31
<i>Event Viewer</i> .....	31
<i>System Monitor</i> .....	31
Managing Software Update Infrastructure.....	35
Managing Software Site Licensing .....	36
Managing Servers Remotely .....	37
<i>Terminal Services Licensing</i> .....	37
Troubleshooting Print Queues .....	38
Disk Quotas .....	38
Optimizing Application Performance.....	39
Manage a Web Server.....	40
<i>Worker Process Isolation Mode</i> .....	40
<i>Methods of IIS Administration</i> .....	41
<i>Other IIS Features</i> .....	41
<i>IIS Installation</i> .....	42
<i>IIS Authentication Methods</i> .....	42
<b>Managing and Implementing Disaster Recovery</b> .....	<b>44</b>
Perform System Recovery for a Server .....	44
<i>Startup Options</i> .....	44
<i>Recovery Console</i> .....	44
<i>Automated System Recovery (ASR)</i> .....	46
Managing Backup Procedures.....	51
Scheduling Backup Jobs .....	56
<b>Practice Questions</b> .....	<b>62</b>
<b>Answers and Explanations</b> .....	<b>74</b>

## Abstract

This certification exam measures your skills and your ability to manage, maintain and run a Microsoft Windows Server 2003 environment. Before taking the exam, you should have hands-on experience in the basic administration and operation of a Windows server environment, including: user and group management, device management, file and access management, and skills in disaster recovery.

## What to Know

Microsoft's exam 70-290, "Managing and Maintaining a Microsoft Windows Server 2003 Environment" is a core networking system requirement for the MCSE (Microsoft Certified Systems Engineer) on Microsoft Windows Server 2003, and MCSA (Microsoft Certified Systems Administrator) on Microsoft Windows Server 2003 certifications. It is designed for IT professionals who "work in the typically complex computing environment of medium to large companies." There is no specific prerequisite for this exam but Microsoft recommends that candidates have "6 to 12 months of experience administering client and network operating systems" in the type of environment.

This exam costs \$125 USD and may be taken from Pearson Vue or Thomson Prometric. "Beginning with the release of the Microsoft Windows Server™ 2003-related exams, Microsoft will provide numerical scores on exams. By the end of September 2003, most exams will have the new score report format, which includes this numerical score... The new scale requires a minimum passing score of 700 on all exams. The maximum score on the exams will vary depending on the complexity of the skills being measured." - Microsoft Exam and Testing Procedures FAQ

Note that Microsoft does not document the format of a particular exam: "Microsoft exams might include adaptive testing technology and simulation items. Microsoft does not identify the format in which exams are presented."

The topics covered by this exam include:

- Managing and Maintaining Physical and Logical Devices
- Managing Users, Computers, and Groups
- Managing and Maintaining Access to Resources
- Managing and Maintaining a Server Environment
- Managing and Implementing Disaster Recovery

## Tips

This exam requires hands-on experience with Windows 2003 Server. Build a server, and review all the administrative tasks mentioned in this exam manual. Along with this manual, read Technet articles and whitepapers on the features and functions of the server, and how they differ with previous versions.

# Managing and Maintaining Physical and Logical Devices

## Managing Basic and Dynamic Disks

Disks are managed through the Disk Management MMC snap-in. It allows the administrator to manage the physical disks, and logical volumes, or partitions. The interface allows:

- Disk initialization
- Formatting of volumes (NTFS and FAT)
- The creation of fault-tolerant disk systems

Windows 2003 has two different types of disks:

- Basic disks – Contain basic volumes (primary partitions and logical drives in extended partitions). Basic disks are used on portable devices, or on devices that will have multiple operating systems involved.
- Dynamic disks – Dynamic disks were introduced in Windows 2000, and allow the administrator greater flexibility in disk subsystem configuration. Dynamic disks allow the following:
  - ▶ Extension of volumes
  - ▶ Mirroring
  - ▶ Addition of disks without restarting
  - ▶ Fault tolerant configurations

Note: System and boot volumes cannot be extended.

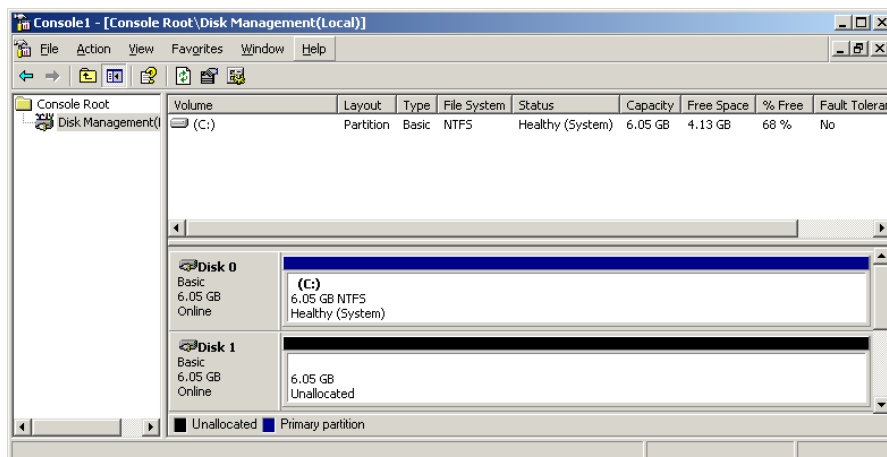


Figure 1 - Disk Management Console

## Converting Basic Disks to Dynamic Disks

Dynamic disks provide features that basic disks do not, such as the creation of multi-disk volumes for fault tolerance and enhanced performance. Some items to know about the conversion:

- Before converting disks, you need to close any programs that are running.
- Note that the conversion is not reversible as dynamic disks cannot be changed back to basic partitions without first deleting all the dynamic volumes on the disk.
- If a volume or partition is in use before conversion, you must reboot for the changes to take affect. Any files that are locked open during the conversion may be lost – do not convert the disks from basic to dynamic while users are accessing resources on the server.
- Dynamic disks cannot be directly accessed by MS-DOS, Windows 95/98, Windows Me, Windows NT or XP Home.
- Only Windows 2000, XP Professional and Windows .NET server can access dynamic MBR disks.
- You cannot dual-boot multiple installations of Windows 2000, Windows XP Professional, or Windows 2003 off of the same dynamic disk. A dynamic disk set can only be “owned” by one copy of Windows (through registry settings) – the other installations trying to use the same dynamic disk set will refuse to boot.
- When converting a basic disk that contains Shadow Copies, you can do a straight conversion without data loss only if the Shadow Copy storage resides on a boot volume. If the Shadow Copies are stored elsewhere you will need to dismount and take offline the disk containing the original files before the disk holding the Shadow Copies is upgraded from Basic to Dynamic. The volume containing the original files must then be brought back online within 20 minutes to avoid data loss.

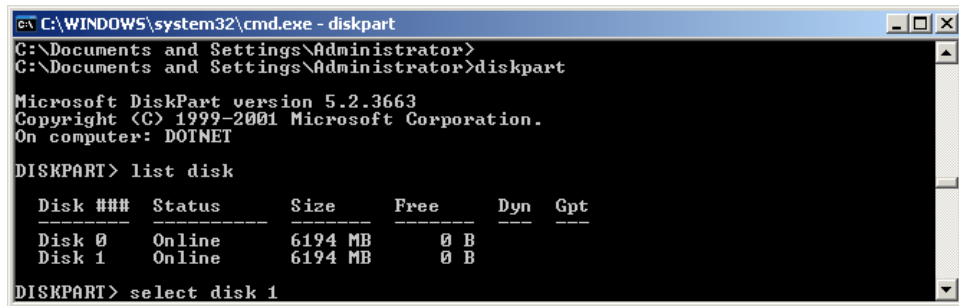
There are two ways to convert disks from basic: from the Disk Management GUI, or the command line.

Steps using Disk Management GUI:

1. Open the Computer Management interface.
2. Right-click the basic disk you would like to convert, and select Convert to Dynamic Disk. Here are two reasons you may not see this option: a) you have clicked a volume instead of a disk; b) the computer you are using is a portable (Dynamic Disks are not supported on removable or detachable disks, shared SCSI disks, fire wire or USB).

Steps using the command line:

1. Open a command prompt.
2. Type `diskpart`.
3. You have now entered the Disk Partition command line utility. At the prompt, type ***list disk***. This will show the disks on the server, and their associated number and properties.
4. Type ***select disk disk-number***. Enter the desired disk number from the previous step.
5. Type ***convert dynamic***.



```
C:\WINDOWS\system32\cmd.exe - diskpart
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>diskpart

Microsoft DiskPart version 5.2.3663
Copyright (C) 1999-2001 Microsoft Corporation.
On computer: DOTNET

DISKPART> list disk

   Disk ###  Status         Size           Free           Dyn    Gpt
   -----  -
   Disk 0             Online        6194 MB         0 B
   Disk 1             Online        6194 MB         0 B

DISKPART> select disk 1
```

Figure 2 – The diskpart command

## Monitoring Server Hardware

### Device Manager

Device Manager allows the administrator to view all the hardware devices that are installed on the server. The interface can be used to manage devices, troubleshoot, upgrade drivers, and modify hardware settings.

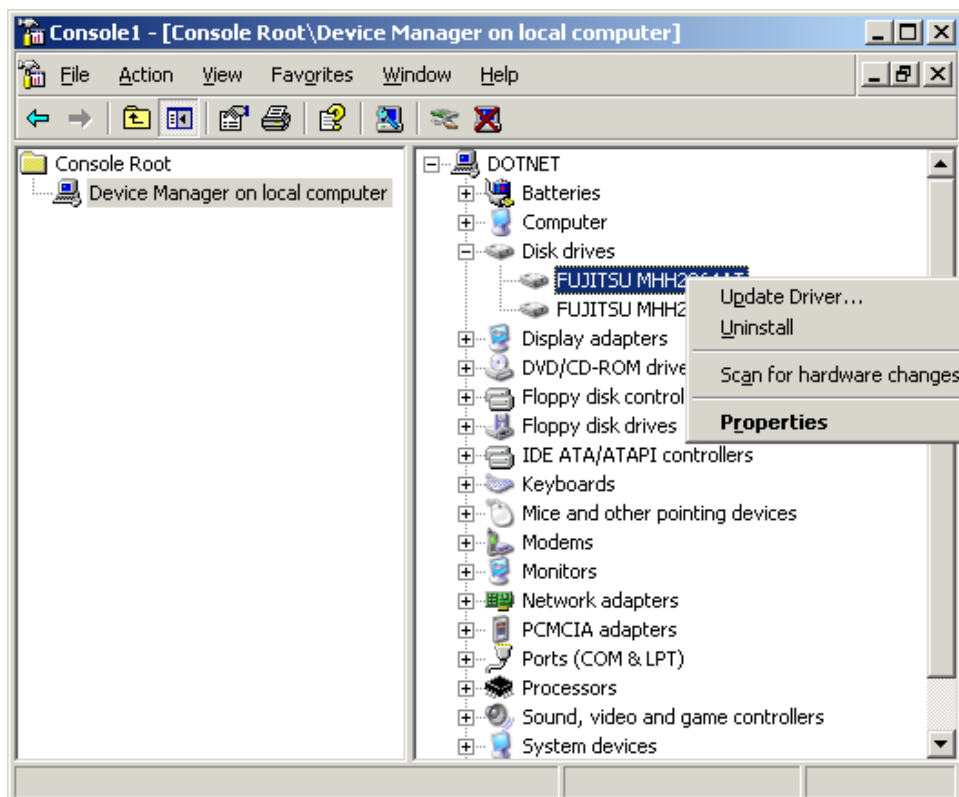
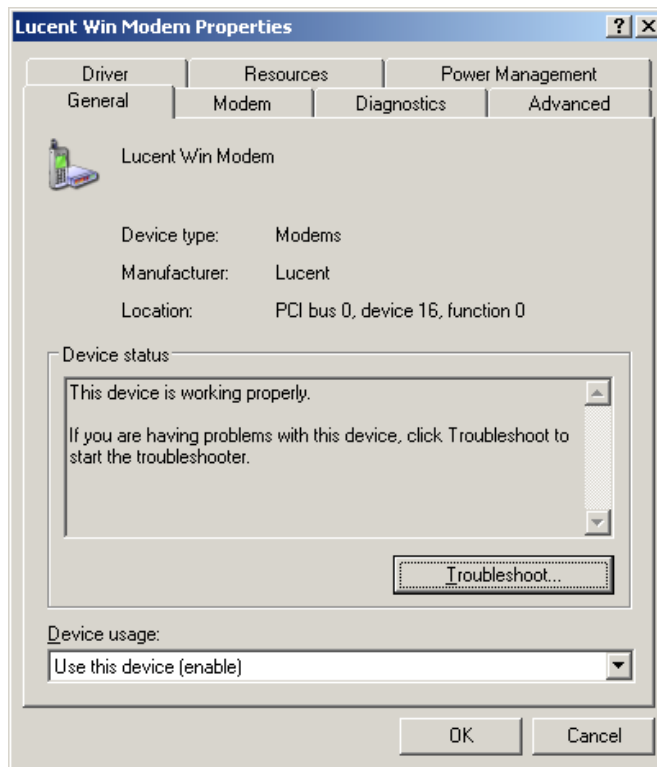


Figure 3 - Device Manager interface and options



More specifically, Device Manager can be used to:

- Determine whether or not a device is functioning properly.
- Change hardware configuration settings (DMA, IRQ, I/O, etc).
- Identify and gain information about the current driver and firmware.
- Change advanced settings and properties.
- Update device drivers.
- Uninstall, enable and disable devices.
- Print a summary of devices installed on the server.
- Set power management options.



**Figure 4** - Device Manager and the tabs for configuration and information

## Hardware Troubleshooting Wizard

The Hardware Troubleshooting Wizard allows convenient troubleshooting through the Device Manager interface. By clicking the Troubleshoot button on the General tab for a device, you will be walked through a series of pages to help resolve the problem.

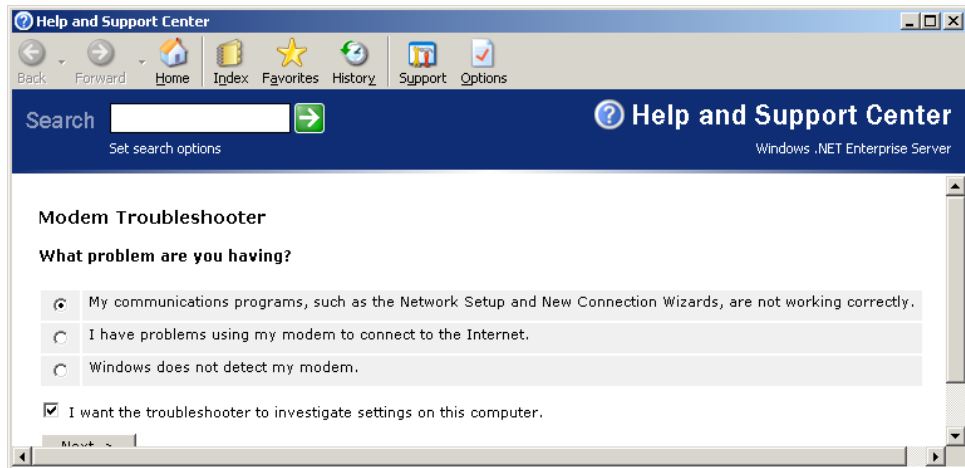


Figure 5 - The troubleshooting screen for a modem

## Optimizing Server Disk Performance

### Implementing a RAID Solution

Windows Server 2003 allows the creation of software RAID solutions, and has the added flexibility, through the use of dynamic disks, to extend volumes without repartitioning or reformatting the disks. Windows 2003 does not support any volumes, stripe sets, mirror sets, or stripe sets with parity on a Basic Disk (these are installed by Windows NT 4 Server). These features are now only available on Dynamic Disks and have been renamed accordingly. Below are the disk sets, and the different names for each OS:

Windows NT 4.0	Windows 2003
Volume Set	Spanned Volume on a Dynamic Disk
Mirror Set	Mirrored Volume on a Dynamic Disk
Stripe Set	Striped Volume on a Dynamic Disk
Stripe Set with Parity	RAID 5 Volume on a Dynamic Disk

There are certain preparations you need to make when upgrading to Windows 2003 from NT 4:

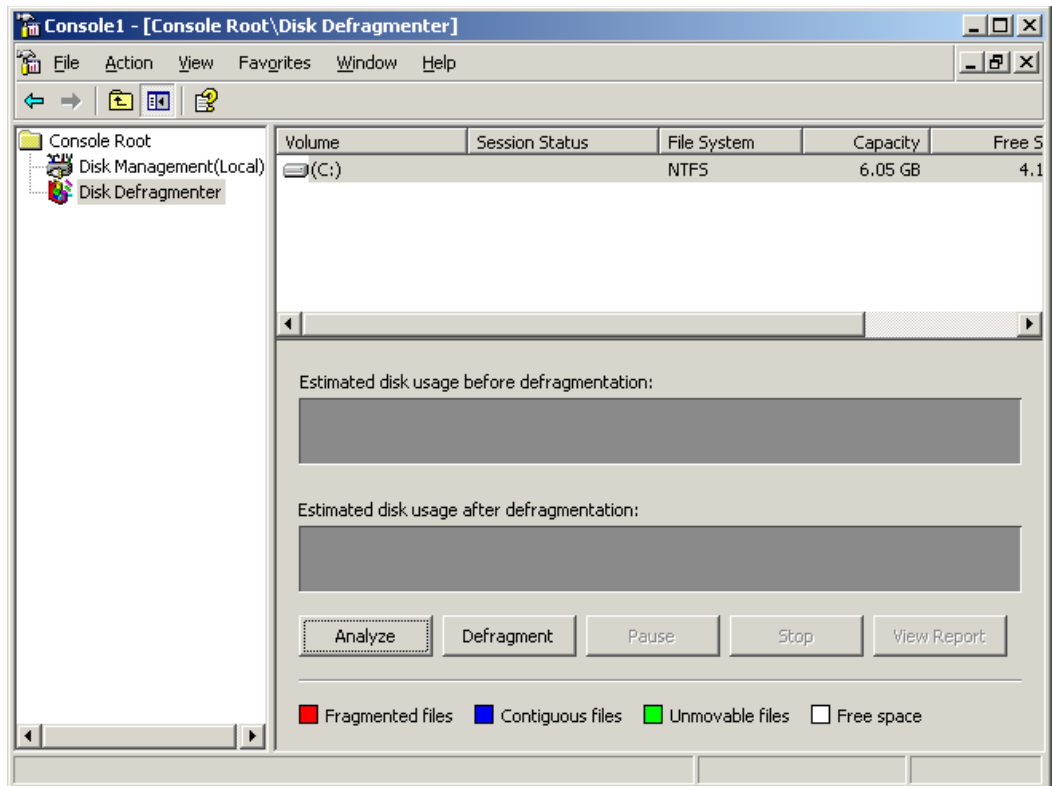
- **Mirror Set** – You need to back up the data, and then break the mirror. Ensure you have Service Pack 5 or above, and then run the upgrade.
- **Volume, Stripe, and Stripe with parity** – You will need to back up the data, and then delete the set. When you install Windows 2003, you need to create the dynamic disk and create the volume. Then restore the data.

## Defragment Volumes and Partitions

Windows 2003 includes the Disk Defragmenter utility which provides the ability to consolidate fragmented files and folders. This allows the system to use the disk more efficiently, and provides better performance. Along with consolidating files and folders, the utility also consolidates disk free space.

Defragmenting Best Practices:

- **Analyze the volume before performing a defrag** – Analyze the volumes once per week, and only defragment them if the utility recommends it.
- **Analyze after many files are added** – File servers will need to be analyzed much more often than a laptop. Analyzing after many files are added will allow efficient use of the space.
- **Volumes need at least 15% free space** – For the utility to work correctly, it needs at least 15% free space. This space is used for sorting of files and folders.
- **Run the utility during low-usage periods** – The process will have a large impact on performance.
- **Defrag after installing or upgrading Windows** – The install/upgrade process installs and removes a large number of files. Running the software after these events will “clean up” the disk.
- **A consistently high number of Split I/O's per second** under either the Physical Disk or Logical Disk counters in Performance Monitor usually indicates your disks are in need of defragmentation.



**Figure 6** – Disk Defragmenter

The Disk Defragmenter Utility is shown above. To analyze the volume, click on the Analyze button. Once the analysis is complete, the report will show disk statistics, and give a recommendation of whether or not to defrag.

To defragment a volume using the command line, run:

**Defrag** *volume /v*

Note that you still need 15% free space to complete the defrag. You cannot defrag a “dirty volume”. “The dirty bit can be set because the volume is online and has outstanding changes, because changes were made to the volume and the computer shutdown before the changes were committed to disk, or because corruption was detected on the volume.”

Check if the volume is dirty by running the **fsutil dirty query** command.

## Installing and Configuring Server Hardware Devices

### Configuring Driver Signing Options

Microsoft uses digital signatures to ensure that particular drivers have had a certain level of testing, and that they have not been altered in any way. The Designed for Microsoft Windows .NET logo ensures that drivers have been authorized for the utmost compatibility.

Windows Server 2003 will handle non-signed drivers in different ways. The administrator can configure the system to do one of the following when a non-signed driver is encountered:

- Ignore the warnings and driver.
- Display a warning about the driver (the default).
- Prevent the installation of non-signed drivers.

These settings can be configured in the Policy Console through the Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options tree. (See below)

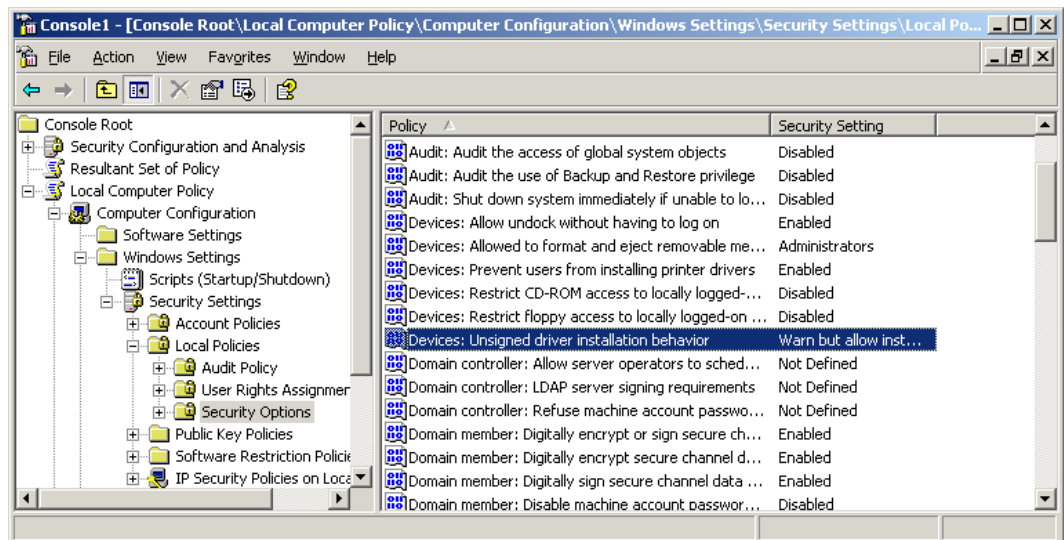
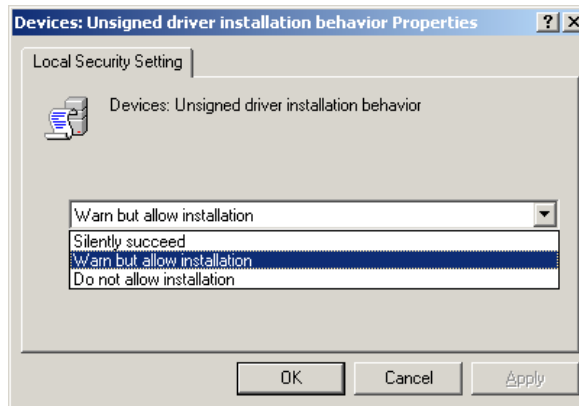


Figure 7 – Security options

Right-click the “Unsigned driver installation behavior” and you will get the property window below.



**Figure 8** – Unsigned driver installation options

Windows uses the following features to protect your system, and ensure that signing is utilized to ensure the integrity of the system:

- Windows File Protection
- System File Checker
- File Signature Verification

### Configuring Resource Settings for a Device

To change device resource settings:

1. Open the Device Manager.
2. Double-click the device, and the properties window will open.
3. Select the Resources tab, and uncheck the "Use automatic settings" check box.
4. Highlight the resource to change, and select the "Change setting" button to change the properties.

## Configuring Device Properties and Settings

The device manager offers the administrator the ability to configure custom settings and information for devices on the computer. Below is an example of a modem Property Sheet:

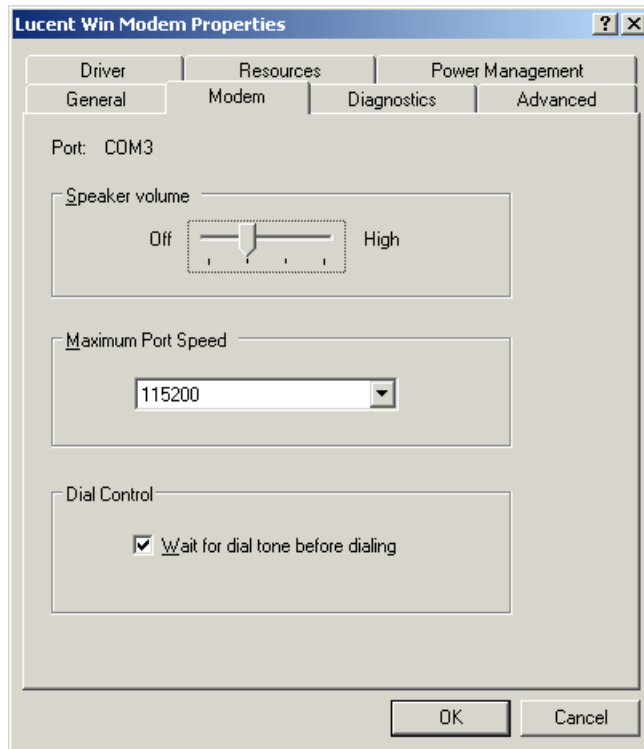


Figure 9 – Configuring device properties

Different devices will have additional property sheets that can be selected for custom configurations.

### Hardware Profiles

Multiple hardware profiles may be configured for a Win Server 2003-based mobile computer through the Control Panel, System applet. Click the Hardware tab, then Hardware Profiles. Click Copy and type a name for the new profile. Upon clicking OK, the name of the new profile will be selectable. Select it and go to Properties, click "This is a portable computer" and select one of the profile descriptions that appear. Click "Always include this profile as an option when Windows starts".

Besides the obvious convenience of enabling different hardware profiles on a server for consultants, trainers, and other mobile workers, there is this: If a non-mobile computer is ever booted without LAN connectivity, the "Preparing network connections" step will search needlessly until it times out and delay the bootup.

## Managing Users, Computers and Groups

### Managing Local, Roaming, and Mandatory Profiles

User profiles are used in Windows 2003 server to maintain user settings and preferences on the local computer. The profile is created for each individual user upon first login, and is automatically updated when changes are made.

User profiles provide several advantages:

- They allow more than one individual to use the computer, and maintain their own customized workspace.
- The profiles are maintained separately, and allow user changes to be made independently, not affecting other users.
- Profiles can be stored on a server, allowing the profile to follow the user through the enterprise (roaming profiles).

Profiles also offer several advantages to the administrator:

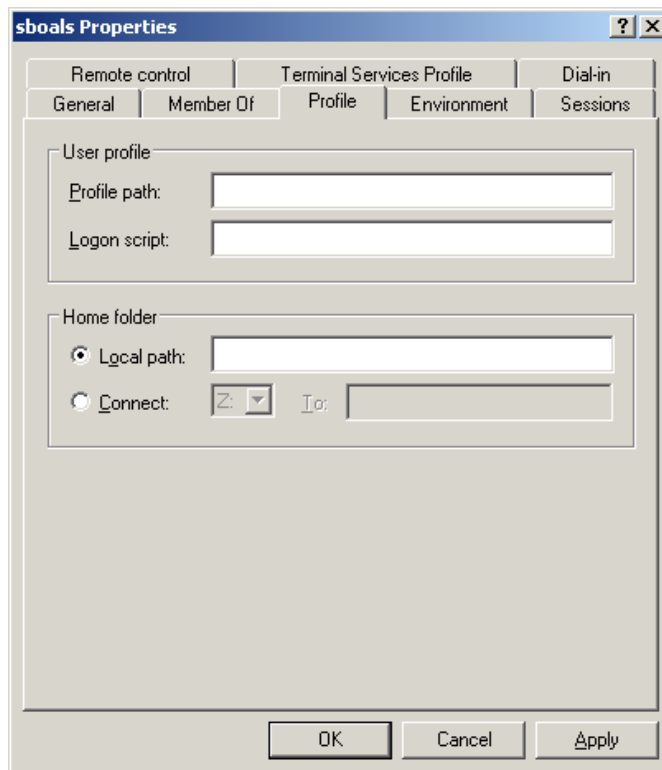
- Default profiles can be created to give new users a basic set of settings.
- Mandatory profiles do not allow the user to save changes. He can modify his environment, but the changes are not saved on exit.
- You can add default items that will be included in all profiles.

The following are the profile types:

- Local – The local profile is created on the local machine when a user first logs in. The profile and changes are stored on the local computer.
- Roaming – Roaming profiles are stored on a central server, and are available anywhere on the network. Changes are also updated to the server.
- Mandatory – These are a type of roaming profile that is assigned to a certain individual, or group. Only the system administrator can make changes to this type of profile.
- Temporary – This profile type is used whenever there is an error with other profile types. It is not saved, and is deleted upon exit.



Editing profiles can be done through the User Properties Profile tab:



**Figure 10** – Profile properties

The profile path can be set here. To enable a mandatory profile, change the file extension on the profile from .dat to .man.

To view current profiles on the local computer, or change the profile type, go to the System in the Control Panel. Click the Advanced tab, and choose the User Profiles Settings.

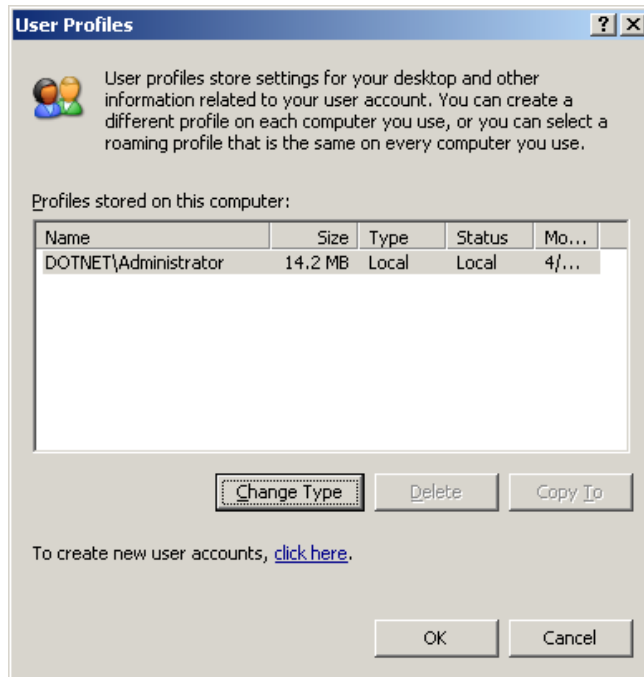


Figure 11 – User profiles

## Creating and Managing Computer Accounts in an Active Directory Environment

Creating and managing computer accounts in the Windows 2003 environment is accomplished through the "Active Directory Users and Computers" Interface shown below.

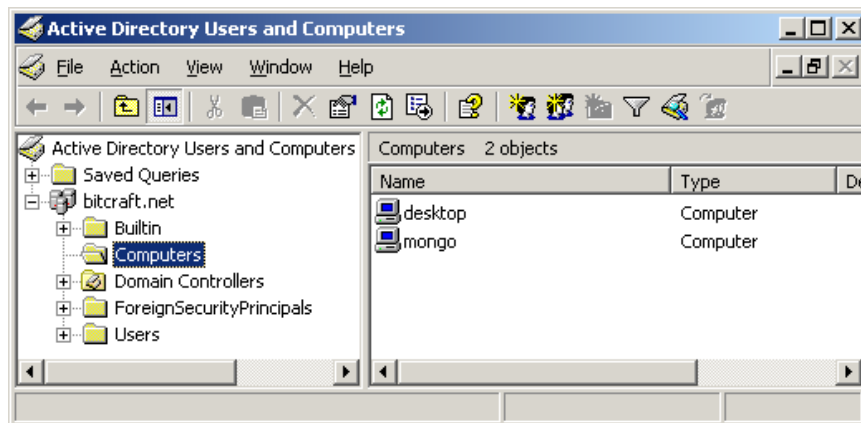


Figure 12 – Active Directory Users and Computers

To perform the task, you must be a member of the Account Operators, Domain Admins or Enterprise Admins group, or have the ability delegated by the proper authority. Note that Account Operators cannot create computer accounts in the Builtin, Domain Controller, System, User, LostandFound or Program Data Containers.

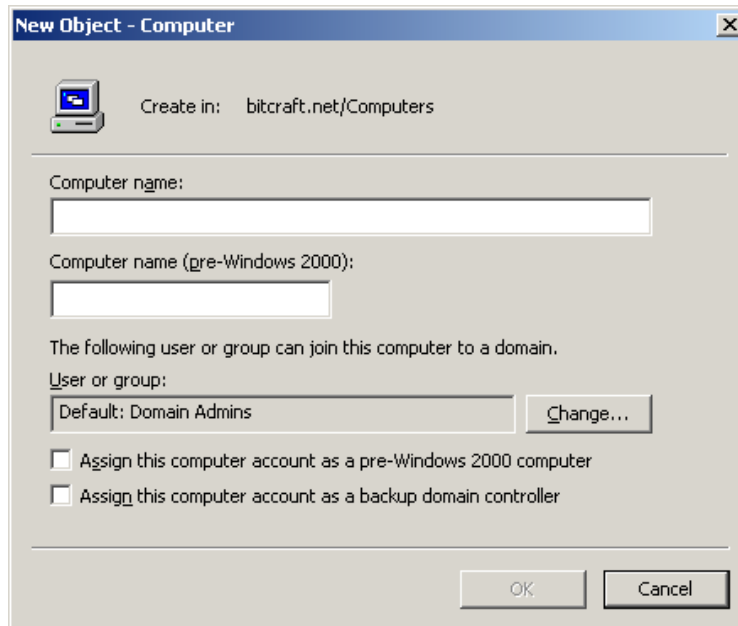


Figure 13 – Creating a new computer object

To create a new computer account, right-click the “Computers” container in the left pane of the console. Select New, and Computer and the above “New Object” dialog box will appear. In this box, you enter the Computer name, pre-Windows 2000 name, and then select the options for pre-Windows 2000 or BDC.

Once the account has been created, you will have access to advanced properties for the object. Right-click the computer in the right-hand pane, and select properties. The computer properties dialog box has the following tabs:

- General – Shows the name (including DNS), the role, description and the ability to allow Trust through delegation.
- Operating System – Includes Name, Version and Service pack.
- Member Of – Lists the groups to which the object belongs, and allows you to add other groups. Also allows you to set the primary group for POSIX or Apple computers.
- Location – Self Explanatory.
- Managed By – Information about the manager of this object. Allows you to select this information.
- Dial-In – Allows the setting of RAS info.

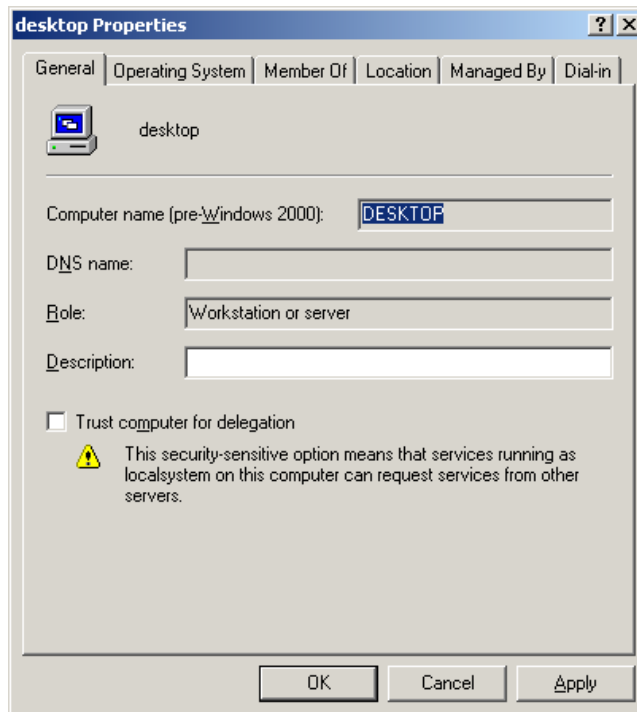


Figure 14 – Desktop properties

Right-clicking the Computer name will also allow you to disable, reset, move, manage and delete the object. Selecting manage will allow you to use the “Computer Management” console on the remote computer.

## Creating and Managing Groups

### Group Types

Groups are used in Windows 2003 as repositories for computer and user accounts, along with other group types. Proper group management leads to simpler administration, and reduction of administrative tasks. Below are two types of groups:

- Distribution Groups – This group type is used for e-mail applications, such as Exchange, to distribute messages to many users. This group type is not “security-enabled”; and is not for use with Access Control.
- Security Groups – Security groups are used to streamline the security process, and “group” together individual users that all need the same rights or access to resources. There are some important concept to understand when looking at the scope of groups and permissions:
  - ▶ Rights and Active Directory – User rights determine access privileges with the Active Directory structure, and dictate what a user can do within a given domain.
  - ▶ Permissions – It is Important to understand the difference between rights and permissions. Permissions are set on security groups, and control access to objects.

## Group Scope

The scope defines how broadly the group's properties apply in the domain. There are three different group scopes:

- Universal – Universal Groups can include other groups and accounts from any domain or forest. Permissions can be assigned in any domain in the forest/domain tree.
- Global – Global groups can have users or groups originating from the domain in which the group is created. This group can then be assigned permissions in any domain in the forest.
- Local – Local groups can only have members that are in the local domain.

The best way to organize permissions is to grant them to local groups, then place domain-wide groups as members of those local groups. A list of local groups that are available and preconfigured on Win2003 include the following:

- Administrators- Can perform all administrative tasks on the local system. The built-in Administrator account is made a member of this group by default.
- Server Operators - Can manage the domain servers (this group is only found on domain controllers). It can create, manage, and delete printer and network shares, backup and restore data, format fixed disks, lock and unlock servers and files and change the system time.
- Account Operators - Can create and delete user accounts and groups. It cannot modify Administrator accounts, Domain Admins global group, local Administrators group, Account Operators, Print Operators and Backup Operators.
- Print Operators - Can create, manage, and delete printer shares.
- Backup Operators - Can use Windows Backup to back up and restore data on the computer.
- Guests - Used for gaining temporary access to resources for which the Administrator has assigned permissions. Members of Guests can't make permanent changes to their desktop environment. When a computer or member server running Client for MS Networks joins a domain, Windows 2000 adds Domain Guests to the local Guests group.
- Replicator - Supports file replication in a domain.
- Power Users - Can create and modify local user accounts on the computer, share resources and can install drivers for legacy software. This group only exists on W2K Professional workstations and on non-domain controllers/member servers.
- Users - Can perform tasks for which they have been assigned permissions. All new accounts created on a Windows 2000 machine are added to this group. When a computer or member server running Client for MS Networks joins a domain, Windows 2000 adds Domain users to the local Users group.

## Creating Groups

Use the following procedure to create a new group:

1. Open Active Directory Users and Computers.
2. Double click the domain.
3. Right click the container in which you would like to create the group, and choose New, then Group.
4. Type in the name, and choose the Group Type and Group Scope.

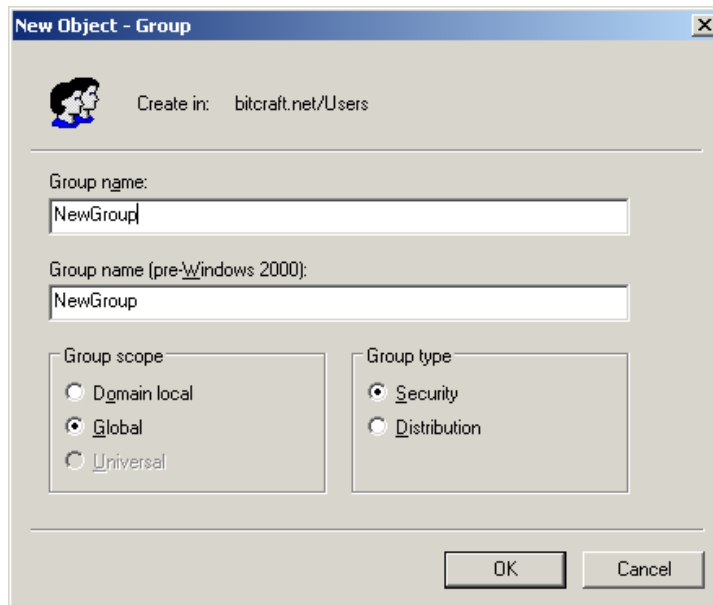


Figure 15 – Creating a group object

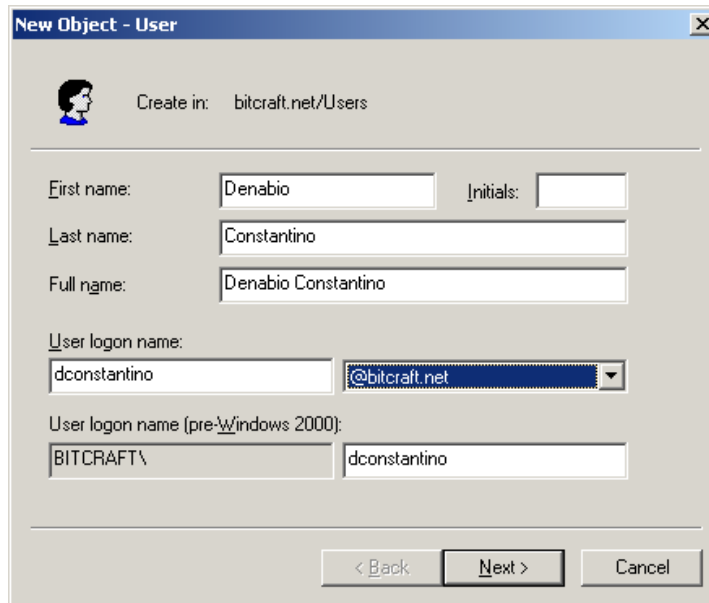
## Creating and Managing User Accounts

User accounts are used in Active Directory for the following purposes:

- Allowing authentication of an individual. The user account identifies a person to the domain, and the user is authenticated through the use of a password.
- Providing the ability to authorize/deny access to resources. Users can be assigned permissions that will allow them to access specific resources.
- Providing administrative capabilities. Accounts can be permitted specific rights which allow them to manage objects within the Active Directory.

To create a user account:

1. Open Active Directory Users and Computers.
2. Right-click the OU where you want the user created, click New, then User.
3. Fill in the required boxes.
4. Note that the User Principal Name (UPN) is everything after the @sign, and is required when logging in.



The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: bitcraft.net/Users'. Below this, there are several input fields: 'First name' with 'Denabio', 'Initials' (empty), 'Last name' with 'Constantino', and 'Full name' with 'Denabio Constantino'. Under 'User logon name', there is a text box with 'dconstantino' and a dropdown menu showing '@bitcraft.net'. Below that, 'User logon name (pre-Windows 2000):' has two text boxes: 'BITCRAFT\' and 'dconstantino'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Figure 16** – Creating a user object

5. Click next, and then enter password information.
6. Click Next and then Finish.

# Managing and Maintaining Access to Resources

## Configuring Access to Shared Folders

Sharing folders is one of the primary advantages of networking. Windows 2003 carries on the tradition of Windows, making the sharing of resources simple and convenient. The steps to create a share in Active Directory are:

1. Open the Active Directory Users and Computers.
2. Open the Domain node, and right click the container in which you would like to create the folder.
3. Choose New, and then Shared Folder.
4. Enter the Name, and UNC path.

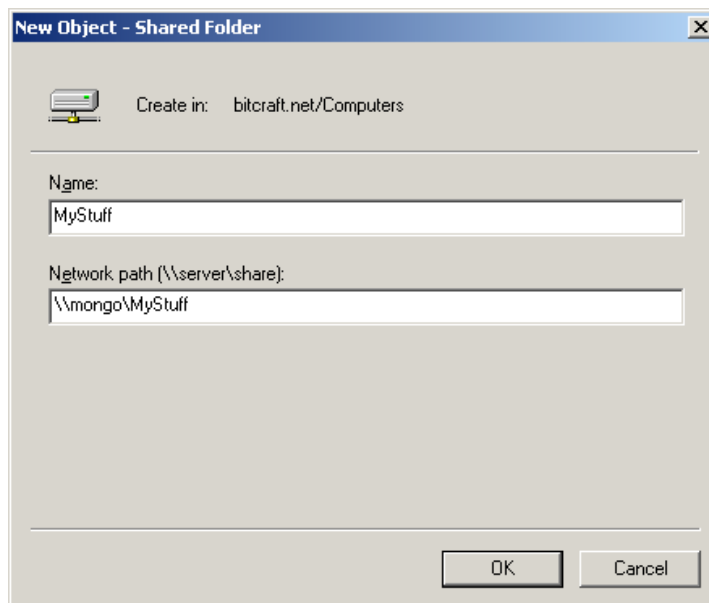


Figure 17 – Sharing a folder

Shared folders allow you to:

- Examine lists of files that are open by remote users, and close these files.
- Create, set and view permissions.
- View a list of users that are connected to shared resources.

To create and use shared folders, you must be a member of the Administrators or Power Users Group.

Offline Files, which is supported only on Windows 2000/2003 and XP-based clients, replaces My Briefcase and works a lot like Offline Browsing in IE5.



Share a folder and set its caching to make it available offline. There are three types of caching:

- Manual caching for documents - Default setting. Users must specify which documents they want available when working offline.
- Automatic caching for documents - All files opened by a user are cached on his local hard disk for offline use. Older versions on user's machine are automatically replaced by newer versions from the file share when they exist.
- Automatic caching for programs - Same as above, but for programs.

When synchronizing, if you have edited an offline file and another user has also edited the same file you will be prompted to keep and rename your copy, overwrite your copy with the network version, or to overwrite the network version and lose the other user's changes (a wise SysAdmin will give only a few key people write access to this folder or everyone's work will get messed up).

Using Synchronization Manager, you can specify which items are synchronized, using which network connection and when synchronization occurs (at logon, logoff, and when computer is idle).

To manage shares, use the MMC Console to open the snap-in "Shared Folders" (See below).

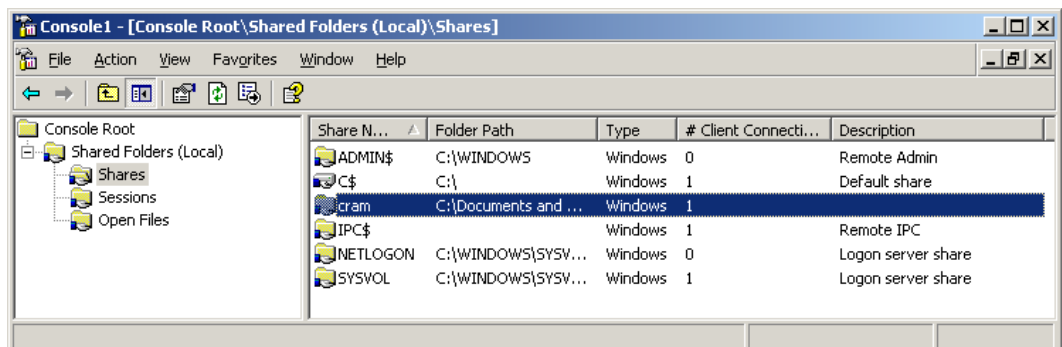


Figure 18 – Managing Shares

This console allows you to view the Shares, Sessions and Open Files. You can close resources, as well as set share permissions with this administrative console.

### Share/NTFS permissions

Characteristics:

- Folders residing on FAT, FAT32 and NTFS volumes can all be shared.
- Share level permissions only apply to accesses made to the shared object via a network connection. They do not apply to a user logged on at the local console.
- When folders on FAT and FAT32 volumes are shared, only the share level permissions apply. When folders on NTFS volumes are shared, the effective permission of the user will be the most restrictive of the two (e.g., a user with a Share level permission of Change and an NTFS permission of Read will only be able to read the file. A user with a Share level permission of Read and an NTFS permission of Full Control would not be able to take ownership of the file).

**Enabling Shadow Copies of shared folders**

To enable Shadow Copies of shared folders, right-click Properties on a fixed NTFS volume in My Computer, and click the Shadow Copies tab. An alternative method is done in the Computer Management console. Right-click Shared Folders | All Tasks | Configure Shadow Copies. Click the desired volume and click Enable. To enable Shadow Copies of shares on a remote server volume in Computer Management, right-click Disk Management | All Tasks | Configure Shadow Copies.

**Enabling Shadow Copies of shared folders in a cluster**

Enabling Shadow Copies of shared folders in a *cluster* is more involved. Create a cluster-managed file share on the appropriate cluster node (create a folder on the cluster disk and give Full Control to the Cluster Service account, then open Cluster Administrator from Admin Tools and create Physical disk, Network Name, IP Address, and File Share resources, all in the same resource group).

Set this File Share to have a dependency on the Physical Disk resource you're using to manage Shadow Copies (this will be automatic if the shadow copy volume and the designated storage volume are on different physical disks; these two volumes must also be in the same resource group) and a dependency on the Network Name resource for the share (File | New | Resource takes you to a wizard).

Highlight the file share resource, then File | Properties | Path | Parameters; enter the complete path pointing to the shared folder.

In Computer Management, right-click Shared Folders | All Tasks | Configure Shadow Copies; click the desired volume, then Enable.

**Shadow Copies Settings**

When sharing of Shadow Copies is first enabled, default settings are created for all shadow copies shared afterward; this can be configured under Shared Folders | All Tasks | Configure Shadow Copies; click on the volume to change, then Settings. These include:

- Storage Area - Details the volume where shadow copies will be placed. This can only be changed before enabling shadow copies or after deleting current shadow copies. The default location is the source volume; placing the shadow copies on another disk/volume can improve performance.
- Maximum Size - Configures the maximum space allowed for shadow copies on the volume. Must be at least 100 MB, and is 10% of the size of the source volume by default.
- Schedule - By default, shadow snapshots are taken at 7 AM and 12 noon, Mon-Fri. If that doesn't work well, change it here.

**Other Shadow Copy Facts**

- When a share is shadow copy-enabled, a Previous Versions tab appears on the share's Properties sheet.
- The Shadow Copy process stores only the changes to files and not the entire contents of the file: it is not a replacement for backup procedures. However, if a file is deleted or corrupted, a stored previous version can be used to restore the file without Admin assistance.
- Up to 64 shadow copies of a file can be stored; after that, or when the maximum storage size is exceeded, the oldest entries drop off to make room for new ones.
- The shadow copies cannot be viewed directly by users from the volume they are stored on; they must be accessed through the share. ACLs of the source files/folders apply also to the shadow copy shares.

- Shadow copies of shared folders apply at the volume level, and cannot be applied only to certain files/folders in the volume; it's all-or-nothing.
- You must be a member of Administrators or have appropriate rights delegated to your account in order to administer shadow copies.

## Troubleshooting Terminal Services

Terminal server allows individuals remote console access to Windows devices. Windows 2003 has renamed and/or replaced several Terminal Server/Remote Desktop features.

In order to allow remote connections, you must enable the Remote Desktop. This can be done through the Control Panel, using the System Properties. Choose the Remote tab, and check the Remote Desktop check box. This properties sheet will also allow you to set permissions, as well as allow Remote Assistance.

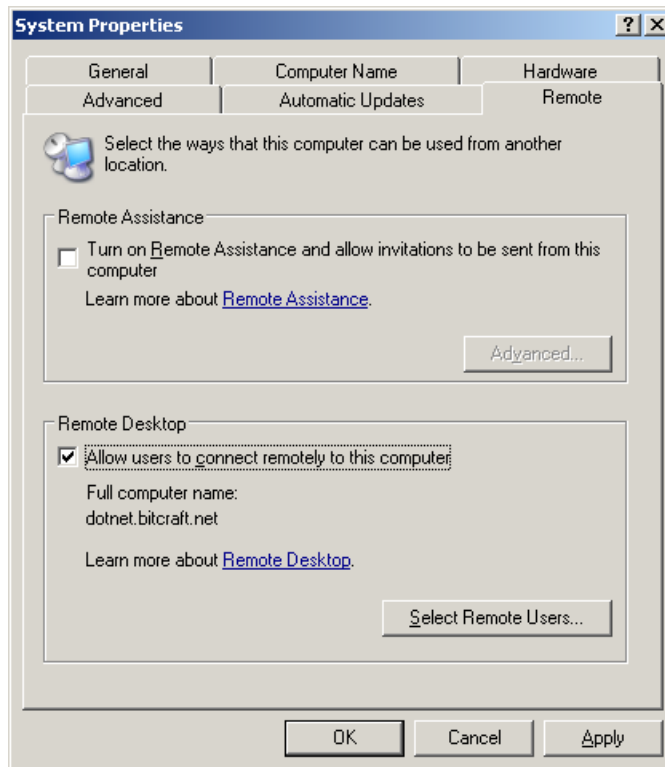


Figure 19 – Remote Desktop configuration

## Configuring Data Compression

Files and folders on NTFS volumes can have their compression attributes set through My Computer or Windows Explorer.

Compact is the command-line version of the real-time compression functionality used in Windows Explorer. It can be used to display or alter the compression attributes of files or folders on NTFS volumes (does NOT work on FAT or FAT32 volumes). Its switches are:

- none - Displays the state of the current folder.
- /c - Compresses the specified folder or file.
- /u - Uncompresses the specified folder or file.
- /s[:folder] - Specifies that the action be applied to all sub-folders of the parent folder.
- /a - Displays files with hidden/system attribute.
- /l - Ignores errors.
- /f - Forces specified file or folder to compress/decompress.
- /q - (Quiet) reports only essential information.
- /? - Displays user help.
- filename - Specifies a file or folder: it can use multiple filenames and wildcards.

## Configuring File System Permissions

Permissions on files and folders include the following:

- Full Control
- Modify
- Read and Execute
- List Folder Contents
- Read
- Write

Each of the above permissions includes special permissions (these can be reached by using the Advanced Tab on the Permissions Property sheet). These are a select few that need to be understood:

- Traverse Folder/Execute - This permission allows users to traverse the folder structure to reach the designated file/folder. The user must have the Bypass Traverse Checking right in order to perform this activity.
- List Folder/Read - For folders, this will dictate if the folder contents can be viewed. For files, it dictates if the file itself can be read.
- Create Files/Write - Allows the creation of files in a folder, or the writing of content to the file.
- Take Ownership - allows the user to take ownership of the file/folder.

- Synchronize – This is used in multi-threaded apps, and allows different threads to access the file while others have control of the data.

Here is a table, from the Windows 2003 Help System, to memorize in advance of taking exam 70-290:

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Permissions are set on files/folders by right-clicking, and then selecting Properties. Choose the Security Tab, and this will allow you to set permissions on the object.

## Encrypting File System (EFS)

EFS is only available on Windows 2000, Windows 2003, and Windows XP operating systems using NTFSv5 partitions and volumes.

Characteristics:

- Encryption is transparent to the user.
- EFS uses public-key encryption. A public key from the user's certificate encrypts keys that are used to encrypt the file. The list of encrypted file-encryption keys is kept with the encrypted file and is unique to it. When decrypting the file encryption keys, the file owner provides a private key that only he has.
- If the owner has lost his private key, an appointed recovery system agent can open the file using his/her key instead.
- EFS resides in the Windows OS kernel and uses the non-paged memory pool to store file encryption keys - this means no one will be able to extract them from your paging file.
- Encrypted files can be backed up using the Backup Utility, but will retain their encrypted state as access permissions are preserved.
- Microsoft recommends creating an NTFS folder and encrypting it. In the Properties dialog box for the folder click the General tab then the Advanced button and select the "Encrypt Contents To Secure Data" check box. The folder isn't encrypted, but files placed in it will be automatically encrypted. Uncheck the box if you want to decrypt the contents of the folder.
- Although it is recommended that encryption take place at the folder level, it can be done at the file level. Encryption at the folder level will automatically result in all files inside the folder being encrypted. Files moved into or created in an encrypted folder will automatically become encrypted at that time.
- Default encryption strength is 128-bit.
- Compressed files can't be encrypted and vice versa.

## Copying and Moving files encrypted with EFS

Several different situations are listed below in terms of the final state of an encrypted file that is moved or copied to another location.

From one NTFS partition to another NTFS partition on the same computer:

- Copy the file as normal, it will remain encrypted.
- Move the file as normal, it will remain encrypted.

From an NTFS partition to a FAT partition (includes floppy disks):

- Copy the file as normal, it will not be encrypted.
- Move the file as normal, it will not be encrypted.

From one NTFS Windows 2000 computer to another Windows 2000 NTFS computer:

- Copy the file as normal, it will remain encrypted.
- Move the file as normal, it will remain encrypted.

From one NTFS Windows 2000 computer to another Windows FAT computer:

- Copy the file as normal, it will not be encrypted.
- Move the file as normal, it will not be encrypted.

## Managing and Maintaining a Server Environment

### Monitoring and Analyzing Events

#### Event Viewer

The Event Viewer is a centralized location for viewing Server events, and below are the logs that are available to the administrator:

- Application Log – This houses specific application log items.
- System Log – This log maintains information on the operating system and its components. Driver and hardware information would be here.
- Security Log – This is a central store for all security information and events. Unlike other logs, this log must be enabled to produce information through a Security Policy.
- Directory Service Log – Active Directory uses this log to write events, including replication issues and global catalog information.
- File Replication Log – Contains information on the Windows File Replication service.
- DNS – This log maintains information about the DNS service, and communications between servers.

Through the event viewer console, an administrator can configure specific properties that define how the logging behaves. Below are the properties you can configure:

- Maximum Log Size.
- Overwrite policy (overwrite as needed, overwrite by age, manually overwrite).
- Creating log filters that can help in searches for specific log entries.

The interface also allows you to clear, save and load event logs.

## System Monitor

The System Monitor interface provides the ability to monitor system performance using three different methods:

- Graphs – The graphing interface provides a real-time view of system performance.
- Logs- Logs are best suited for long term performance monitoring, and allows for tracking multiple computers, and piping data into a single log file.
- Alerts – Alerts are best suited for logging performance events that exceed a certain threshold.

### Graphing

The System Monitor provides a real-time graphing interface for examination of performance counters. To open the System Monitor interface, go to the Administrative Tools menu, and select Performance. Below is the default interface:

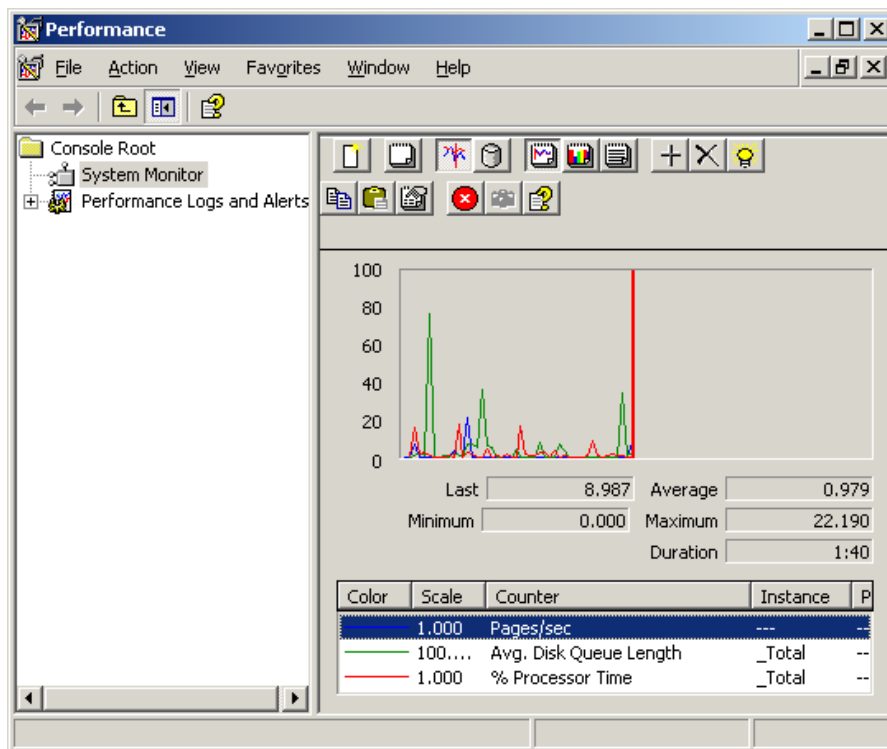


Figure 20 – System Monitor

The System Monitor defaults to the graph view, but you can also have a histogram or report view. The histogram view gives a bar graph representation of the performance data, and is useful for monitoring trends over time. The report view gives a numerical representation of the data, and is used for a quick view of performance and system information.



To add new counters to the current set, use the “+” sign on the tool bar. To highlight a specific counter, use Ctrl+H.

### Logs

In order to observe long term performance trends, and create baselines, the Log interface is appropriate. The counter log allows you to specify counters, and then collect the data in a specified logging format. The data can then be imported into a spreadsheet for graphing and analysis. To create a new log, right click the Counter Logs, and choose New Log Settings.

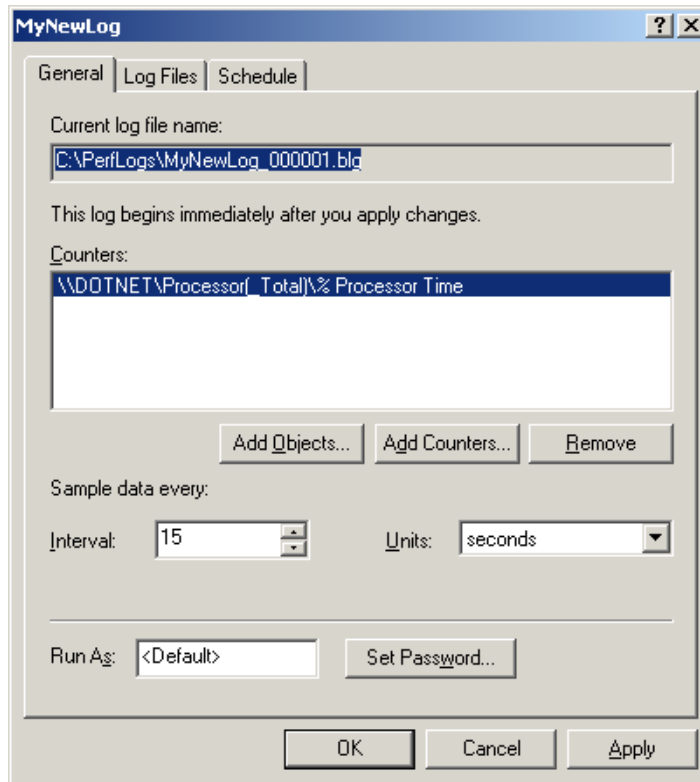


Figure 21 – New log settings

The Properties Sheet for you newly create log allows you to choose the log format:

- csv
- tsv
- binary
- SQL

The interface also provides the ability to schedule logging.

### Alerts

The Alerting functionality allows you to specify certain counters, and provide notification when that counter is over or under a specified value. When certain conditions are met, the Alerts give you the ability to:

- Send a network message.
- Log an event log entry.
- Start a performance log.
- Run a program.

You can also schedule when the alerting function occurs through the scheduling interface. Below is an example of the Event Log entry.

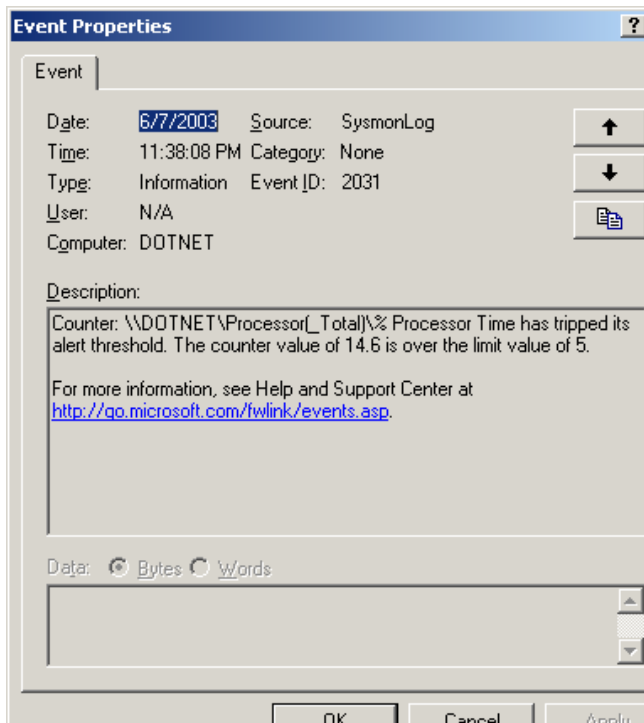


Figure 22 – Event properties

Performance Console Objects and Counters:

- Important objects are cache (file system cache used to buffer physical device data), memory (physical and virtual/paged memory on system), physicaldisk (monitors hard disk as a whole), logicaldisk (logical drives, stripe sets and spanned volumes), and processor (monitors CPU load).
- Processor - % Processor Time: This counter measures the time the CPU spends executing a non-idle thread. If it is continually at or above 80%, a CPU upgrade is recommended.

- Processor - Processor Queue Length: More than 2 threads in the queue indicates CPU is a bottleneck for system performance
- Processor - % CPU DPC Time (Deferred Procedure Call): This measures software interrupts.
- Processor - % CPU Interrupts/Sec: This measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check for a poorly written driver (bad drivers can generate excessive interrupts) or upgrade the CPU.
- Logical disk - Disk Queue Length: If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set.
- Physical disk - Disk Queue Length: Same as above.
- Physical disk - % Disk Time: If above 90%, move data/pagefile to another drive or upgrade drive.
- Memory - Pages/sec: More than 20 pages per second is a lot of paging so add more RAM.
- Memory - Committed bytes: This should be less than amount of RAM in computer.
- The diskperf command for activating logical disk counters has been eliminated in Windows 2003. Both physical and logical disk counters are now enabled by default.

## Managing Software Update Infrastructure

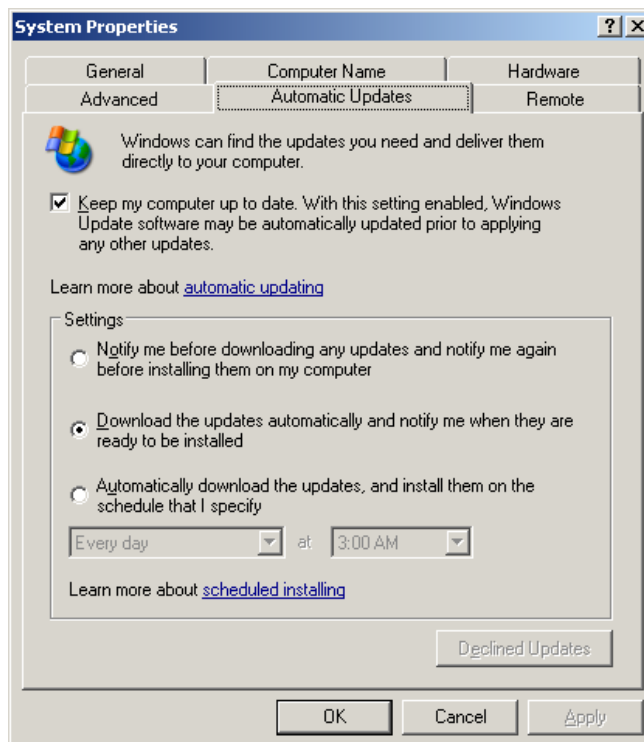


Figure 23 – Managing software updates

Managing software updates is accomplished through the System Properties sheet, using the Automatic Updates tab. This tab allows you to enable the automatic update feature, and select one of the following settings:

- Notify before download, and before install.
- Automatic download, and notification before install (default setting).
- Automatic download and install of updates. This option gives you the ability to schedule updates.

## Managing Software Site Licensing

Tracking and managing licenses can consume some serious time, and be a daunting task in the enterprise. Server 2003 provides two interfaces for the management and tracking of licenses:

- Control Panel Licensing – This interface allows the management of a single Windows 2003 computer. It lets you add or remove client licenses (for those in the per server mode), lets you change the licensing mode (per server to per seat), and lets you control the replication of licensing information to a centralized server.

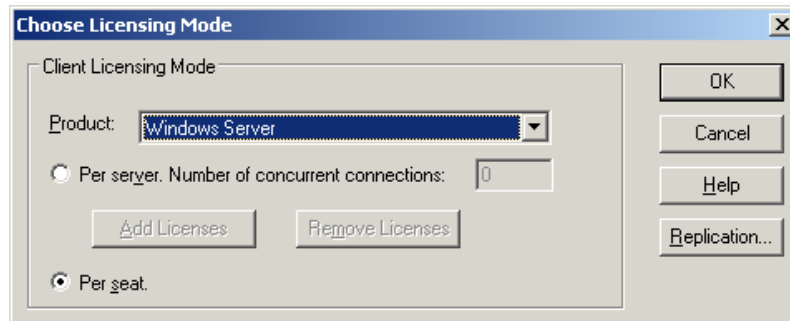


Figure 24 – Control Panel licensing

- Administrative Tools – Licensing – This interface provides for centralized license management, and tracking. Through the interface, you can:
  - ▶ View licensing for the site or group.
  - ▶ Manage license purchasing.
  - ▶ View licensing stats for users.
  - ▶ Remotely manage server licensing.
  - ▶ Manage license replication.

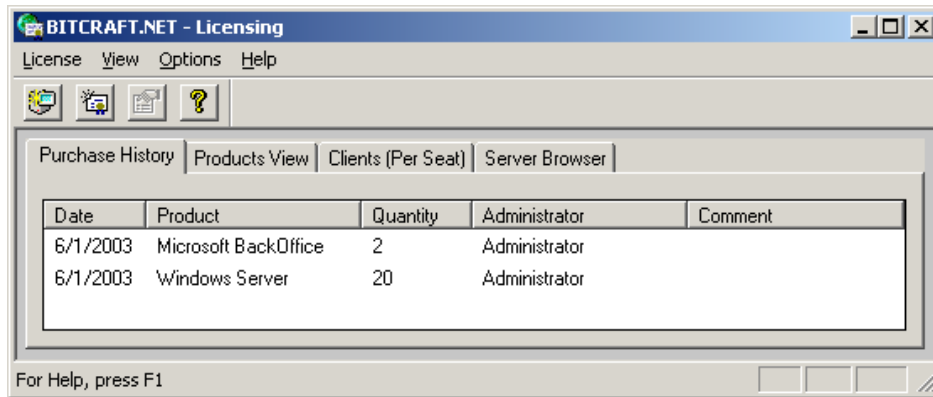


Figure 25 – Admin Tools licensing

## Managing Servers Remotely

Windows 2003 offers several methods, and improvements in how to manage servers remotely. The tools for remote management are:

- Microsoft Management Console (MMC) – The MMC allows the administrator to customize management consoles for both local and remote services. The MMC has a snap-in to manage just about every aspect of Windows.
- Windows Script Host (WSH) – WSH allows you to script admin functions for remote management. The WSH allows scripts written in VB and also JavaScript.
- Remote Installation Services (RIS) – RIS allows you to create Operating System images of machines, and then make them available to remote users for installation. Under Windows Server 2003, RIS can now be used to deploy W2k Pro, W2k Server, Win XP Pro, and Win2003 Server. The procedure for setting up a RIS server is changed very little from W2k Server.
- Remote Desktop – Allows the user to create a “terminal session” to a remote computer, with full desktop functionality.
- Web Interface – You can now manage a remote file or web server through the use of a web interface.
- Telnet – The Telnet service allows you to log into the remote server via command line. This is most useful for servers that will not respond to GUI management tools due to a failure.

## Terminal Services Licensing

Characteristics:

- There are two types of Terminal Server Client Access Licenses (CAL) available: TS Device CAL or TS User CAL.
- The TS Device CAL allows a single device to be used to open and conduct sessions on any TS server. Any user connecting through the licensed device is automatically under the device license.
- The TS User CAL permits that licensed user to open and conduct sessions on any TS server, connecting through any device.

- An important change in Windows Server 2003: ALL TS clients must now be operating under a license. This differs from W2k Server; the "desktop operating system equivalency" policy (that would apply only to WinXP) is no longer in effect. Owners of XP desktop licenses may be eligible to apply for a free TS User CAL or a TS Device CAL, at their option.
- Before a CAL can be used, Terminal Server Licensing must be installed and activated. Activation of a Licensing Server may be done locally (or remotely through a Web browser) through the Terminal Server Licensing applet from Administrative Tools. If the Terminal Server Activation and Licensing Website is unavailable, a license server ID number may be acquired from Microsoft by telephone. Upon activation, a License Server obtains a digital certificate from Microsoft that validates the server and enables it to receive TS CALs from Microsoft. The first time a Terminal Services client logs on to a terminal server, that server requests a license for the client from the License Server, which in turn requests a CAL from Microsoft and passes it on down the line.

## Troubleshooting Print Queues

The print queue shows documents waiting to be printed, and includes a list of document information, including: Doc name, Status, Owner, Pages, Size, Time Submitted, and Port.

Print queues can be monitored through the Performance tool. Some of the counters available to monitor are: Network Printer Calls, Bytes Printed, Jobs, Jobs printed, Pages Printed and Out of Paper Errors.

To pause, restart and stop print jobs, go to Printers and Faxes, and double-click the printer. This will show associated print jobs. You can right-click the job to get options.

Other facts to know:

- Internet Printing is continued in Windows 2003.
- Print Pooling allows two or more identical printers to be installed as one logical printer.
- Print Priority is set by creating multiple logical printers for one physical printer and assigning different priorities to each. Priority ranges from 1, the lowest (default) to 99, the highest.
- Enabling "Availability" option allows Administrator to specify the hours the printer is available.
- You can select Restart in the printer's menu to reprint a document. This is useful when a document is printing and the printer jams. Resume can be selected to start printing where you left off.
- You can change the directory containing the print spooler in the advanced server properties for the printer.
- To remedy a stalled spooler, you will need to stop and restart the spooler services in the Services applet in Administrative Tools in the Control Panel.
- Use the fixprnsv.exe command-line utility to resolve printer incompatibility issues.

## Disk Quotas

Disk quotas are used to monitor and control the disk space usage on an NTFS volume on a file server. For more information on designing a disk quota strategy, check out the wealth of articles at [technet.microsoft.com](http://technet.microsoft.com).

## Optimizing Application Performance

Windows 2003 server allows for the administrator to tune the way the server runs applications. Performance Options are adjusted by using the Advanced Tab on the System Properties sheet. Click on the Settings button in the performance section.

In order to make system performance changes, you must be an administrator, or have the specific right delegated.

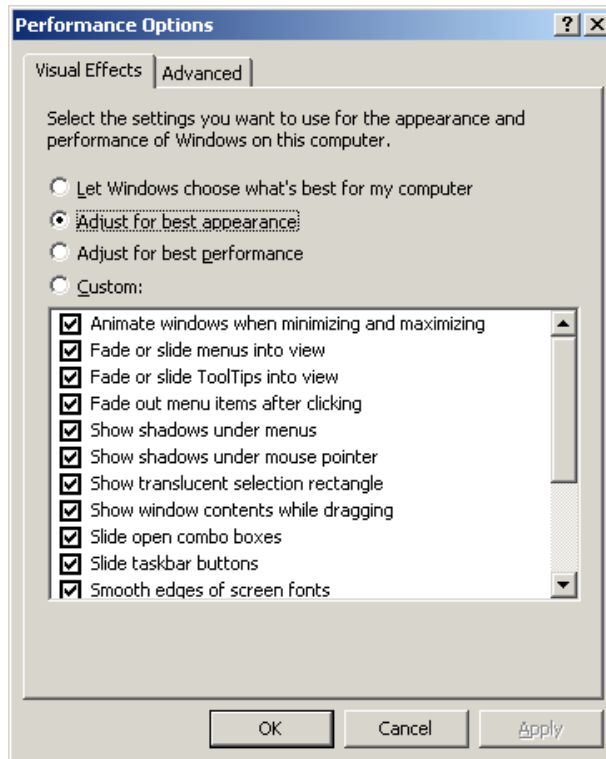


Figure 26 – Performance Options:Visual Effects

The Visual Effects tab allows you to adjust the graphical representation of Windows, and optimize your performance by letting Windows choose the right settings, adjusting for appearance, adjusting for performance or creating a custom template.

The Advanced tab has several options for improving the performance of your server, depending on how you intend to use the system. It consists of three sections:

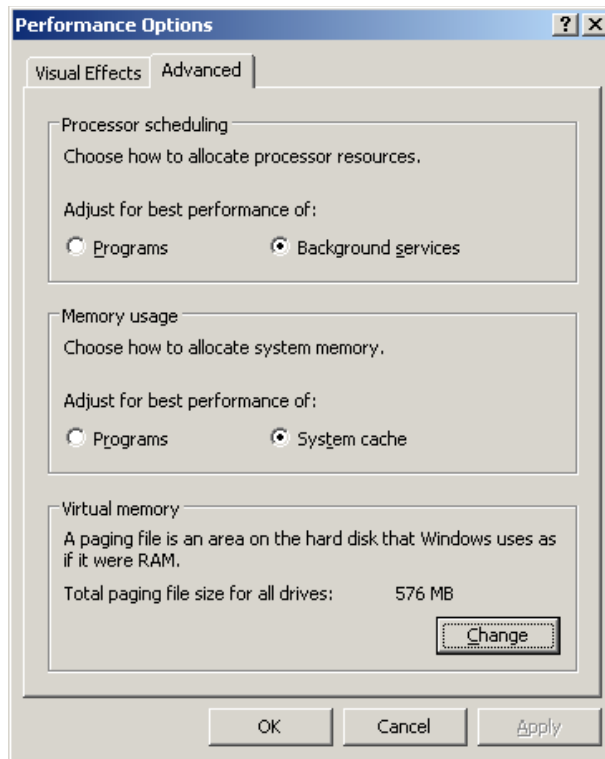


Figure 27 – Performance Options: Advanced

- Processor Scheduling – This section lets you configure how the processor resources will be allocated. Choose the Programs option to increase your foreground application performance. The Background option is best for use with programs that run “out of sight” like backups or web.
- Memory Usage – This section adjusts how the system will use its memory resources. You can choose the Programs option to optimize your server for running user applications. The System Cache option is used for a server that requires a large portion of cache memory.
- Virtual Memory – This section allows you to adjust the page file size on your server. The default page file size is 1.5 times memory, and is created on the system volume as pagefile.sys. To optimize performance, place the page file on a different drive than the system files; don’t spread the file across partitions on the same disk, and don’t place it on a RAID volume.

## Manage a Web Server

IIS 6.0 architecture has been thoroughly redesigned from IIS 5.0/5.1 in terms of security and reliability. The key concept is “isolation”, meaning that a faulty process or unresponsive application will not disrupt other processes, and any malicious attack is contained, with less danger of allowing access to other components and services running on the Web server. This compartmentalization has also been designed with minimum disruption or interruption of service, and continuous uptime as a goal.



## Worker Process Isolation Mode

Most notable is the ability to run in Worker Process Isolation Mode. This separates the actual user processes from the WWW service proper, which allows:

- Multiple Application Pools, with unique configuration for each.
- Application Pool Assignments - Each pool can be assigned to handle one or several applications or sites (sites are treated as applications).
- Application Pool Queue Length Limits, regulating the number of requests accepted for each application pool.
- Web Gardens (for multiprocessor servers); application pools containing multiple worker processes serving requests - These can be assigned to separate processors so that a jam on a process does not interfere with other processes running on the machine.
- Kernel-Mode Queuing - If a worker process fails and stalls out an application pool, requests to that pool will be placed in a queue and the WWW service will start another process to handle them.
- Health Monitoring - The WWW service monitors worker processes; if one fails, it gets killed and another is started to replace it and serve the request. It may also be set to continue for diagnostic purposes when it fails and is replaced.
- Idle Process Timeout - Application pools are shut down if idle for a configurable period.
- Rapid-Fail Protection - An application pool can be set for automatic disable if it fails repeatedly.

As not all Web applications are yet compatible with worker process isolation mode, IIS 5.0 isolation mode is available as well. Clean installs run worker process isolation mode by default.

## Methods of IIS Administration

As with all recent versions of IIS, there are several options to administer Web sites and servers. IIS Manager in the MMC remains the basic method of managing IIS computers on your intranet. Terminal Services and the IIS Remote Administration (HTML) tool are still used to manage remote systems running IIS, along with ADSI and WMI. There is also a set of eight supported command-line scripts that can be used as is or modified to suit (if modified, they must be saved with a different filename).

The biggest change is in the IIS6 metabase. This is equivalent to a high-speed Registry in a Windows OS: it contains configuration information and now resides in two plain-text (as opposed to the old binary) XML files, MetaBase.xml and MBSchema.xml. These can now be read and edited manually or by using scripts. The IIS6 metabase can now be edited while IIS is running, and the changes applied directly to memory without interruption of service if so configured. Any previous versions of the metabase can be restored quickly with no disruption of service as well. Site and application configuration settings are easier to import and export using Admin Base Object (ABO) methods. Backing up the metabase and restoring it locally with a password is a new ADSI function.

## Other IIS Features

The FTP Service has been secured more tightly against tampering; users employing FTP to upload content are isolated into their own home directories with no access to higher levels of the tree. This allows a user full freedom to manage his or her file transfers, without exposing the IIS infrastructure.

FrontPage 2002 Extensions are fully supported in IIS6, and include new security and monitoring features. IIS6 log files can now be recorded in UTF-8 (Unicode Transformation Format, 8-bit) format for languages other than English. ASCII log file formats are W3C Extended log file format, IIS log file format, NCSA Common log file format, ODBC logging, and Centralized binary logging. With the Remotable Certification Object, SSL certificates may be managed locally and remotely through a COM object (MMC/IIS Manager can only do this locally).

*There is an important change in 2003 Server that you should know about.* IIS is by default NOT installed when the basic server OS is installed clean, and if IIS6 is selected for installation, its initial default configuration is highly locked-down and serves only static content; dynamic content such as that offered by ASP, ASP.NET, Server-Side Includes, WebDAV publishing, and FrontPage 2002 Server Extensions may not function until enabled. While the sense of all this may seem obvious, it is advertised as a major feature in Microsoft's new emphasis on security. At the least, it does save a bit of planning - a server planned for dedicated SQL, file/print, or Exchange duty with no WWW/FTP functions intended will not have a loose IIS installation emplaced through sins of Admin omission, thus "reducing the surface area of exposure" to attack. With the above in mind, upgrading IIS from previous versions to IIS6 *does* result in all functions *fully-enabled*.

## IIS Installation

IIS may be installed after 2003 Server installation by means of three methods:

- Configure Your Server wizard
- Control Panel
- Unattended setup

### Configure Your Server Wizard

Click Start | Manage Your Server; from Managing Your Server Roles, click Add or Remove a Role. This starts the Configure Your Server Wizard. Under Server Role, click Application server (IIS, ASP.NET) and finish out the wizard-guided steps. (This will enable ASP.NET functionality by default!)

### Control Panel

Start | Control Panel | Add or Remove Programs | Add/Remove Windows Components; click Application Server | Details | Internet Information Services Manager. Under Details, select all IIS optional components you want installed. There are subcomponents under the WWW Publishing Service available under Details; select those desired and complete the wizard.

### Unattended Setup

Setting up IIS6 on multiple Win 2003 servers may be accomplished by creating an answer file and running WINNT32.EXE with the desired options. A list of these switches can be viewed by inserting the W2003 Server CD-ROM, going to the command line, switching to the CD-ROM drive and the i386 directory (IA64 directory for Itanium-based machines), and entering WINNT32 /?.

## IIS Authentication Methods

From IIS Manager, expand the desired server, then expand Web Sites; right-click the object to be configured and open Properties. Click Directory (or File) Security; under Anonymous and access control click Edit. Select the check box(es) beside the authentication method(s) to be applied, and OK.

What's available:

- Anonymous access - Works through the "IUSER\_%computername%" default account, which is a member of the Guests group and therefore subject to NTFS restrictions.
- Integrated Windows authentication - Also known as NTLM or Challenge/Response; uses Kerberos 5.
- Basic authentication - Takes a username and password, which are sent over the wire in the clear.
- Digest authentication for Windows domain servers - Similar to Basic authentication, except that the user credentials are sent as an MD5 hash. The hash values are stored in the AD service for more control and security.
- Microsoft .NET Passport authentication - Offers a single sign-in to an array of Web services. The .NET Passport credentials must be contained in a cookie or in the actual request to the Web server configured to accept them.
- Another layer of access control is also available, based upon the properties of the requesting computer itself instead of user credentials. It's possible to Grant or Deny access to the host's IP address, network ID, and domain membership. Go to IP Address and Domain Name Restrictions and click Edit.

More New IIS Security Features:

- The Administrator is able to specify a list of file extensions that IIS6 may serve, exclusively. This is intended to limit a potential attacker's access to the system, since unregistered file types will not be delivered if requested. In addition, the system simply returns a "file not found" error instead of revealing the name of a restricted resource that does in fact exist.
- Users authenticating by means of Anonymous Access have no NTFS Write permissions.
- IIS6 is configured by default not to run command-line tools (except through the Administrator account), hindering execution of command-line server-side scripts. This defends against typical DoS and attacks.
- ASP.NET filters any script code from user requests before the request is accepted.
- The maximum size of user uploads may be restricted to hamper the emplacement of larger blocks of malicious code.
- IIS6 supports SSL ver 3.0 and TLS (Transport Layer Security), IPv6, and Win2003 IPSec.
- Administrators have an extra layer of control over TCP/UDP listening ports, independent from and in addition to native Win 2003 port restrictions.
- Worker processes (by default) and ASP built-in functions (always and only) run as the new Win2003 account "Network Service", with the bare level of rights minimally necessary to function.
- The existence of requested resources is first verified before the request is passed to any handlers. This step is a defense against attacks that would cause a failure or bog down the system as it searches vainly for a resource that isn't there.

# Managing and Implementing Disaster Recovery

## Perform System Recovery for a Server

### Startup Options

The following are Windows 2003 startup options:

- *Safe Mode* – Starts windows with only a small subset of files and system drivers, hopefully avoiding any driver that causes the system to crash.
- *Safe Mode with Networking* – Adds network drivers and functionality to safe mode.
- *Safe Mode with Command Prompt* – Avoids the Windows GUI, and goes to the command prompt on boot.
- *Enable Boot Logging* – Logs all boot events and driver loading to a file called nbtlog.txt in the system root. All the Safe Mode options will log to this file with this option enabled.
- *Enable VGA mode* – Starts Windows with the most basic video driver settings.
- *Last Known Good* – Starts Windows with the registry and drivers saved during the last successful logon. All other changes, such as ones which may have muddled the system, will be lost, thus giving you a chance to fix things.
- *Directory Service Restore Mode* – Used to restore info on a domain controller. It restores the SYS-VOL directory and the AD service.
- *Debugging Mode* – Sends debugging info through a serial cable.

### Recovery Console

The Recovery Console can be used when, for whatever reason, the machine will not boot. It can be used as a manually pre-installed utility, or by booting from a 2003 Server OS CD.

To install as an option on startup:

- Log on with the Administrator account or as a member of a group with Administrator rights.
- Insert the Windows 2003 Server CD, hit Start, Run; type in %CD\_drive%\i386\WINNT32.EXE /cmdcons
- A message will ask if you wish to install the Recovery Console; click "Yes".
- Click "OK" when completed.
- This will add a folder, "cmdcons" at the root of the drive containing the OS, and a pointer entry to BOOT.INI.
- "Microsoft Windows Recovery Console" will then appear as an option for operating systems upon startup.

If you want this as a startup option, edit BOOT.INI so that there is a few seconds' time interval before the default OS boots. The quick way to edit BOOT.INI is through Control Panel, System, then the Advanced tab; under Startup and Recovery click Settings, then under System Startup click Edit. The default setting is the line "timeout=30"; change it to however many seconds are preferred.

To use Recovery Console from the 2003 Server CD:

- The computer must be configured to boot from the CD-ROM or DVD-ROM drive, and you must be able to log in with Admin rights.
- Insert the Windows 2003 Server CD and start the computer.
- Follow the prompts; when the "Welcome to Setup" screen appears press R, which starts the command-line Recovery Console.
- Select the OS installation to repair and follow the prompts; you must supply an Administrator password.
- Key in the commands that will repair the installation; you can get a full list with "HELP".
- Type "EXIT" and hit Enter to leave Recovery Console and restart the machine.

Commands available in Recovery Console:

- attrib - Changes attributes of selected file or folder.
- bootcfg - Used add to, edit, or remove items from the boot.ini file.
- cd or chdir - Displays current directory or changes directories.
- chkdsk - Runs CheckDisk.
- cls - Clears screen.
- copy - Copies from removable media to system folders on hard disk. No wildcards.
- del or delete - Deletes service or folder.
- dir - Lists contents of selected directory on system partition only.
- disable - Disables service or driver.
- diskpart - Replaces FDISK - creates/deletes partitions.
- enable - Enables service or driver.
- expand - Extracts a file from a compressed file. Use this to extract a driver from a cabinet (.CAB) or compressed file.
- fixboot - Writes new partition boot sector on system partition.
- fixmbr - Writes new MBR for partition boot sector.
- format - Formats selected disk.
- help - Provides online information about the Recovery Console commands.
- listsvc - Lists all services.
- logon - Lets you choose which installation to log on to if you have more than one.
- map - Displays current drive letter mappings.
- md or mkdir - Creates a directory.
- more or type - Displays contents of text file.

- net use - Connects a network share to a drive letter.
- rd or rmdir - Removes a directory.
- ren or rename - Renames a single file.
- systemroot - Makes current directory system root of drive you're logged into.

### **Automated System Recovery (ASR)**

ASR is a built-in functionality in Windows 2003 that allows you to create snapshots of system state data. ASR sets should be created on a regular basis, and should be part of an overall system recovery plan. The ASR is used as a last option for system recovery, after other attempts to restore with startup options.

ASR is accessed by pressing F2 during the text mode of startup. You will be prompted to enter a floppy, and the server will then read disk configuration and other information from the disk, and attempt to restore the backup.

Some notes on ASR:

- ASR only takes a snapshot of system information, not data files. Preserve your data files through your normal backup routine.
- Use the "All information on this computer" option to create a floppy and ASR data set.
- You must convert FAT16 volumes to NTFS if their size is > 2.1 GB.

To create an ASR:

- Go to the Accessories menu, and open the Backup utility.
- From the wizard, Choose "Advanced Mode"

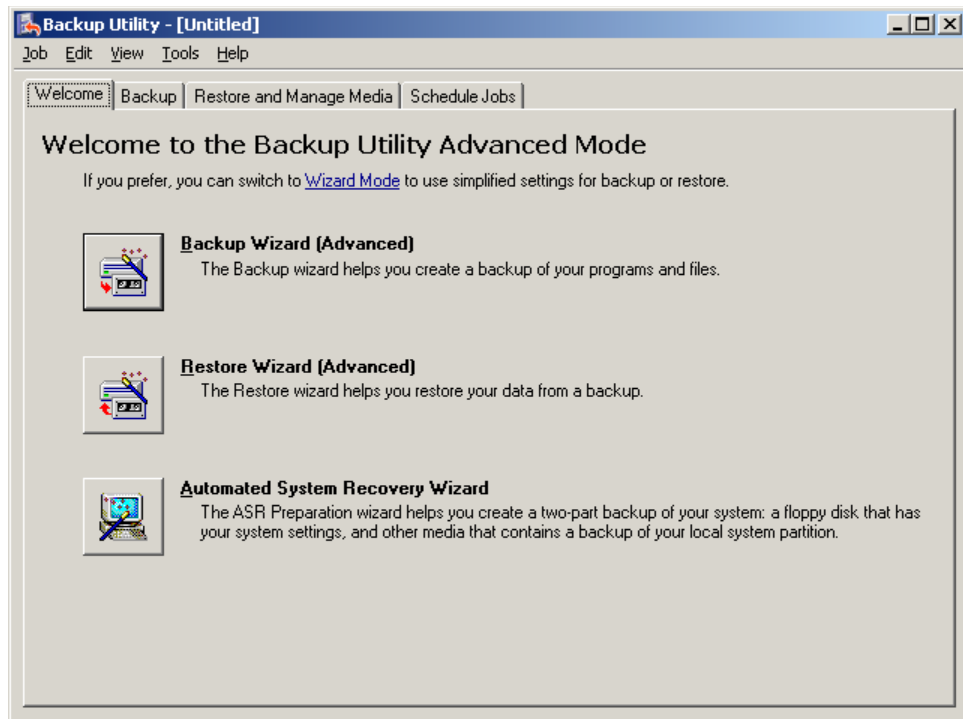


Figure 28 – Backup Utility

- Click on the Automated System Recovery Wizard button.
- The ASR wizard will begin; hit Next.
- Choose the media type, and location of your backup.

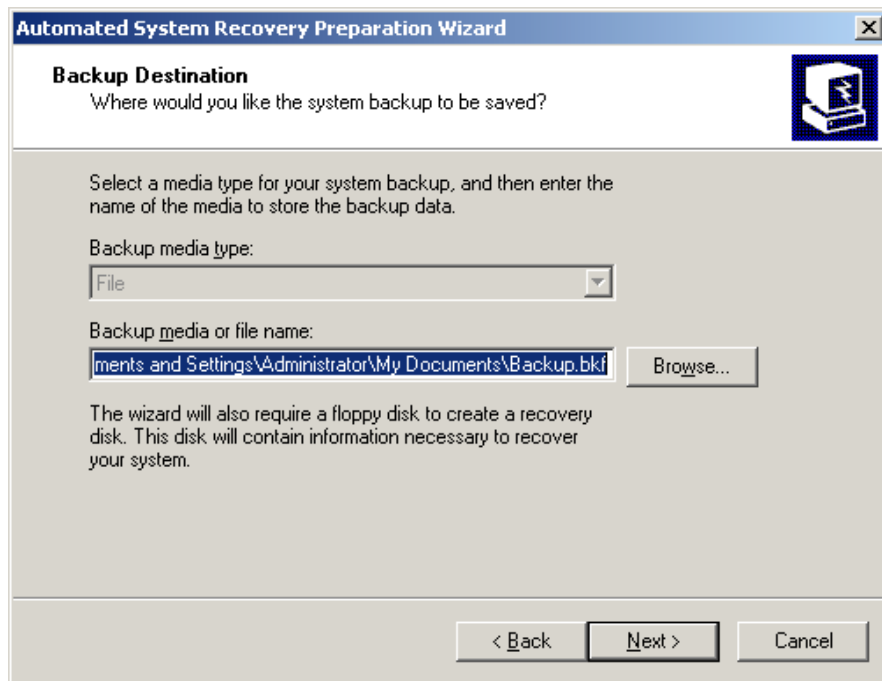
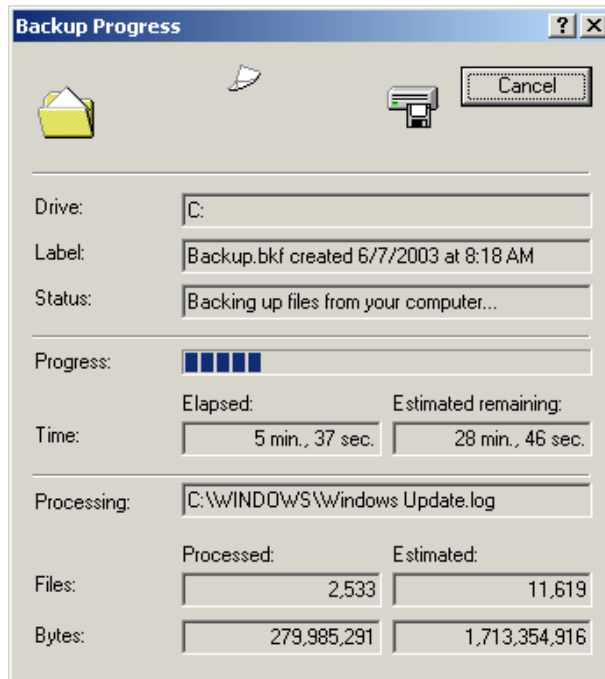


Figure 29 – Backup Destination

- Click Next and Finish.
- The system will begin backing up the necessary information and settings.





**Figure 30** – Backup Progress

You must be a member of the administrators group or Backup operators to accomplish this task.

To recover using ASR:

1. You will need the floppy disk and backup media, the Operation System CD, and any mass storage media drivers.
2. Insert the OS CD, and restart the server.
3. If you need to install drivers, press F6.
4. Press F2 when prompted during setup, and insert the floppy.
5. Follow the instructions.

### Troubleshooting the Boot Process

ARC paths in BOOT.INI:

The Advanced Risc Computing (ARC) path is located in the BOOT.INI file and is used by NTLDR to determine which disk and partition contains the operating system.

ARC path makeup:

multi(x)

Specifies a SCSI controller with the BIOS enabled, or a non-SCSI controller.

x=ordinal number of controller.

scsi(x)

Defines a SCSI controller with the BIOS disabled.  
x=ordinal number of controller.

Either multi(x) OR scsi(x) is used; not both.

disk(x)

Defines the SCSI disk on which the OS resides.  
When multi is used, x always =0.  
When scsi is used, x= the SCSI ID number of the disk with the OS.

rdisk(x)

Defines the disk on which the OS resides.  
Used when OS does not reside on a SCSI disk.  
x=0-1 if on primary controller.  
x=2-3 if on multi-channel EIDE controller.

Both disk(x) AND rdisk(x) must be present in the command.

partition(x)

Specifies the partition number on which the OS resides.  
x=cardinal number of partition, and the lowest possible value is 1.

An example of a BOOT.INI entry would be

```
multi(0)disk(0)rdisk(0)partition(1)
```

This directs NTLDR to look for the first partition of the first disk on the first controller.

### **BOOT.INI Switches**

These include:

- /basevideo - Boots using standard VGA driver.
- /fastdetect=[comx,y,z] - Disables serial mouse detection on all COM ports if port not specified. Included by default.
- /maxmem:n - Specifies amount of RAM used. Use it when a memory chip may be bad, or to simulate a computer with less RAM for testing purposes.
- /noguiboot - Boots Windows without displaying graphical startup screen.
- /sos - Displays device driver names as they load.
- /bootlog - Enables boot logging.
- /safeboot:minimal - Boot in safe mode.
- /safeboot:minimal(alternateshell) - Safe mode with command prompt.
- /safeboot:network - Safe mode with networking support.

**Booting in Safe Mode**

Enter safe mode by pressing F8 during the operating system selection phase. Safe mode loads basic files/drivers, VGA monitor, keyboard, mouse, mass storage and default system services. Networking is not started in safe mode unless specified.

**Last Known Good Configuration**

On bootup, the computer may be started using the LastKnownGood (LKG) configuration. This restores some of the Registry configurations used at the last successful boot (from HKLM\System\CurrentControl-Set only; changes to other keys will remain intact) and is most often used to recover from a crash caused by installing the wrong driver. Go immediately to Event Viewer and check the logs for clues. Most likely, removing the last driver installed will be the best next move; be warned that there may be other repairs to make as well.

To access the LKG, use the F8 key on startup. This will interrupt the boot process and go to a troubleshooting screen. Navigate to Last Known Good Configuration with the arrow keys. Select the operating system to boot from (if necessary).

## Managing Backup Procedures

The Windows Backup utility gives the administrator the capability to perform several different types of backups on a specific system, or network drive. The following are the backup types:

- **Daily** – This provides backup for all files that are modified on the day that the backup is performed. This type of backup does not clear the archive bit.
- **Copy** – This copies all the files, but does not clear the archive bit. This is a useful backup to use in-between incremental and normal backups, as it does not affect them.
- **Differential** – This type provides a backup of all files that have been created/changed since the last full/incremental job. It does not clear the archive attribute. To do a restore when using normal and differential backups, you would restore the last normal, as well as the last differential.
- **Incremental** – The incremental backup copies those files that have been changed/created since the last incremental, or normal backup. It clears the archive bit. Using incrementals requires you to restore the last normal, and all the incrementals. Thus compared to differential backups and restores, incremental backups are quicker but incremental restores take longer.
- **Normal** – This is the standard backup type, and copies all the files, and clears the archive bit.

**The Volume Shadow copy Service (VSS)** is unique to Windows Server 2003 and Windows XP. Microsoft recommends not disabling it. This service will take a snapshot of the state of a volume at the instant the backup starts, providing consistency of data at the given backup time. It also issues a notification of backup to applications and services so that they can prepare. Disabling the VSS will revert the backup solely to features in previous versions of Windows.

To set the default backup type in the Windows Backup utility:

1. Open the Backup utility.
2. Go to Tools, and select Options.
3. Click on the Backup Type tab, and choose the default setting you require.

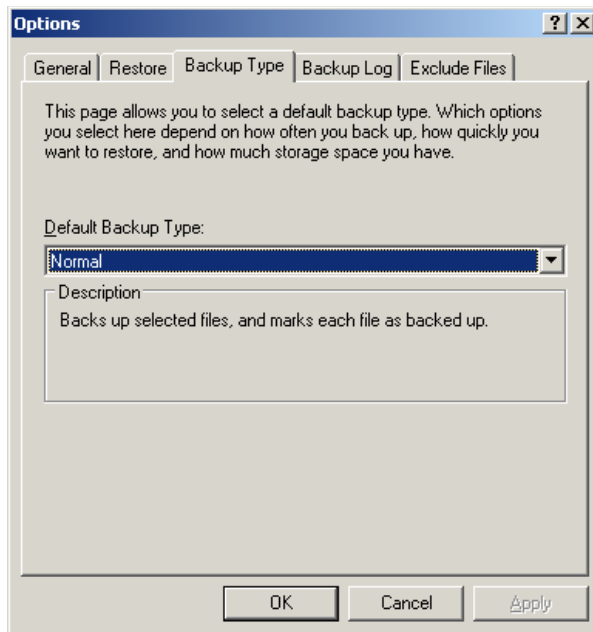


Figure 31 – Backup Type

The Backup utility's advanced features are accessed through the use of the Tools/Options Properties sheet. The selections on this set of sheets allows the following:

- Backup Log Settings – There are 3 choices:
  - ▶ Detailed
  - ▶ Summary
  - ▶ None

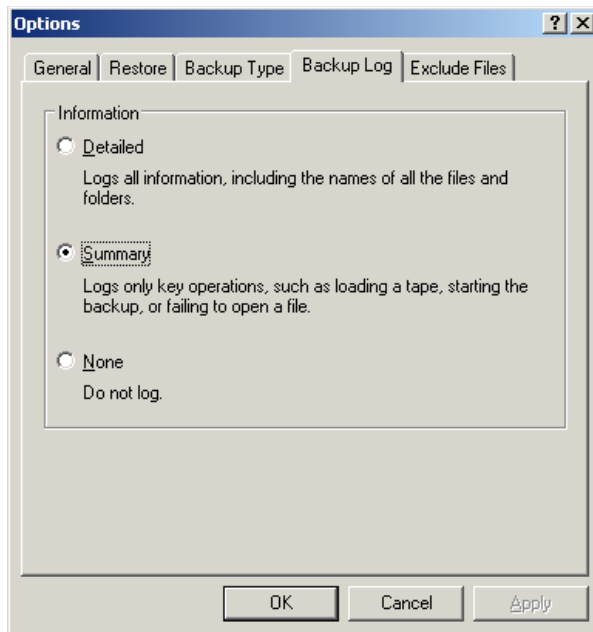


Figure 32 – Backup log settings

- Exclude Files – The ability to exclude file types from backups. You can set types for all users, and types for the administrator account only.

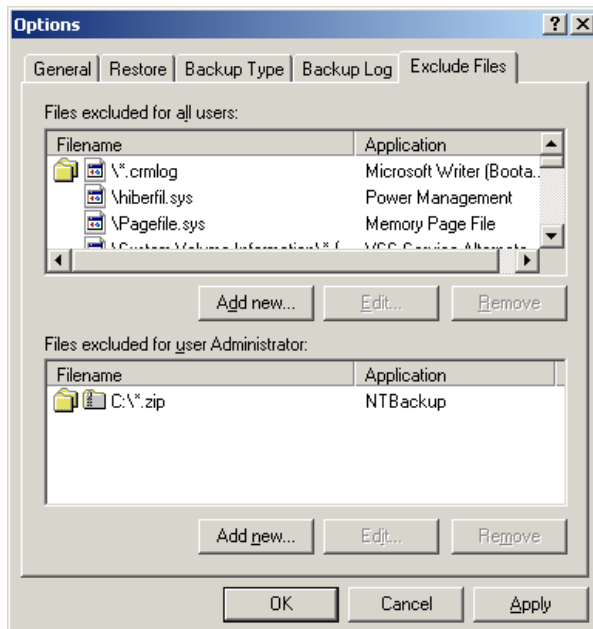
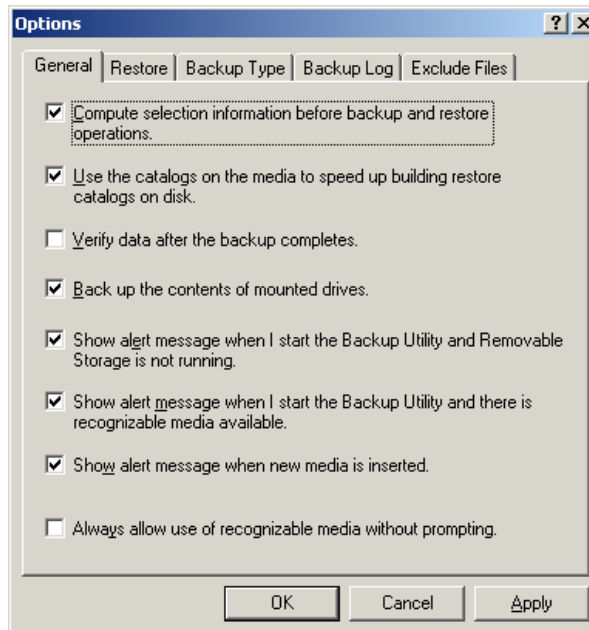


Figure 33 – Excluding files from a backup

- From the Restore tab, you may define how files are restored:
  - Do not replace.
  - Replace older.
  - Always replace.
- The options shown below are on the general tab:



**Figure 34** – General backup options

- Restoring Backup Data

Basic restore procedures:

- Open the Backup Utility, and the wizard should begin.
- Click on the Advanced link to go to the Backup interface, and select the Restore Wizard.
- Click next, and you will be able to choose the Backup to restore.

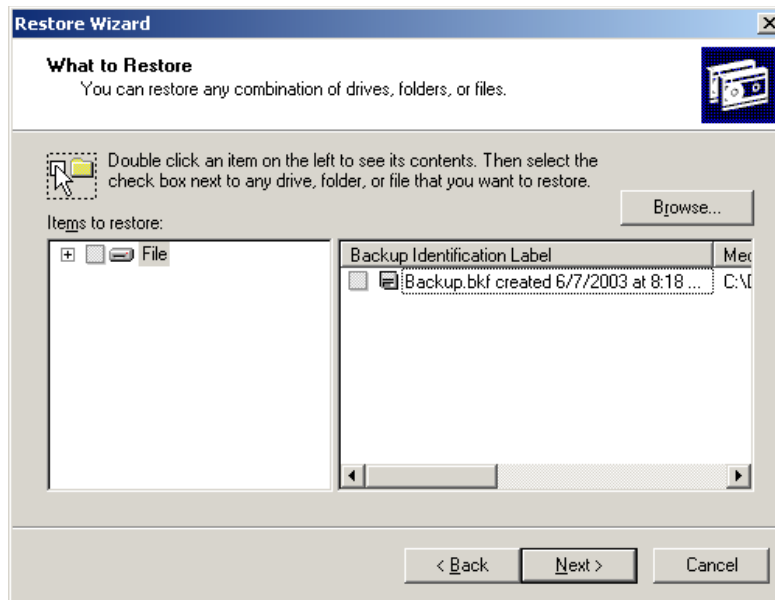
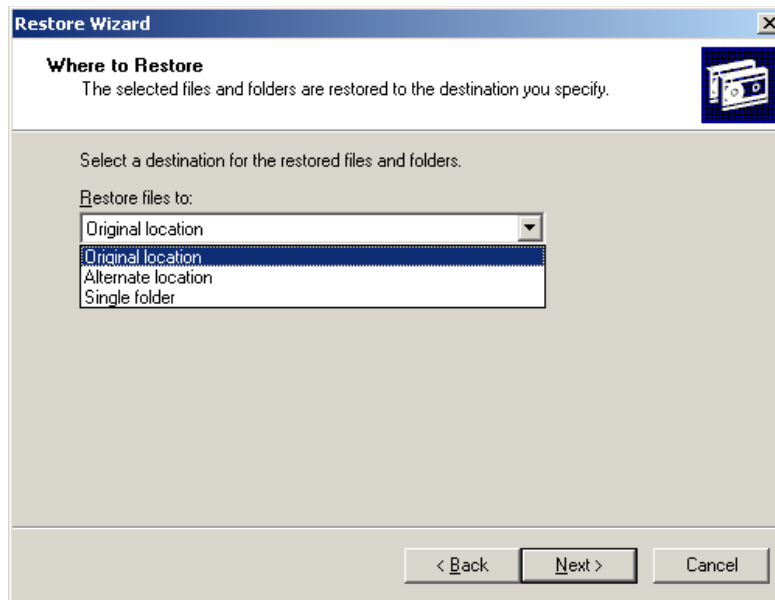


Figure 35 – Restore Wizard

- Choose the files to restore, and click next.
- Click on Advanced to specify details about the restore. The first page will let you choose where to restore:
  - ▶ The original location.
  - ▶ An alternate location.
  - ▶ A single folder (choose this if you want to merge files from different places in the backup set to one location).



**Figure 36** – Choosing where to restore

- You will next be prompted on how to treat the files: leave the existing files, replace the existing files if they are older, or just replace them.
- The next screen allows you to set security settings for the restore. You can restore the security settings, which include file permissions, audit information and ownership. Once you have made your choices, click Next and Finish.



## Scheduling Backup Jobs

To schedule a backup job, follow the procedures below:

- Open the Backup utility, and select the Schedule Job tab:

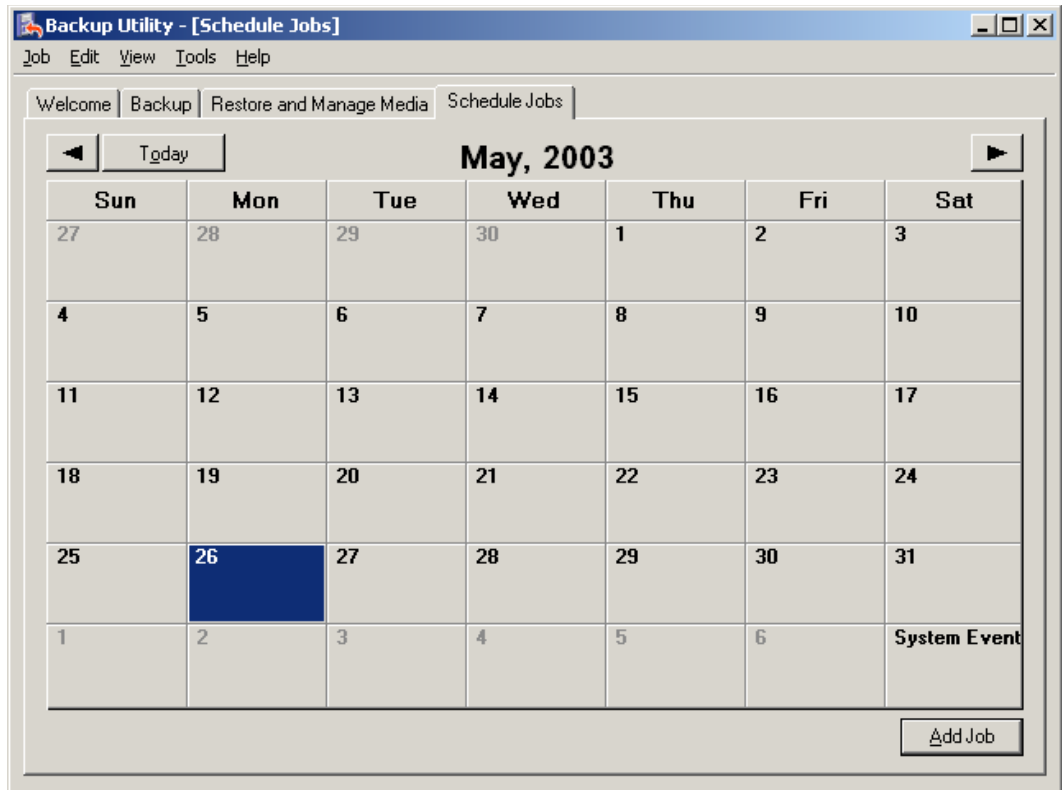


Figure 37 – Scheduling jobs

- Click on the Add Job button.
- The Backup Wizard will begin. Click Next, and you can select the files and folders you would like to backup.

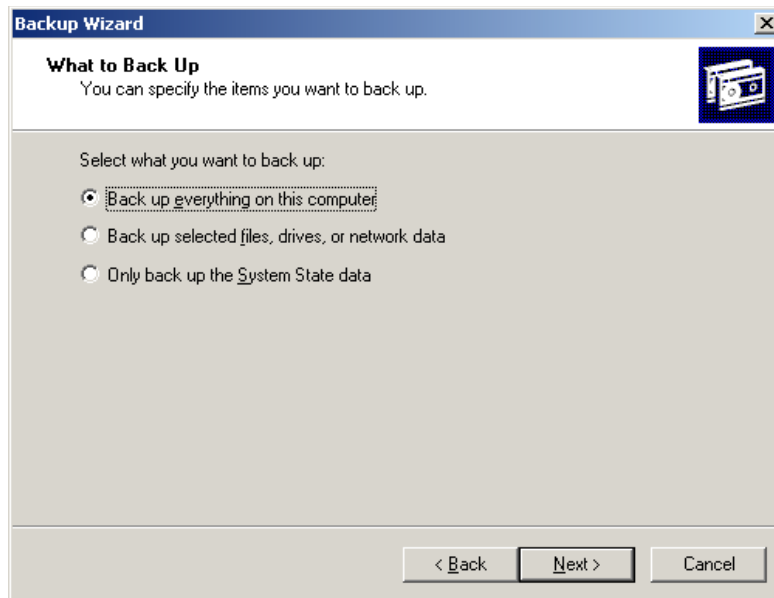


Figure 38 – Choosing what to backup

- Click Next.
- You will be able to select the Backup Type (File, Tape) the place to save your backup, and a Name.

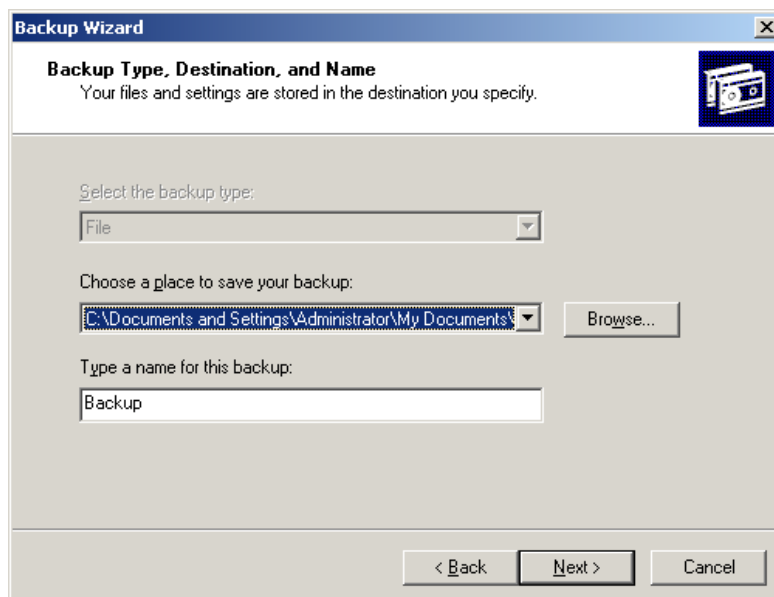
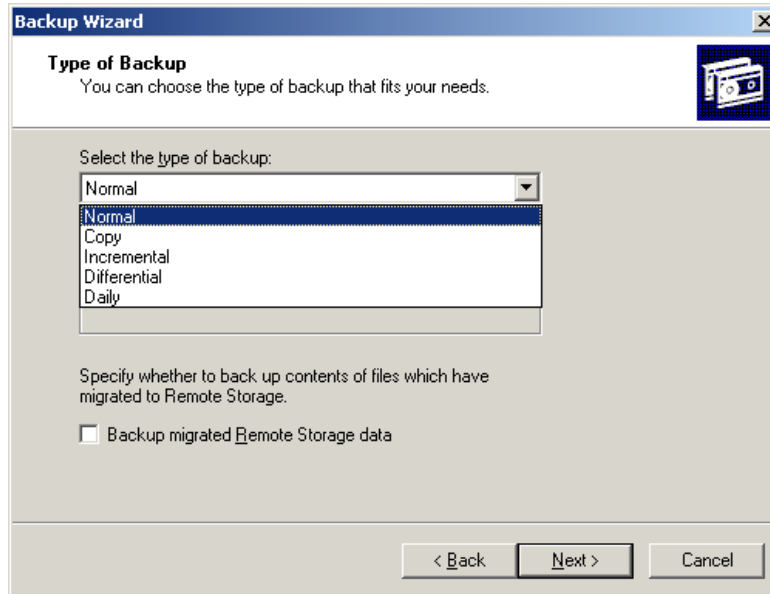


Figure 39 – Choosing where to store the backup

- The next page will allow you to choose the type of backup to perform. These types are defined in a previous section of this exam manual.



**Figure 40** – Choosing the backup type

- Click Next, and now you will be able to choose some options:
  - ▶ Verify Data after Backup.
  - ▶ The ability to use Hardware Compression (if your tape drive supports it).
  - ▶ The ability to disable volume shadow copy (explained below).
- Click Next, and now choose whether to append the backup to an existing backup volume, or replace the existing backups. You can also set security on the backups here, which allows only the administrator or owner to access the backup.

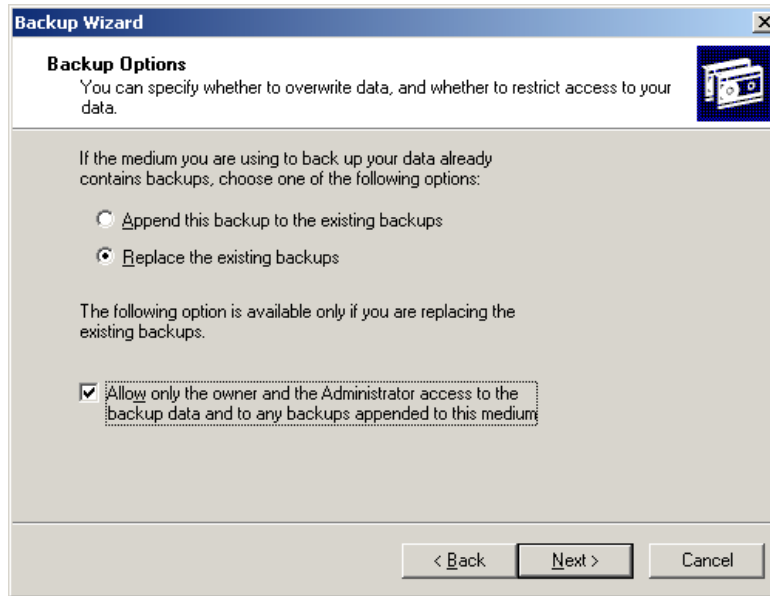


Figure 41 – Choosing other backup options

- Click Next, and you can schedule the backup to occur now, or later.

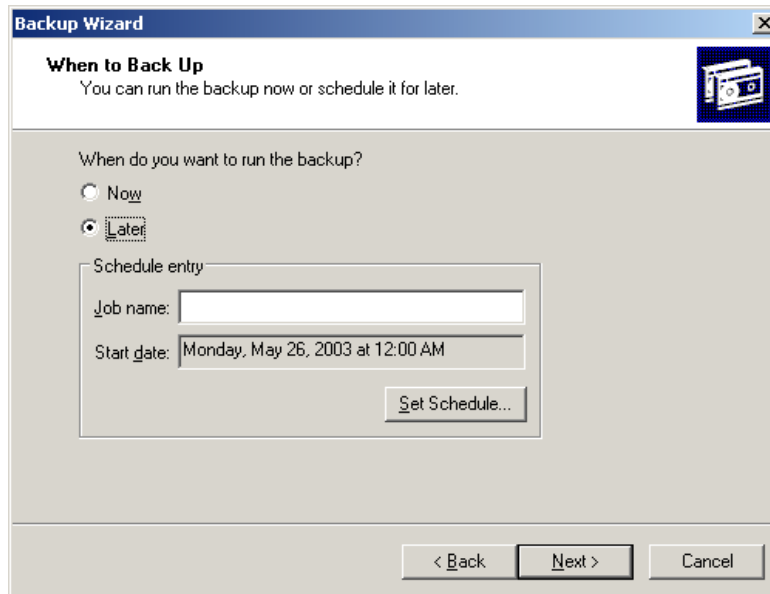


Figure 42 – Choosing when to run the backup

- At this point, click next, and you will be prompted for security information.
- Click Next and Finish.

**Backup Media Rotation**

The *media rotation scheme* that you choose will depend on the number of backup tapes that you have available, the size/configuration of your network and the amount of data being backed up. Small organizations may use five tapes to perform a full daily backup (one per day) and re-use them each week. Enterprise organizations may use a brand new tape every day to perform a partial or full backup, and permanently archive older tapes for both security and legal reasons. The needs of most organizations usually fall somewhere between these two extremes.

One of the most popular media rotation schemes is the grandfather-father-son, or *GFS backup*. This scheme is so named because it uses three “generations” of tapes for daily, weekly, and monthly backups:

- *Grandfather* – This is a full backup that is performed every month. Tapes are usually stored for at least a year, preferably off-site.
- *Father* – This is a full backup performed on a weekly basis; tapes are stored for a month.
- *Son* – This backup is performed daily and the tapes are retained for a week. The backup can be full, incremental, or differential depending on the amount of data being backed off and organizational needs.

Be sure to monitor the age of the tapes and take care not to use them beyond their serviceable life as specified by their manufacturer. Tapes should be stored in a temperature and humidity controlled environment, preferably in a fire safe or vault. Make a point of keeping copies of data off-site as well in the event a disaster, natural or otherwise (the World Trade Center attacks were a tragic reminder of the importance of off-site backups).

## Practice Questions

### Chapter 1 Managing and Maintaining Physical and Logical Devices

- Janet works in the test lab for a software development firm. Part of her job is to configure the test servers so that the application developers can load and run their applications on them. To streamline the test process, Janet has decided to set up the test servers so that they will boot six versions of Windows Server 2003. Janet wants to configure the single disk on the test servers as follows:

  - C: 10GB (Primary Partition)
  - D: (Reserved for CD-ROM)
  - E: 10GB (Primary Partition)
  - F: 10GB (Primary Partition)
  - G: 10GB (Logical Drive)
  - H: 10GB (Logical Drive)
  - I: 10GB (Logical Drive)

After explaining her plan to her supervisor, he tells Janet that it won't work. What is the most likely explanation for Janet's inability to boot from all six of the displayed partitions?

  - A. The fifth partition on a basic disk must be a volume.
  - B. Janet cannot create more than four partitions on the disk.
  - C. You cannot boot from logical drives.
  - D. You cannot mix primary partitions and logical drives on the same disk.
- You are one of the server administrators in your Windows Server 2003 domain which is configured at a Domain functional level of Windows Server 2003 interim. You have been tasked to convert all of the drives that are attached to a Windows Server 2003 system named PRTSRV006 to dynamic. After successfully using Disk Manager to convert all of the physical disks in your server, you try to convert the disk in a USB 2.0 connected drive that you use for archiving sensitive files. However, when you try to select the option to convert the disk to dynamic, the option is not displayed. Why is the Convert to Dynamic disk option not displayed?

  - A. You must be a member of the local administrators group.
  - B. Dynamic disks are not supported in laptops or removable disks.
  - C. Dynamic disks are not supported in Windows Server 2003 via a USB 2.0 interface. You will need to use USB 1.1.
  - D. You need to run Chkdsk before the drive can be converted.

3. You are the system administrator responsible for several servers running Windows Server 2003. Another Windows Server 2003 machine failed, and you decided to add the drives from that server to another operational server. After adding the drives to the new server and restarting, you notice that you can't access the new drives. You open the Disk Manager utility and notice that the drive is displaying a status of Foreign.
- Which of the following actions should you take?
- A. Reseat the cables to the disk, then reboot the server.
  - B. Run Chkdsk.
  - C. Select the option to Reactivate the disk.
  - D. Import the disk.
4. James works as the system administrator for a large legal firm. The firm has a large amount of old files that they do not want on their production servers, but will need to be accessed occasionally. All of the old files are safely stored on backup tapes and will not be modified. The firm wants the files to be available, with great read performance, but they want to spend the least amount of money, so they don't want to use any more disks or disk space than needed.
- Required Result:  
Old files should be readily available.
- Optional Results:  
Archive old files using the least amount of space.  
Provide great read performance.
- Proposed Solution:  
Configure a Windows Server 2003 server with a mirrored volume for file storage.
- Which result(s) does the proposed solution produce?
- A. The proposed solution produces the required result but neither of the optional results.
  - B. The proposed solution produces the required result and one of the optional results.
  - C. The proposed solution produces the required result and both of the optional results.
  - D. The proposed solution does not produce the required result.
5. Jan is a junior administrator for a network that consists of 20 servers running Windows Server 2003 hosting various roles, as well as 500 Windows 2000 Professional clients and 2000 Windows XP Professional clients.
- After having several driver-related issues on the servers, the lead administrator has locked everything down, so that in the future, only signed drivers can be installed. Jan has been instructed to inventory all of the servers running Windows Server 2003, and locate any unsigned drivers.
- What is the easiest way for Jan to generate a list of the unsigned drivers that are installed on her servers running Windows Server 2003?
- A. At a command prompt, type the following: `drivers /signed`
  - B. At a command prompt, type the following: `msinfo signed`
  - C. At a command prompt, type the following: `msinfo32`
  - D. At a command prompt, type the following: `sigverif`

## Chapter 2 Managing and Maintaining Access to Resources

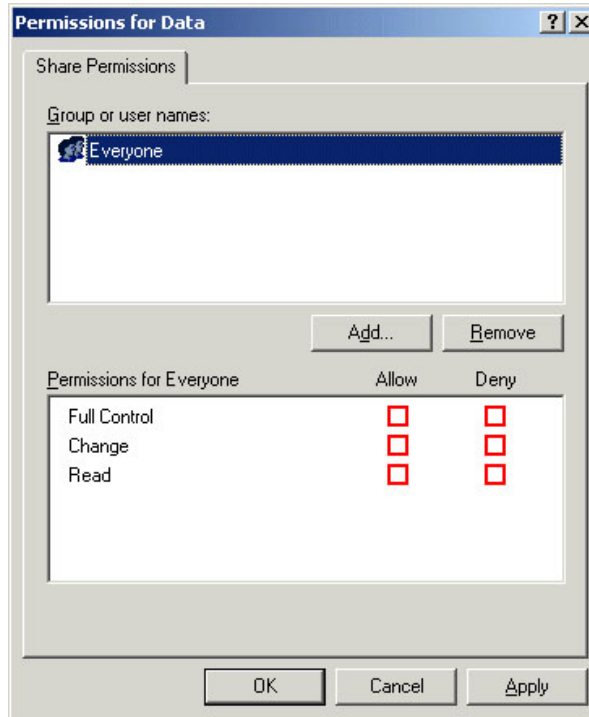
1. Frank is the administrator of a small network with 10 servers running Windows Server 2003. The accounting department has purchased a new application that can be installed only on Windows XP or later. Approximately half of the 300 users in the company require access to the new application. Unfortunately, most of the client computers in Frank's company are running Windows NT 4.0 or older operating systems.  
What technology in Windows Server 2003 will allow Frank to give access to the new application to his users?
  - A. Windows Update
  - B. Remote Desktop for Administration
  - C. Terminal Services
  - D. Telnet
  
2. James is the firewall administrator for a community bank. Because of the sensitive nature of the banking business, they have to be very careful as to what ports are open on the firewall. The bank has purchased and installed a new application to run on a Windows Server 2003 Terminal Server that will be accessed via the Internet.  
Because James will need to open a specific port on the firewall to support the Terminal Services server, he will need to know what protocol Terminal Services uses to communicate with the Terminal Services client.  
What protocol does Windows Server 2003 Terminal Services use to communicate with its clients?
  - A. RDC
  - B. RDP
  - C. ICA
  - D. TCP
  
3. Janet is the system administrator for a firm that performs customer service functions for other companies. The customer service employees all use a small suite of applications that are provided via a Windows Server 2003 Terminal Services session.  
In an effort to provide more fault tolerance, Janet's boss David has requested that she investigate several Windows Server 2003 technologies.  
Which of the following Windows Server 2003 technologies will not provide fault tolerance for a Windows Server 2003 Terminal Services configuration?
  - A. Round Robin DNS
  - B. Network Load Balancing
  - C. Windows Clustering
  - D. Session Directory



4. Janet is the system administrator for BankTwo, Inc., a Windows 2003 Server domain with Domain functional level of Windows 2000 mixed. Janet was requested by the head of the accounting department to create a shared folder on one of the Windows Server 2003 file and print servers to house the monthly balance sheets. Unfortunately, it's Friday afternoon, and Janet is in a hurry to leave the office early for a late tee time.

Janet creates the folder accepting the defaults, then moves the files into the folder.

What groups were granted what permissions on the folder due to her use of the default settings? To answer, click the appropriate option in the exhibit.

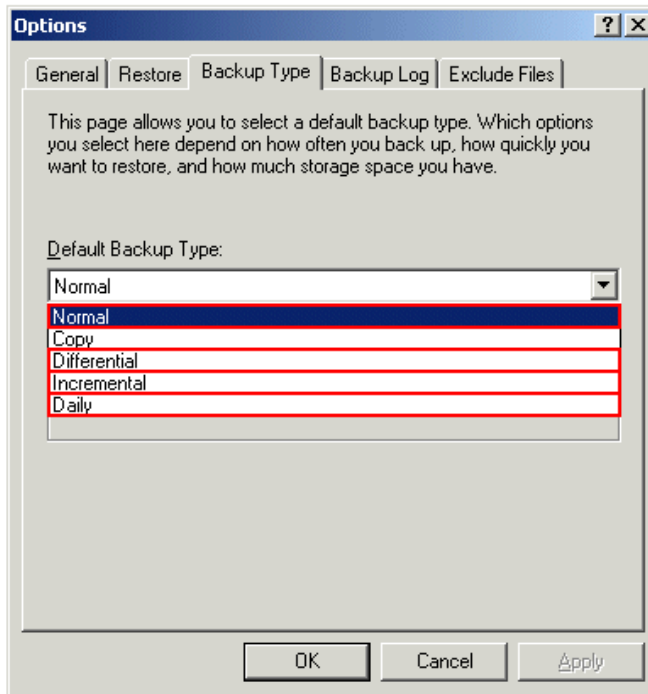


## Chapter 3 Managing and Implementing Disaster Recovery

1. Jeff is the backup operator for MCM, Inc. Jeff is trying to define a backup strategy for the servers running Windows Server 2003 that are used for file and print services in the Windows Server 2003 domain. Jeff plans to run an unattended backup during non-business hours so as not to disrupt normal operations and needs to back up all of the available data.  
Which of the following types of backups can Jeff schedule to run unattended during non-business hours that would allow him to complete his task? (Choose two.)
  - A. Normal backup
  - B. Incremental backup
  - C. Differential backup
  - D. Daily backup
  - E. System State backup
  
2. Mary is one of the backup administrators for BigCo, Inc. After a hardware failure on one of their file and print servers, Mary decides to temporarily restore the contents of one of the volumes on the failed server to another server. The failed volume was 40GB, so she locates a server that has a volume with 50GB of free space.  
Mary mounts the backup media and starts the restore. While she is monitoring the progress of the restore, she receives a message stating that there is insufficient space on the volume that the data is being restored to.  
What is the most likely cause of the insufficient space message?
  - A. The original volume was FAT, the restored volume in NTFS.
  - B. The new volume is marked as compressed.
  - C. The data on the original volume was encrypted.
  - D. The data on the original volume was compressed.
  
3. Mary is one of the backup administrators for BigCo, Inc. One of Mary's duties is to monitor the backup logs to verify the successful completion of the daily backups. BigCo is currently using the Windows Backup utility for their daily backups. While reviewing the backup logs, Mary notices that when the backup program attempts to backup a specific database file, it keeps retrying, then posts an error message, that the retry timeout period has expired and the file was not successfully backed up.  
What can Mary do to make sure that the file will get backed up successfully? (Choose the best answer.)
  - A. Purchase an open file backup add-on utility. Windows Backup can't back up open files without a third-party add-on.
  - B. Use a third-party backup program. Windows Backup can't back up open files.
  - C. Turn On Volume Shadow Copy.
  - D. Stop the database program, back up the file, restart the database program.

4. You are the backup administrator for a small advertising firm based in the Midwest. Your network consists of 5 Windows Server 2003 file and print servers, 3 Windows 2000 Server application servers, and 3 Windows Server 2003 domain controllers, along with a mixture of 400 Windows NT/2000/XP client computers.
- To simplify the network, you want to be able to backup all servers to a central backup server. However, you are on a tight budget. You also want to backup the System State data on all your servers.
- Required Result:**  
All servers should be backed up to a designated backup server.
- Optional Results:**  
Back up System State data on all servers.  
Use as little money as possible.
- Proposed Solution:**  
Buy a tape changer and install it on one of the Windows Server 2003 servers. Use the Windows Server 2003 version of Windows Backup installed on the server with the tape changer to backup all files on all of the servers.
- Which result(s) does the proposed solution produce?
- A. The proposed solution produces the required result but neither of the optional results.
  - B. The proposed solution produces the required result and one of the optional results.
  - C. The proposed solution produces the required result and both of the optional results.
  - D. The proposed solution does not produce the required result.
5. John is the administrator of a Windows Server 2003 Web site for a chemical company, chemicalsrus.com. The Web site is used to promote the products of his company, and to provide an online order entry function that now supports about 50% of the company's sales.
- One morning, John gets a call from the help desk telling him that it seems that the Web server isn't working. John walks into the server room reboots the server and receives the following message "NTLDR is missing. Press any key to restart."
- What Windows Server 2003 technology will assist John in quickly restoring his Web server to operation?
- A. Recovery Console
  - B. Safe Mode
  - C. Automated System Recovery (ASR)
  - D. Emergency Repair Disk (ERD)

6. You decide to reconfigure the TCP/IP Registry settings to improve the speed of the network throughput in your Windows Server 2003 server. You use Regedit to edit the Registry. When you restart the computer, it stops responding before the logon screen appears. What can you do to restore your server to its previous condition?
- A. Restart the computer by using the Recovery Console. Run the fixboot c: command, and then run the Exit command.
  - B. Restart the computer by using the Recovery Console. Run the enable winlogon service\_auto\_start command and then run the Exit command.
  - C. Restart the computer, and select Last known good configuration at the boot menu.
  - D. Restart the server from your Windows Server 2003 boot diskettes. Select the option to restore the server using the Emergency Repair Disk (ERD).
7. You are the backup administrator for a small advertising firm based in the Midwest. Your network consists of 5 Windows Server 2003 file and print servers, 3 Windows 2000 Server application servers, and 3 Windows Server 2003 domain controllers, along with a mixture of 400 Windows NT/2000/XP client computers. You are trying to define an appropriate backup strategy for your firm. You will need to backup all of your servers everyday. If you perform a Normal backup every Saturday, which backup method should you use on the other days to minimize the restore time? To answer, select the appropriate backup type in the Default Backup Type list box in the exhibit.



## Chapter 4 Managing and Maintaining a Server Environment

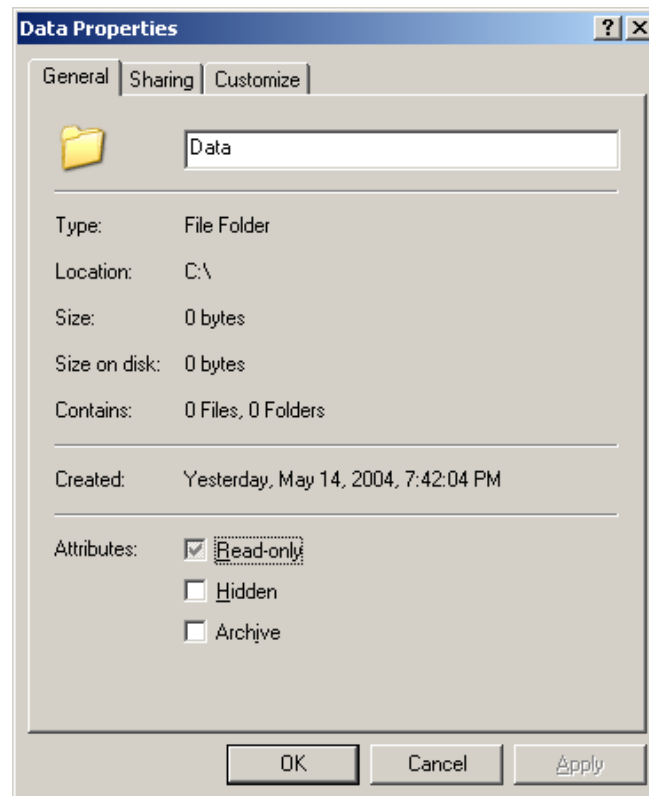
1. Sarah is the system administrator for a small painting firm based in the Pacific Northwest. Sarah suspects that someone is accessing several sensitive files on one of her Windows Server 2003 file servers.

In an attempt to identify which files are being accessed and by whom, Sarah attempts to enable auditing on a sensitive folder. She opens the Local Group Policy MMC on the server, and enables the Audit Object Access selection under Audit Policy. After closing the MMC and opening the Properties dialog for the folder (shown in the exhibit), she can't seem to locate the option to turn auditing on.

Why can't Sarah turn auditing on for the folder?

- A. Auditing can be enabled only at the domain level.
- B. Sarah must restart her server before she can enable auditing.
- C. The folder is on an NTFS volume.
- D. The folder is on a FAT volume.

### Exhibit(s):



2. John runs a small business out of his home and doesn't have a lot of money to spend on computer equipment. He is going to need to have this Windows Server 2003 system perform multiple roles. The major role will be as a Web server. However, John's hardware budget is limited, so he only has a single Network Interface card and a single IP address from his ISP. What technology in Windows Server 2003 can be used to allow John to host multiple Web sites on his server?
- A. HTTP Custom Headers
  - B. Virtual Directories
  - C. Host Headers
  - D. ISAPI Filters
3. Connie is the system administrator for an advertising firm. Due to the nature of the business, their file servers are used to store a large quantity of graphics files, some of which take up a lot of space. Because Connie is starting to run low on free space on the file server, she has decided to require the users to manage their use of space. The users will be allowed only a certain amount of space on the server, and they will have to archive or delete their old files. In addition, she wants both herself and her users to be notified when they are running low on file space.
- Required Result:  
The users' space on the volume must be limited.
- Optional Results:  
Connie wants to be notified when users are running out of disk space.  
Notify users when they are running out of space.
- Proposed Solution:  
Turn on Disk Quotas for all users; configure the quotas so that they send out a notification when the users reach their warning threshold.
- Which result(s) does the proposed solution produce?
- A. The proposed solution produces the required result but neither of the optional results.
  - B. The proposed solution produces the required result and one of the optional results.
  - C. The proposed solution produces the required result and both of the optional results.
  - D. The proposed solution does not produce the required result.
4. Jack is the system administrator for a small market research firm. The firm has a database mining application that runs once a month. This application is usually running during the day, at the same time other users are trying to run their applications. How can you run this application with the least amount of performance impact for the other users?
- A. Use Task Manager to set the database application to a priority of 6.
  - B. Use Task Manager to set the database application to a priority of Below Normal.
  - C. Use Task Manager to set the database application to a priority of Realtime.
  - D. Use Task Manager to set all of the other applications to a priority of 15.

5. Maria works on the performance team in the Kansas City Network Control Center for a large telecommunications company. Maria is responsible for troubleshooting performance problems on the various servers in the enterprise.

One afternoon, the help desk calls Maria and tells her that they have received several calls from users reporting performance problems on a server running Windows Server 2003. Maria looks at her server locator and sees that the server is located in the Dallas data center. Maria will use one of the following tools to diagnose this problem.

To answer, match the following tools with their descriptions. Drag the tool name on the left to the right, dropping it next to the appropriate description.

- A. System Monitor   B. Performance Manager   C. Performance Monitor  
D. Task Manager   E. Event Manager

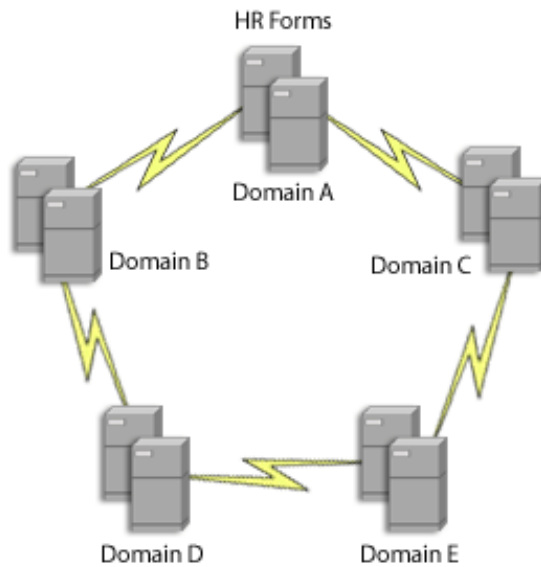
This tool can give you a quick overview of system performance, or can be used to view the logs that were generated using the Performance Logs and Alerts tool. It is capable of monitoring remote servers.	
This tool is not included in Windows Server 2003.	
This tool was included in pre-Windows 2000 operating systems. It is not available for Windows Server 2003.	
This utility is included in Windows Server 2003 to give administrators a way to monitor and manage the state of currently running applications and processes. However, it is not capable of monitoring remote servers.	
This tool is not included in Windows Server 2003.	

## Chapter 5 Managing Users, Computers, and Groups

1. You are the system administrator for a Windows Server 2003 forest that includes the us.abc.com and the europe.abc.com domains. Your company has purchased a high-speed color laser printer for printing brochures for your sales force. Because the printer is very expensive, your company has only purchased one of them for the NY office.  
You make the printer a member of the us.abc.com domain and grant Print permission to the Domain Local Group ColorPrt.  
What is the best way to allow the users in the europe.abc.com domain to print to the printer?
  - A. Give the users in the europe.abc.com domain a user account in the us.abc.com domain.
  - B. Add the users in the europe.abc.com domain to the ColorPrt group in the us.abc.com domain.
  - C. Add the users in the europe.abc.com domain to the Global group Europe\_Prt in the Europe.abc.com domain. Add the Global group Europe\_Prt to the Domain Local group ColorPrt, in the us.abc.com domain.
  - D. Add the users in the europe.abc.com domain to the Domain Local group Europe\_Prt in the Europe.abc.com domain. Add the Domain Local group Europe\_Prt to the Domain Local group ColorPrt, in the us.abc.com domain
  
2. Steven is the security officer for a small bank located in the southwest. The IT manager suspects that someone is logging on to one of the domain controllers and reading the contents of some of the sensitive files. He suspects that it has to be someone that is logging on to the server console, since the share permissions are extremely restrictive.  
Which of the following groups do not have log on locally rights on a Windows Server 2003 domain controller? (Choose two.)
  - A. Power Users
  - B. Users
  - C. Account Operators
  - D. Server Operators
  - E. Print Operators
  
3. You are one of the system administrators for a bank that has multiple locations. Domains in use in this Windows Server 2003 forest are running in Windows 2000 mixed mode. Because some of your tellers rotate between banks, you have decided to implement roaming profiles.  
Which of the following folders is NOT included in a roaming profile? (Choose two.)
  - A. Application Data
  - B. User Data
  - C. Default User
  - D. Start Menu
  - E. My Documents



4. You are the network administrator for a company that has five domains in a Windows Server 2003 forest. The domains are located in separate locations connected by 56K WAN links. There is a folder in Domain A named HRForms that contains medical, dental, and other various forms that most of the employees in the company will need access to. How can you grant access to this folder, while minimizing replication overhead over the slow WAN links?
- A. Create a universal group and assign this group permissions for the HRForms folder. Add the appropriate groups from the other domains to this universal group.
  - B. Create a distribution group and assign this group permissions for the HRForms folder. Add the appropriate groups from the other domains to this distribution group.
  - C. Create a global group and assign this group permissions for the HRForms folder. Add the appropriate groups from the other domains to this global group.
  - D. Create a domain local group and assign this group permissions for the HRForms folder. Add the appropriate global groups from the other domains to this domain local group.

**Exhibit(s):**

# Answers and Explanations

## Chapter 1

### 1. Answer: C

Explanation A. This is not a correct answer as you cannot mix partitions and volumes on the same disk.

Explanation B. This is not a correct answer. You can have up to four primary partitions, or three primary partitions and an extended partition that contains multiple logical drives, on a single physical hard disk that is configured as a basic disk. The basic disk was the only type supported in versions of Windows prior to Windows 2000.

**Explanation C.** This is the correct answer: You can have up to four primary partitions, or three primary partitions and an extended partition that contains multiple logical drives, on a single physical hard disk that is configured as a basic disk. However, logical drives are not bootable.

In order for the system to start in a basic disk configuration one of the partitions needs to be marked as active and needs to contain the Windows boot files. On Intel-based computers running the Windows operating system, the system partition must be a primary partition that has been marked as active for startup purposes.

Explanation D. This is not a correct answer. You can have up to four primary partitions, or three primary partitions and an extended partition that contains multiple logical drives, on a single physical hard disk that is configured as a basic disk. The basic disk was the only type supported in versions of Windows prior to Windows 2000.

### 2. Answer: B

Explanation A. This is not a correct answer. With the account being used you were able to convert all of the physical disks in your server so the account used already had appropriate rights.

**Explanation B.** This is the correct answer: Dynamic disks are not supported in laptops or removable disks, such as Zip disks or disks connected via a Universal Serial Bus (USB) or FireWire (IEEE 1394) interface.

Explanation C. This is not a correct answer. Dynamic disks are not supported in laptops or removable disks, such as Zip disks or disks connected via any version of Universal Serial Bus (USB) or FireWire (IEEE 1394) interface.

Explanation D. This is not a correct answer. Dynamic disks are not supported in laptops or removable disks, such as Zip disks or disks connected via a Universal Serial Bus (USB) or FireWire (IEEE 1394) interface.

### 3. Answer: D

Explanation A. This is not a correct choice as it is not the source of the problem. A disk displaying the status of Foreign tells you that it is a dynamic disk that was removed from a Windows 2000/XP/2003 computer and placed into this Windows Server 2003 computer, but has not yet been imported.

Explanation B. This is not a correct answer as Chkdsk cannot run against a Foreign drive and would not help you to get this disk back from this status.

Explanation C. This is not a correct choice. A disk displaying the status of Foreign tells you that it is a

dynamic disk that was removed from a Windows 2000/XP/2003 computer and placed into this Windows Server 2003 computer, but has not yet been imported.

**Explanation D.** This is the correct answer: A disk displaying the status of Foreign tells you that it is a dynamic disk that was removed from a Windows 2000/XP/2003 computer and placed into this Windows Server 2003 computer, but has not yet been imported. To Import the disk, right-click the disk and select Import Foreign Disks.

#### 4. Answer: A

**Explanation A.** This is a correct answer: Although the solution will make the files readily available, mirroring the volumes requires the purchase of an extra drive, with no increase of usable space. Fault tolerance is not required because the data is static and safely backed up.

Explanation B. This is not a correct answer. Although the solution will make the files readily available, mirroring the volumes requires the purchase of an extra drive, with no increase of usable space. Fault tolerance is not required because the data is static and safely backed up.

Explanation C. This is not a correct answer. Although the solution will make the files readily available, mirroring the volumes requires the purchase of an extra drive, with no increase of usable space. Fault tolerance is not required because the data is static and safely backed up.

Explanation D. This is not a correct answer. Although the solution will make the files readily available, mirroring the volumes requires the purchase of an extra drive, with no increase of usable space. Fault tolerance is not required because the data is static and safely backed up.

#### 5. Answer: D

Explanation A. This is not a correct action to take as it is not a valid command in Windows Server 2003.

Explanation B. This is not the correct answer as Msinfo is not a valid command in Windows Server 2003. The msinfo32 executable will open the System Information tool to display a comprehensive view of the hardware, system components, and software environment on the local computer; it is not the easiest way to generate a list of the unsigned drivers that are installed on servers running Windows Server 2003.

Explanation C. This is not the correct command to use as it will open the System Information tool to display a comprehensive view of the hardware, system components, and software environment on the local computer; it is not the easiest way to generate a list of the unsigned drivers that are installed on servers running Windows Server 2003.

**Explanation D.** This is the correct answer. File Signature Verification checks to see which system files and device driver files are not digitally signed and displays its findings. If you have enabled logging, the search results are also written to a log file.

## Chapter 2

### 1. Answer: C

Explanation A. This is not a correct answer. Windows Update is used to patch Windows 2000 and later operating systems, and cannot be used to provide application access.

Explanation B. This is not a correct answer. The Remote Desktop for Administration feature in Windows Server 2003, provides only three remote connections to the server (two remote sessions plus console).

**Explanation C.** This is the best answer for this question. Terminal Services can be used to run applications on older computers by installing the Remote Desktop Client software.

Explanation D. This is not a correct answer as Telnet would not be able to run a Windows XP compatible application remotely.

### 2. Answer: B

Explanation A. This is not the correct answer as RDC is not a protocol, it is an abbreviation for the Remote Desktop Client.

**Explanation B.** This is the correct answer. RDP is the abbreviation for the Remote Desktop Protocol, the protocol that Windows Server 2003 Terminal Services uses to communicate with its clients.

Explanation C. This is not a correct answer as ICA is the protocol used by the Citrix MetaFrame add-on.

Explanation D. This is not the correct answer as TCP is the abbreviation for Transmission Control Protocol.

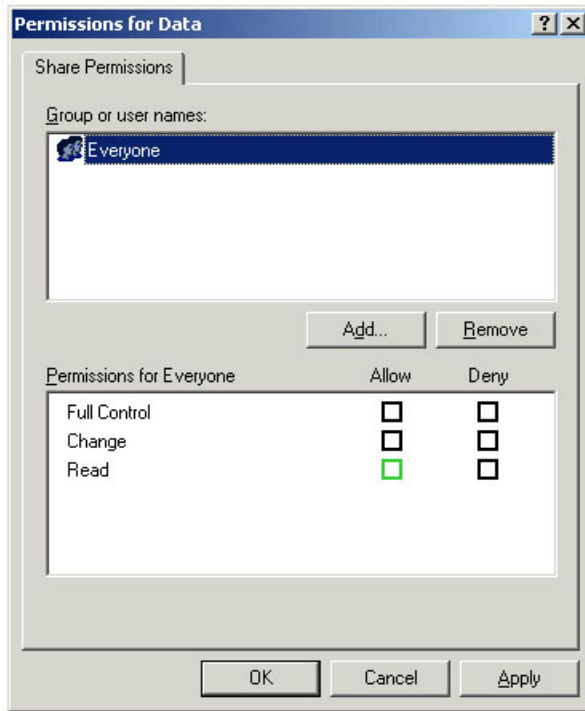
### 3. Answer: C

Explanation A. This is not the correct answer. Round Robin DNS can be used to make a group of Windows Server 2003 Terminal Servers loaded with identical applications to appear as a single server to the Terminal Services clients. This allows the clients to connect to another server if one should fail.

Explanation B. This is not the correct answer. Network Load Balancing can be used to make a group of Windows Server 2003 Terminal Servers loaded with identical applications to appear as a single server to the Terminal Services clients. This allows the clients to connect to another server if one should fail.

**Explanation C.** This is the best answer for this scenario as Windows Server 2003 Terminal Services cannot be clustered.

Explanation D. This is not a correct choice. Session Directory is a new feature in Windows Server 2003 Terminal Services that assures that a disconnected Terminal Services session is reconnected to the correct server.

**4. Answer:**

Explanation: Although Everyone-Full Control was the default permission in previous versions of Windows, in Windows Server 2003, the default share permission is Everyone-Read.

**Chapter 3****1. Answers: A, D**

**Explanation A.** This is one of two correct answers. A normal (sometimes referred to as a Full backup) backup is used to back up all of the files and folders that you select, regardless of the setting of the archive bit. It then clears the archive bit of the files to show that they were backed up.

Explanation B. This is not a correct answer as an incremental backup would only allow for the back up of all of the files that have changed since the last backup, regardless of the backup type and not all of the data as outlined in the question.

Explanation C. This is not a correct answer as a Differential backup would only allow for the back up of all of the files that have changed since the last last full backup and not all of the data as outlined in the question.

**Explanation D.** This is one of two correct answers. A daily backup is used to back up only the files and folders that have been created or modified on that day. It does not read or change the archive bit. A daily backup is typically used to make a quick snapshot of the daily activity.

Explanation E. This is not a correct answer as a System State backup includes the registry, the COM+ Class Registration database, files under Windows File Protection, and system boot files but it would not include all of the data on the system as outlined in the question.

**2. Answer: D**

Explanation A. This is not a correct answer as going from a FAT volume to an NTFS volume will not result in a large difference in allocated drive space.

Explanation B. This is not a correct answer. Moving data from a compressed volume to a compressed volume will result in the same amount of space consumed on the new volume as on the old. Moving data from an uncompressed volume to a compressed volume results in the data being compressed. Data moved between volumes inherits the compression state of the target volume.

Explanation C. This is not a correct answer. Encryption has no effect on the size of files.

**Explanation D.** This is the correct answer. If the data on the original volume was compressed, and the target volume is not, the data will be restored in an uncompressed state, thereby consuming more space. Data moved between volumes will inherit the compression state of the target volume.

**3. Answer: C**

Explanation A. This is not the best answer for this question. The Windows Server 2003 version of Windows Backup can back up open files when the Volume Shadow Copy option is configured.

Explanation B. This is not the best answer for this question. The Windows Server 2003 version of Windows Backup can back up open files when the Volume Shadow Copy option is configured.

**Explanation C.** This is the correct answer. The Windows Server 2003 version of Windows Backup can back up open files when the Volume Shadow Copy option is configured. Using Volume Shadow Copy, you are now able to back up most open files. During a backup, when an open file is encountered, a snapshot is taken of the file. This is an exact copy of the file that is saved to another area on the disk. This copy is then saved via the Backup utility.

Explanation D. This is not the best answer for this question. The Windows Server 2003 version of Windows Backup can back up open files when the Volume Shadow Copy option is configured.

**4. Answer: B**

Explanation A. This is not a correct answer. The solution satisfies the required result, but it only satisfies one of the optional results. Although Windows Backup can be used to back up remote servers and it is free, it cannot back up the Registry or the System State data on remote computers.

**Explanation B.** This is the correct answer. Although Windows Backup can be used to back up remote servers and it is free, it cannot back up the Registry or the System State data on remote computers.

Explanation C. This is not a correct answer. The solution satisfies the required result, but it only satisfies one of the optional results. Although Windows Backup can be used to back up remote servers and it is free, it cannot back up the Registry or the System State data on remote computers.

Explanation D. This is not a correct answer. The solution satisfies the required result, but it only satisfies one of the optional results. Although Windows Backup can be used to back up remote servers and it is free, it cannot back up the Registry or the System State data on remote computers.

## 5. Answer: A

**Explanation A.** This is the best answer for this question. Boot to the Recovery Console, and copy the NTLDR file from the Windows Server 2003 CR-ROM to the root of the system partition.

Explanation B. This is not a correct answer because if NTLDR cannot be found, the Safe Mode will not work.

Explanation C. This is not the best answer for this question. While ASR will recover from this error, it will take longer to perform than other options.

Explanation D. This is not a correct choice as the Emergency Repair Disk is not supported in Windows Server 2003.

## 6. Answer: C

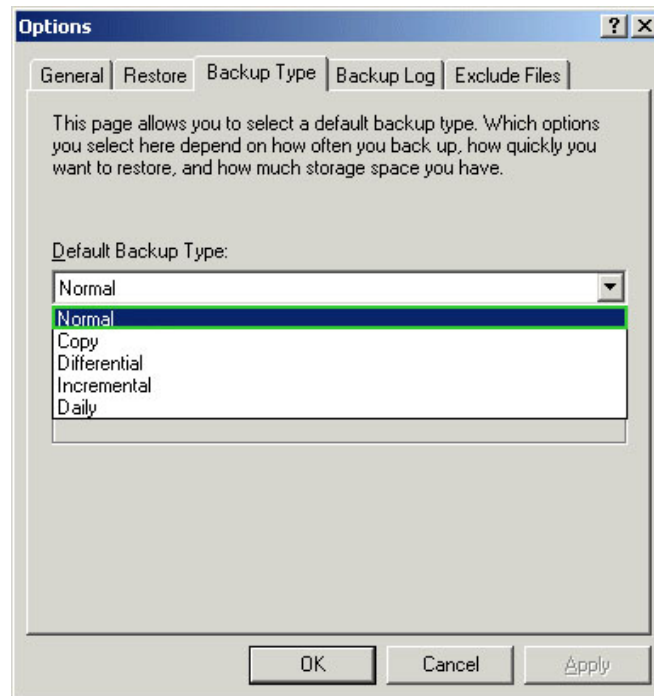
Explanation A. This is not a correct answer. The boot sector is not damaged, so there is no need to run the fixboot command.

Explanation B. This is not a correct answer. The Winlogon service should not have been disabled, so enabling it will not correct your problem.

**Explanation C.** This is the correct answer. When you start your server using the Last Known Good Configuration, system setting changes made after the last successful startup are lost.

Explanation D. This is not a correct answer. There are no boot diskettes for Windows Server 2003; likewise, the ERD no longer exists and it has been replaced by Automated Server Recovery (ASR).

## 7. Answer:



**Explanation:** A normal backup is used to back up all of the files and folders that you select, regardless of the setting of the archive bit. A normal backup has the advantage of only requiring a single media (or set of media) for a full restore.

A daily backup is used to back up only the files and folders that have been created or modified on that day. A differential backup is used to back up only the files and folders that have been created or modified since the last normal or incremental backup. When you perform a full restore, it requires the media for both the last normal backup and the last differential backup.

An incremental backup is used to back up only the files and folders that have been created or modified since the last normal or incremental backup. When you perform a full restore, it requires the media for the normal backup and all the incremental backups performed since the normal backup, which can be time consuming, depending on how many incremental backups you must restore.

## Chapter 4

### 1. Answer: D

Explanation A. This is not a correct answer as Auditing can be enable via either local or domain policy.

Explanation B. This is not a correct answer as restarting the server will have no effect on auditing.

Explanation C. This is not a correct answer as only files and folders on an NTFS volume can be audited.

**Explanation D.** This is the correct answer. Only files and folders on an NTFS volume can be audited.

### 2. Answer: C

Explanation A. This is not a correct answer. Custom headers allow you to add additional information to the HTTP information that is exchanged between the client and the Web server; they cannot be used to host multiple Web sites on a single Windows Server 2003 system running in the Web Server role under a single IP address.

Explanation B. This is not a correct answer. Although Virtual Directories allow you to save multiple Web sites on a server or group of servers, it doesn't enable you to host multiple Web sites with a single IP address.

**Explanation C.** This is the correct answer for this question. A host header is a unique DNS name that is used to identify one of the additional Web sites. The site that is using the host header shares the same port and IP address, but when the browser connects to the default Web site, it asks for the site using the host header entry. This allows you to host multiple sites at the same IP address; they just have to have unique header names, such as www.abc.com, www.xyz.com, and so on.

Explanation D. This is not a correct answer. ISAPI Filters are custom-written filters that respond to specific events during an HTTP request and cannot be used to host multiple Web sites on a single Windows Server 2003 system running in the Web Server role under a single IP address.

### 3. Answer: C

Explanation A. This is not the correct answer for this question. Quotas can be configured so that when users reach a preset warning level, they get a warning message telling them that they are running out of space. The users can continue to save files to the volume until they reach their quota limit. At that time, they are unable to save any more files to the volume. These actions not only generate a message to the users, but they also record an event in the event log.



Explanation B. This is not the correct answer for this question as the proposed solution produces the required result and both of the optional results rather than just one of the optional ones. Quotas can be configured so that when users reach a preset warning level, they get a warning message telling them that they are running out of space. The users can continue to save files to the volume until they reach their quota limit. At that time, they are unable to save any more files to the volume. These actions not only generate a message to the users, but they also record an event in the event log.

**Explanation C.** This is the correct answer for this question as the proposed solution produces the required result and both of the optional results. Quotas can be configured so that when users reach a preset warning level, they get a warning message telling them that they are running out of space. The users can continue to save files to the volume until they reach their quota limit. At that time, they are unable to save any more files to the volume. These actions not only generate a message to the users, but they also record an event in the event log.

Explanation D. Quotas can be configured so that when users reach a preset warning level, they get a warning message telling them that they are running out of space. The users can continue to save files to the volume until they reach their quota limit. At that time, they are unable to save any more files to the volume. These actions not only generate a message to the users, but they also record an event in the event log.

#### 4. Answer: B

Explanation A. This is not a correct choice as Task Manager does not allow you to set a process to a specific number; it only allows you to set priority classes.

**Explanation B.** This is the correct answer for this scenario. The monthly application should be run at a low priority to make the least performance impact on the other applications.

Explanation C. This is not a correct answer and this type of high manual priority setting should not be encouraged. Running the monthly application at a priority of Realtime would take resources away from the other applications.

Explanation D. This is not a correct answer. Task Manager does not allow you to set a process to a specific number; it only allows you to set priority classes.

**5. Answer:**

This tool can give you a quick overview of system performance, or can be used to view the logs that were generated using the Performance Logs and Alerts tool. It is capable of monitoring remote servers.	System Monitor
This tool is not included in Windows Server 2003.	Performance Manager
This tool was included in pre-Windows 2000 operating systems. It is not available for Windows Server 2003.	Performance Manager
This utility is included in Windows Server 2003 to give administrators a way to monitor and manage the state of currently running applications and processes. However, it is not capable of monitoring remote servers.	Task Manager
This tool is not included in Windows Server 2003.	Event Manager

**Chapter 5****1. Answer: C**

Explanation A. Although this will work, creating additional user accounts adds more management overhead for the administrators and creates additional headaches for the users since they have to logon as a different user to print.

Explanation B. Although this will work, it is not a best practice to add users to a Domain Local Group in another domain.

**Explanation C.** This is the correct answer. You should always assign permissions on resources to a Domain Local group, then add Global or Universal groups to that group.

Explanation D. This will not work. You cannot add a Domain Local group to a Domain Local group in another domain.

**2. Answers: A, B**

**Explanation A.** This is one of the correct choices as the Power Users group does not have log on locally rights on a Windows Server 2003 domain controller by default.

**Explanation B.** This is one of the correct choices as the Users group does not have log on locally rights on a Windows Server 2003 domain controller by default.

Explanation C. This is not one of the correct answers as the question asked which groups do not have log on locally rights on a Windows Server 2003 domain controller by default. The Account Operators group does have log on locally rights on a Windows Server 2003 domain controller.

Explanation D. This is not one of the correct answers as the question asked which groups do not have log on locally rights on a Windows Server 2003 domain controller by default. The Server Operators group does have log on locally rights on a Windows Server 2003 domain controller.

Explanation E. This is not one of the correct answers as the question asked which groups do not have log on locally rights on a Windows Server 2003 domain controller by default. The Print Operators group does have log on locally rights on a Windows Server 2003 domain controller.

### 3. Answers: B, C

Explanation A. This is not one of the correct answers since the Application Data folder is included in a roaming profile by default.

**Explanation B.** This is a correct choice as there is no User Data folder included in a roaming profile.

**Explanation C.** This is a correct choice as the Default User folder is not included in a roaming profile.

Explanation D. This is not one of the correct choices as the Start Menu folder is included in a roaming profile by default.

Explanation E. This is not one of the correct choices as the My Documents folder is included in a roaming profile by default.

### 4. Answer: D

Explanation A. This is not the best answer. Although this would work; it is not the best practice for assigning permission to resources.

The method recommended by Microsoft as a best practice is to add domain user accounts (A) into global groups (G), add global groups into domain local groups (DL), and then add the domain local group to the network resource and set the permission (P) access control level to the resource to reflect the appropriate level of permission desired / needed.

Explanation B. This is not a correct answer as a distribution group cannot be used to assign permissions.

Explanation C. This is not a correct answer as a global group cannot contain groups from other domains.

**Explanation D.** This is the correct answer and the method recommended by Microsoft as a best practice. When setting up permissions and access to resources administrators should add domain user accounts (A) into global groups (G), add global groups into domain local groups (DL), and then add the domain local group to the network resource and set the permission (P) access control level to the resource to reflect the appropriate level of permission desired / needed.