



# STUDY GUIDE



Microsoft

## 70-290

### Managing and Maintaining a Microsoft Windows Server 2003 Environment

Chris McCain

MCSE, MCDBA, MCT, CCNA, CISSP, CCSE

**EXAMFORCE**



## About the Exam

There are five major topic areas (domains) that make up this exam:

- 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

This guide walks you through all of the technologies in the objectives and sub-objectives as published by Microsoft.

Please note that proper hands-on experience is required to pass this test, so setting up a home lab is a must. This is true for all MCSE exams, as they all pre-suppose that the test taker already has real world experience of the product on which they are tested. For this test, I recommend a set up with two domain controllers and at least two workstations. Please note that these machines do not have to be state of the art. Indeed, we are more interested in duplicating concepts in real life than in actual performance of the network and its machines.

# Objectives

---

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

Manage basic disks and dynamic disks.

Monitor server hardware. Tools might include Device Manager, the Hardware Troubleshooting Wizard, and appropriate Control Panel items.

Optimize server disk performance.

- Implement a RAID solution.
- Defragment volumes and partitions.

Install and configure server hardware devices.

- Configure driver signing options.
- Configure resource settings for a device.
- Configure device properties and settings.

## Chapter 2: Managing Users, Computers, and Groups

Manage local, roaming, and mandatory user profiles.

Create and manage computer accounts in an Active Directory environment.

Create and manage groups.

- Identify and modify the scope of a group.
- Find domain groups in which a user is a member.
- Manage group membership.
- Create and modify groups by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.
- Create and modify groups by using automation.

Create and manage user accounts.

- Create and modify user accounts by using the Active Directory Users and Computers MMC snap-in.
- Create and modify user accounts by using automation.
- Import user accounts.

Troubleshoot computer accounts.

- Diagnose and resolve issues related to computer accounts by using the Active Directory Users and Computers MMC snap-in.
- Reset computer accounts.

Troubleshoot user accounts.

- Diagnose and resolve account lockouts.
- Diagnose and resolve issues related to user account properties.

Troubleshoot user authentication issues.

## Chapter 3: Managing and Maintaining Access to Resources

Configure access to shared folders.

- Manage shared folder permissions.

Troubleshoot Terminal Services.

- Diagnose and resolve issues related to Terminal Services security.
- Diagnose and resolve issues related to client access to Terminal Services.

Configure file system permissions.

- Verify effective permissions when granting permissions.
- Change ownership of files and folders.

Troubleshoot access to files and shared folders.

### **Chapter 4: Managing and Maintaining a Server Environment**

Monitor and analyze events. Tools might include Event Viewer and System Monitor.

Manage software update infrastructure.

Manage software site licensing.

Manage servers remotely.

- Manage a server by using Remote Assistance.
- Manage a server by using Terminal Services remote administration mode.
- Manage a server by using available support tools.

Troubleshoot print queues.

Monitor system performance.

Monitor file and print servers. Tools might include Task Manager, Event Viewer, and System Monitor.

- Monitor disk quotas.
- Monitor print queues.
- Monitor server hardware for bottlenecks.

Monitor and optimize a server environment for application performance.

- Monitor memory performance objects.
- Monitor network performance objects.
- Monitor process performance objects.
- Monitor disk performance objects.

Manage a Web server.

- Manage Internet Information Services (IIS).
- Manage security for IIS.

### **Chapter 5: Managing and Implementing Disaster Recovery**

Perform system recovery for a server.

- Implement Automated System Recovery (ASR).
- Restore data from shadow copy volumes.
- Back up files and System State data to media.
- Configure security for backup operations.

Manage backup procedures.

- Verify the successful completion of backup jobs.
- Manage backup storage media.

Recover from server hardware failure.

Restore backup data.

Schedule backup jobs.

# Chapter 1: Managing and Maintaining Physical and Logical Devices

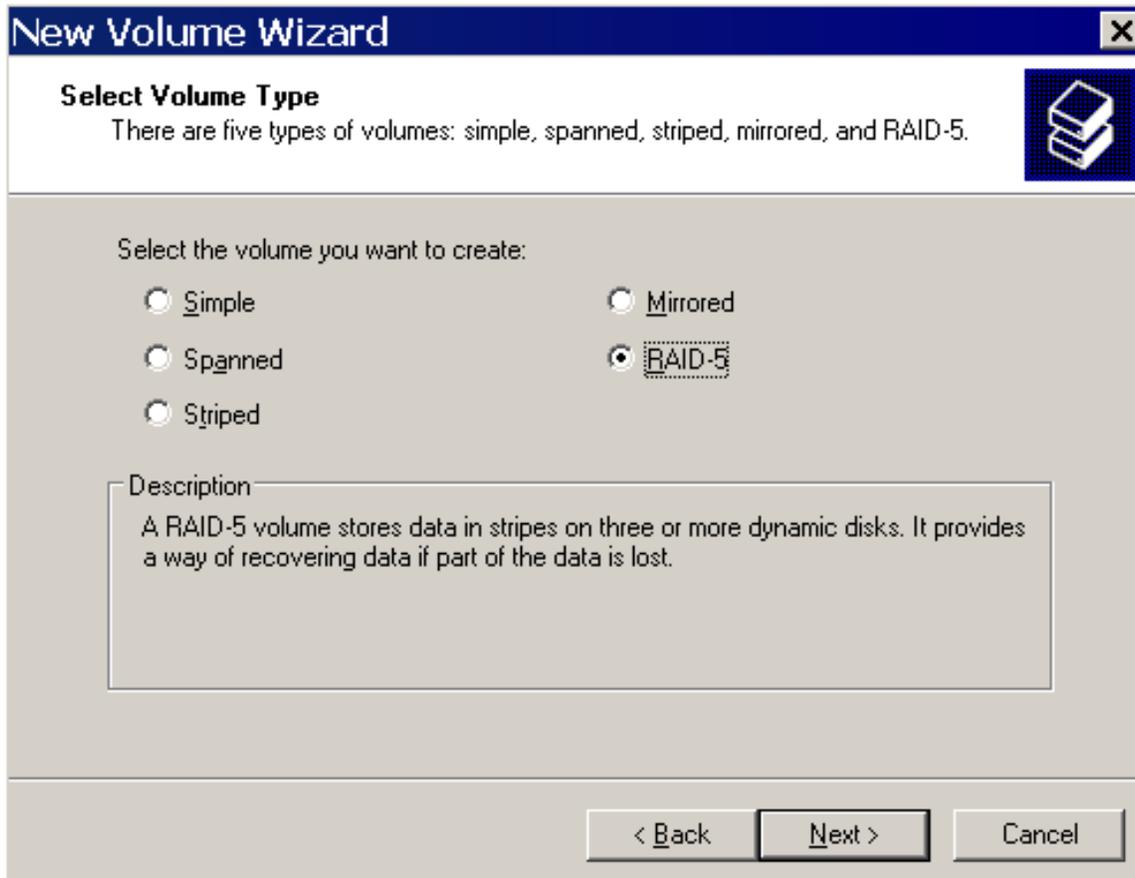
## Chapter 1

### Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5

### Manage basic disks and dynamic disks.

The Microsoft Windows Server 2003 platform is capable of supporting two disk types; basic and dynamic. The basic disk is the default disk type which allows for the creation of extended and primary partitions as we have known them from previous operating systems. Upon opening the Computer Management snap-in for the first time the Disk Management node will initiate the Initialize Disk Wizard and the Disk Conversion Wizard. Once a signature is written to the disk it can be converted to a dynamic disk. The dynamic disk type arrived on the scene with the release of Windows 2000 and remains in the latest Windows Server 2003 operating system.



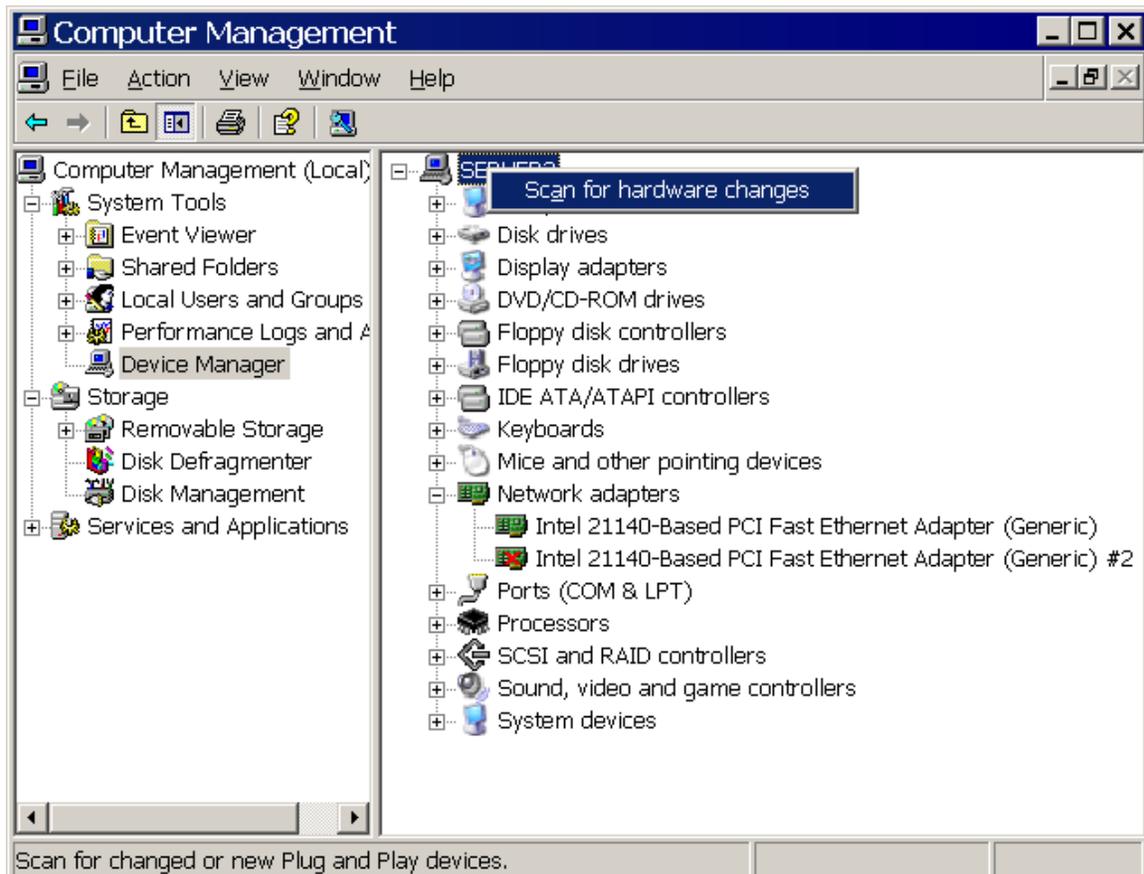
As shown in the figure above dynamic disks can be used to create any of the following volume types:

- 1) **Simple volume:** an area of free space of some size.

- 2) **Spanned volume/extended volume:** a volume that spans across multiple physical disks writing in a sequential fashion to provide extended storage to a single drive letter allocation. The spanned volume does not provide any performance boost or fault tolerance.
- 3) **Striped volume (RAID0):** a volume that reads and writes across two or more equal portions of different physical in a serial manner. Striped volumes do not support fault tolerance, however they do provide a read/write performance enhancement due to the serial nature of data storage and access.
- 4) **Mirrored volume (RAID1):** a volume that writes to two equally sized volumes on separate physical hard drives.
- 5) **RAID-5 volume:** a volume that writes simultaneously to three or more hard drives. The volume spreads data parity equally across all drives to provide fault tolerance in the event of a single drive failure.

**Monitor server hardware. Tools might include Device Manager, the Hardware Troubleshooting Wizard, and appropriate Control Panel items.**

Monitoring server hardware is easily achieved using the Device Manager node of the Computer Management snap-in. As shown in the figure below the Device Manager lists all installed, disabled, and troubled hardware devices for a system. Device Manager offers a Scan for hardware changes option for locating hardware.



Devices labeled with a red X have been disabled, while devices labeled with a yellow warning exclamation are devices with driver problems or IRQ conflicts.

The Hardware Troubleshooting Wizard is still available for a step-by-step walk through of identifying and resolving problems with hardware devices. In addition to these utilities, the Control Panel offers options for installing, removing, and troubleshooting hardware devices like modems, and network interfaces.

### **Optimize server disk performance.**

#### **Implement a RAID solution.**

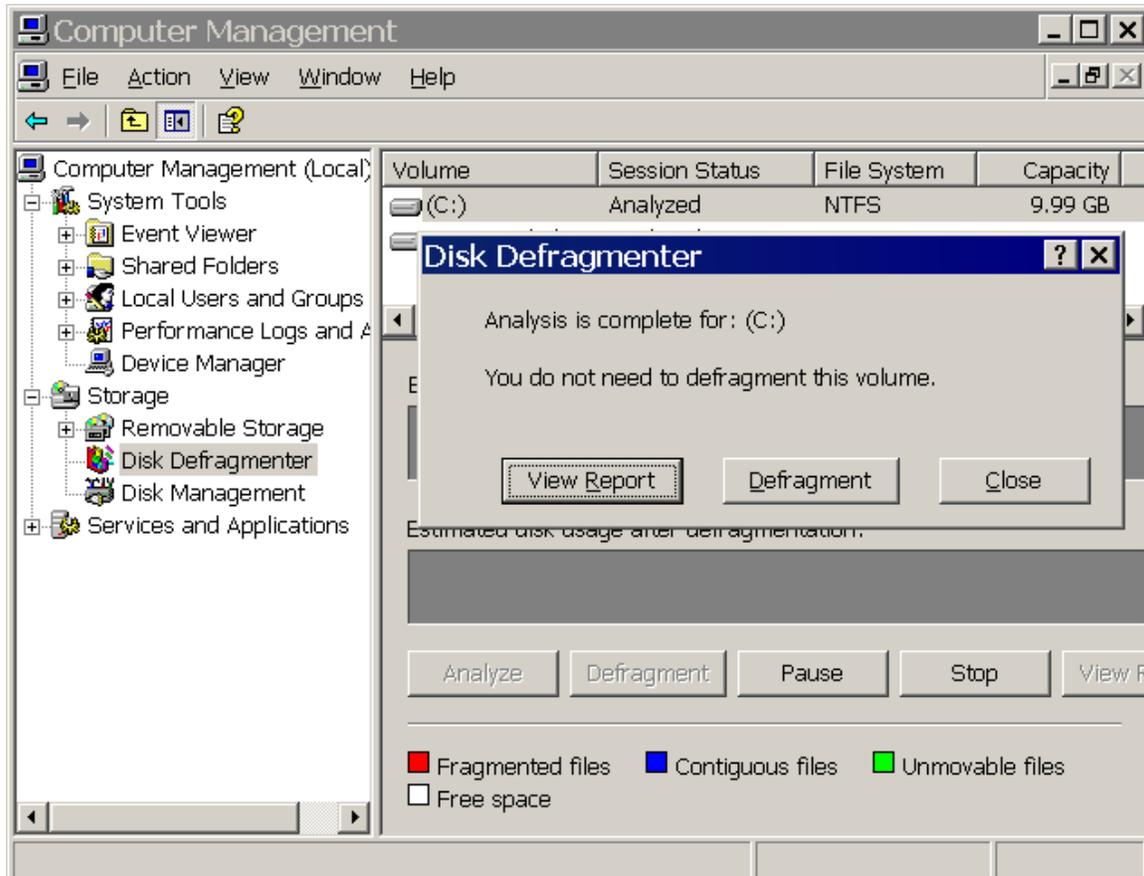
The RAID-1 and RAID-5 volumes are the only ways to obtain fault tolerant disk structures in Windows Server 2003. In each case the volume allows for a single disk failure while maintaining accessible data.

The RAID-1 (mirrored volume) is better used to provide fault tolerance of the system volume to optimize recovery in the event of an operating system failure. By copying all operating system configurations and settings to a second volume, administrators can quickly reboot systems that have failed by using a boot floppy directed to the second disk in the mirrored volume.

The RAID-5 volume is most commonly used to store data as it cannot be used for the system volume. A RAID-5 provides minimal read performance improvements but offers a fault tolerant disk configuration that allows for the failure of a single drive. The RAID-5 volume writes parity data evenly across all drives. The parity data is used to make up the data from a failed drive in the volume. No matter the number of disks, 2 or 32, in the RAID-5 volume it only supports the loss of a single drive.

#### **Defragment volumes and partitions.**

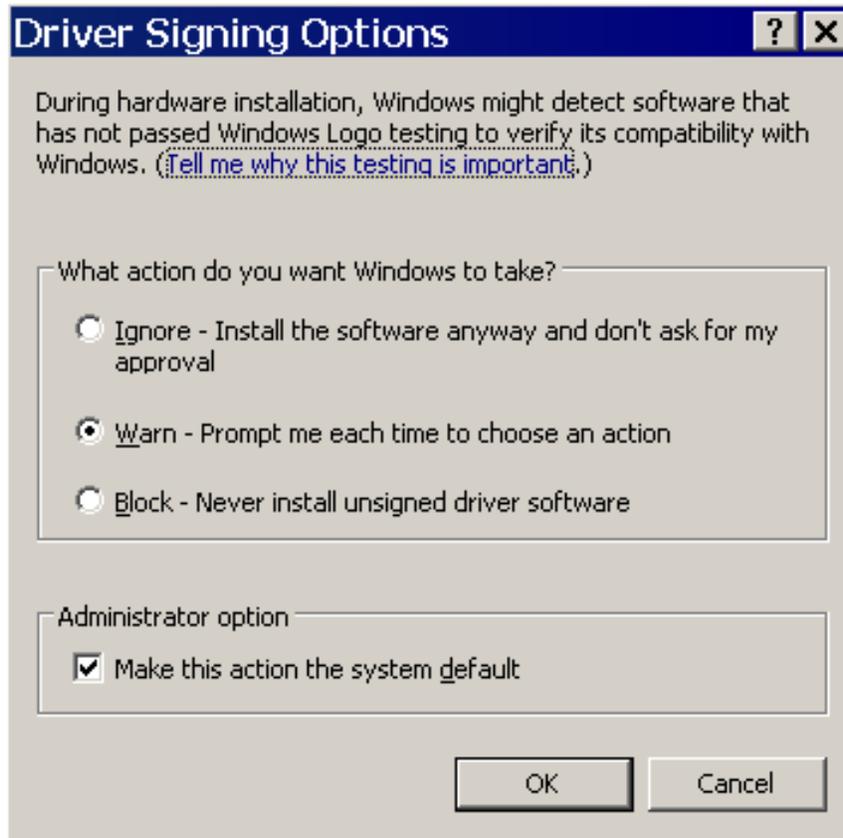
Over time hard drives become fragmented because written to the physical disk cannot be written into contiguous blocks of space. When information needs to be retrieved the drive must find the data from multiple locations before being able to return the information to the user. Users will often be the first to identify the need for defragmentation because of the unusual delay in opening files. The Disk Defragmenter utility in the Computer Management snap-in, shown in the figure below, can be used to analyze system to determine if a defragment is necessary.



### **Install and configure server hardware devices.**

#### **Configure driver signing options.**

Windows Server 2003 provides support Driver Signing Options which all for identifying software that has not passed the Windows Logo testing performed by the Windows Hardware Quality Labs (WHQL). The WHQL tests hardware to ensure compatibility with Windows operating systems. The Driver Signing configuration options, shown in the figure below, are accessible through the System Properties.



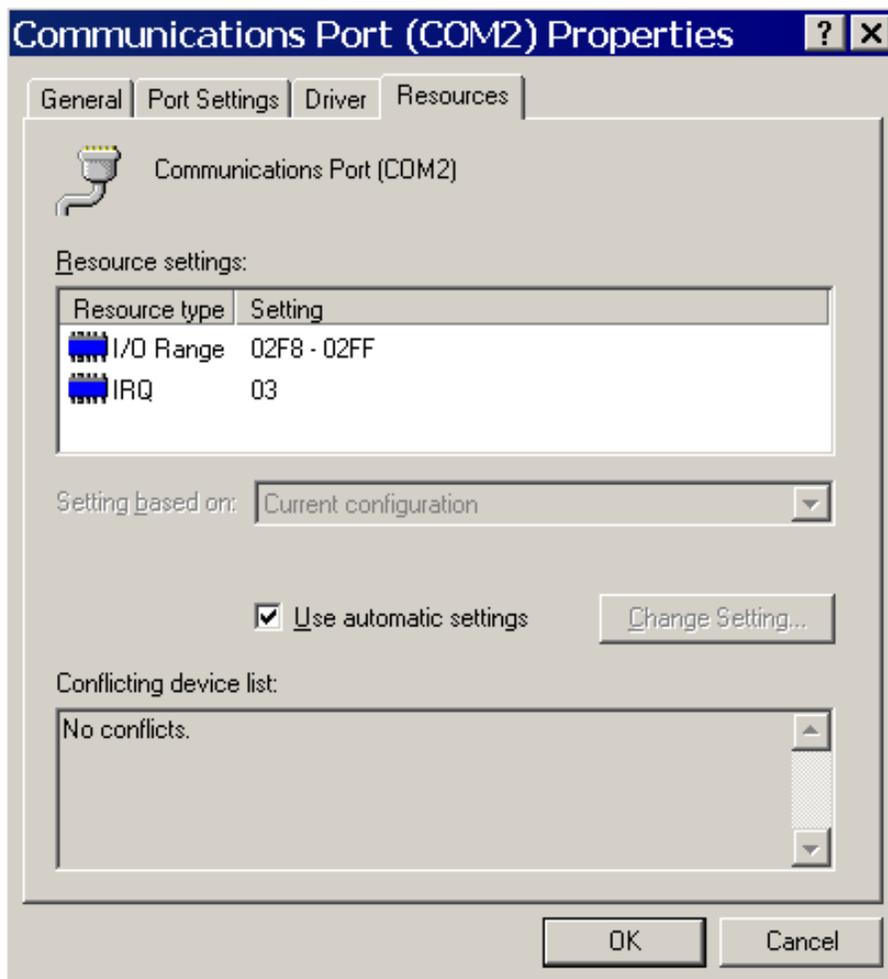
**NOTE:** Driver Signing options can be configured for multiple systems by creating a Group Policy object.



Driver Signing options allow administrators to mitigate the potential problems experienced by allowing users to install third-party drivers that conflict with the Windows operating system.

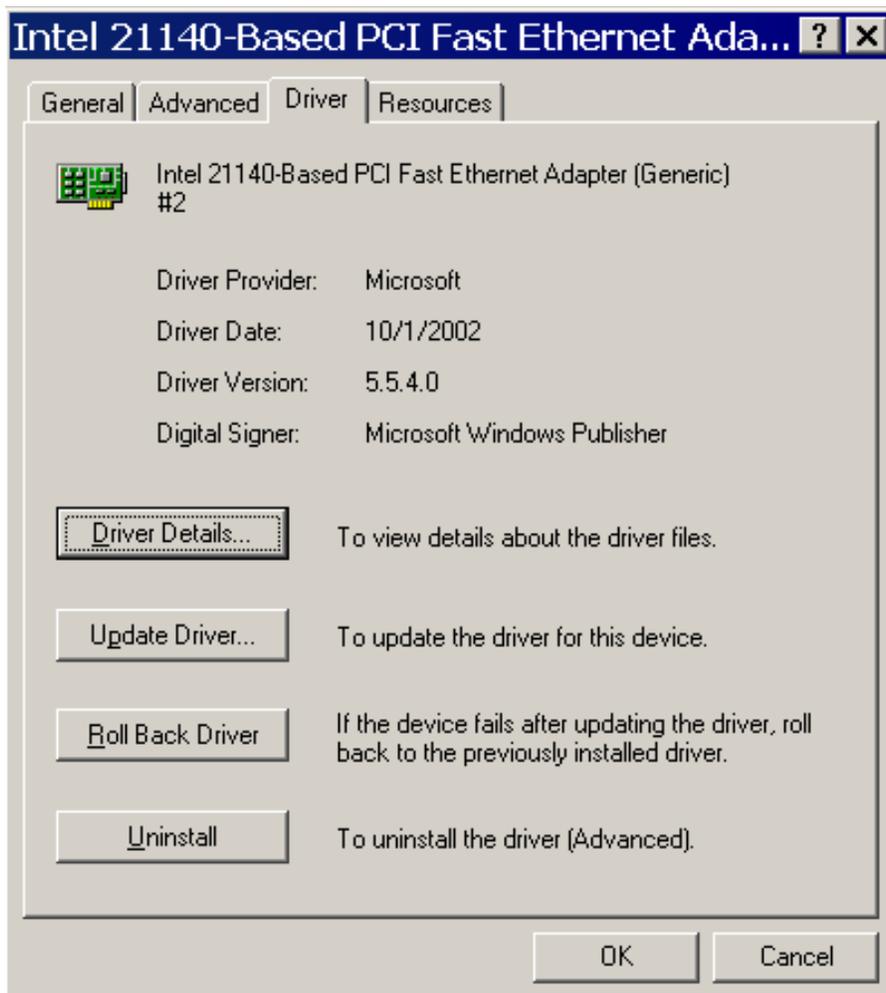
### **Configure resource settings for a device.**

Identifying resource conflicts and device errors is easily done through the Device Manager. As shown in the figure below the properties of a device displays IRQ settings and conflicts.



### Configure device properties and settings.

The device properties and settings also display information about the current driver as well as device specific information. The figure below shows the driver information for a network adapter installed on a Windows Server 2003 system.



The device properties, driver tab, offers administrators the ability to update, rollback, and uninstall drivers to troubleshoot and repair failed devices.

## Chapter 2: Managing Users, Computers, and Groups

### Chapter 2

#### Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5

### Manage local, roaming, and mandatory user profiles.

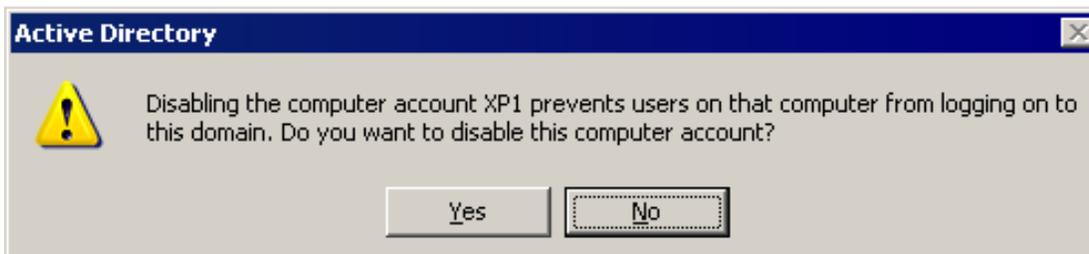
Every user that logs on to a system is provided with a local profile based up the default user profile. Users can then customize their profiles by altering desktop settings, shortcuts, mapped drives, etc. These local profiles are stored on the system and are not available from other systems. If a users logs on to three different systems they will have three different local profiles. Their alterations to the system will not follow them. To ease the pain of local profiles administrators can create roaming user profiles where the user's profile is stored in a centralized location to provide accessibility from any system. The figure below shows location of the user profile path on the properties of a user account.

### Create and manage computer accounts in an Active Directory environment.

Computers added to a Windows Server 2003 domain are listed by default in the Computers container in the Active Directory Users and Computers management console. Administrators can relocate these computer accounts based upon the administrative and security model of their network. Computer accounts created before the physical system is introduced to the network environment are considered pre-staged.

**NOTE:** Pre-staged systems can be associated with a globally unique identifier (GUID) to assist in the management of imaging through Remote Installation Services.

Administrators can prevent logons to specific systems by disabling the computer account in the directory. Computers that are disabled generate an error warning notifying the user that a logon is not available. The figures below display the administrative warning of disabling a computer account, identify a system that has been disabled to prevent logon, and show the user error after the logon attempt.



Computers 2 objects		
Name	Type	Description
 SERVER2	Computer	Windows Server 2003 Enterprise Edition
 XP1	Computer	Windows XP Professional



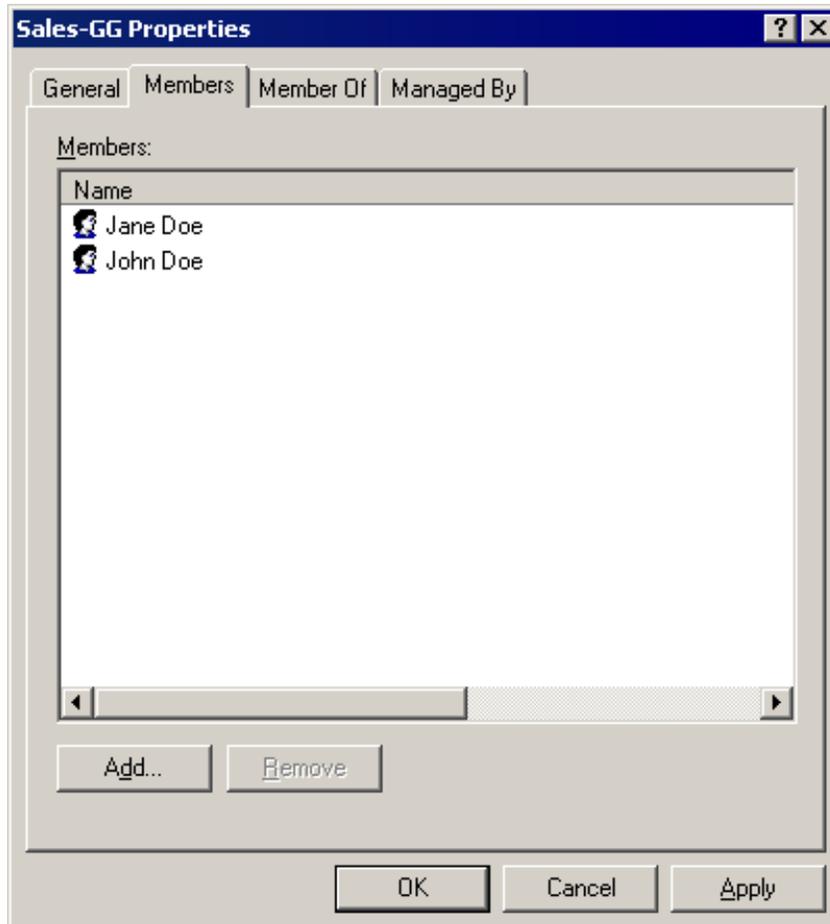
### **Create and manage groups.**

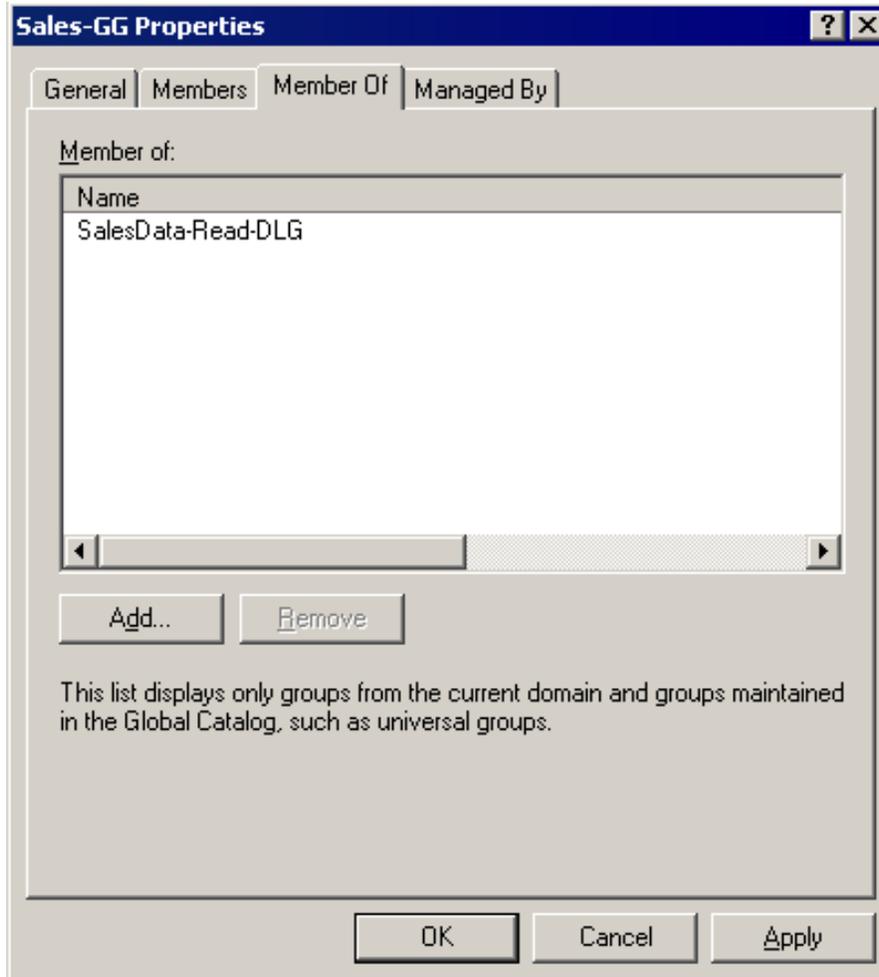
#### **Identify and modify the scope of a group.**

Windows Server 2003 allows for the creation of groups to aid in the management of users and resources. Windows groups have different group types and group scopes used for to accomplish different tasks. The security group type is used anytime administrators are looking to establish resource permission tasks while the distribution group is used for e-mail. The group scopes include domain local, global, and universal. Domain local groups are used by administrators to assign permissions to resources while global groups are used for organizing users. Universal groups are only available in Windows 2000 Native mode domains and Windows Server 2003 functional level domains. Universal groups are a great benefit to administrators who need to share resources across multi-domain forests.

#### **Find domain groups in which a user is a member.**

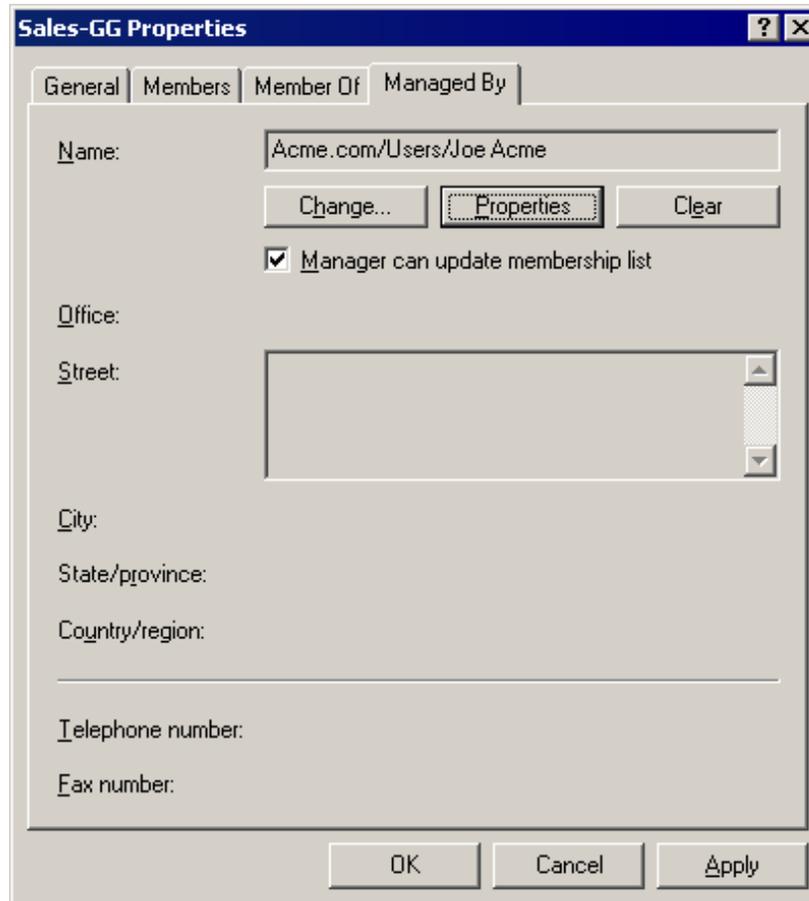
Membership in a group can be obtained from the “Member of” tab of the user account properties or the “Members” tab of the group properties. The figures below display the members that belong to the Sales-GG as well as the domain local groups that Sales-GG belong to.





**Manage group membership.**

On the properties of a group object administrators can configure a user account to be responsible for managing the group memberships. The figure below shows that a user named Joe Acme is able to manage the users who are members of the Sales-GG group.



### Create and modify groups by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.

The most common form of creating and managing group objects is through the Active Directory Users and Computers Management Console, or dsa.msc. The console is an intuitive graphical user interface that provides easing viewing and creation capabilities using either right-clicks or task pad icons.

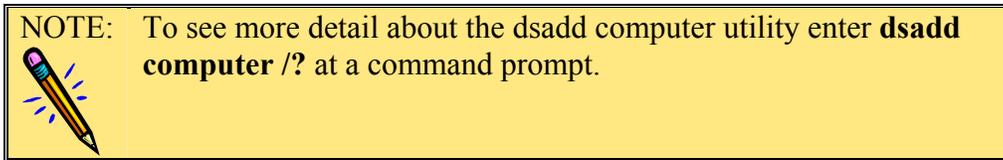
### Create and modify groups by using automation.

When administrators are tasked with creating and modifying groups in bulk the dsa.msc may not be the most efficient tool. For these occasions there are command line utilities including dsadd, dsmod, and visual basic scripting. The figure below displays some of the parameters available with the dsadd utility.

```

C:\WINDOWS\system32\cmd.exe
C:\>dsadd computer /?
Description: Adds a computer to the directory.
Syntax: dsadd computer <ComputerDN> [-samid <SAMName>] [-desc <Description>]
        [-loc <Location>] [-memberof <Group ...>]
        [[-s <Server> | -d <Domain>]] [-u <UserName>]
        [-p <<Password> | *]&] [-q] [-uc | -uco | -uci]
Parameters:

```



## Create and manage user accounts.

### Create and modify user accounts by using the Active Directory Users and Computers MMC snap-in.

The most common tool for managing user accounts is the Active Directory Users and Computers management console. This graphical interface allows for easy creation of accounts and modifications of account properties including tasks like resetting passwords.

### Create and modify user accounts by using automation.

In large enterprise environments administrators are often tasked with creating or managing many objects. Using the GUI methods of right-click > new > can be extremely inefficient. For this reason there are alternative tools that can be used for bulk object creation and modification. These tools include:

1. CSVDE (Comma Separated Values Directory Exchange): allows for import and export of objects to and from Active Directory and comma separated values files. The following syntax imports all of the information from a file named users.txt to a server named dc01.acmecorp.com.

```
Csvde -i -f c:\users.txt -s dc01.acmecorp.com
```

The file users.txt should be a comma separated values file where the first line defines the attributes that are being populated by each additional line of the file. Each additional line should provide the data values for the attributes of each object to be imported.

2. LDIFDE (LDAP Data Interchange Format Directory Exchange): allows for import, export, modifications, and deletions of Active Directory objects. The following syntax creates objects as defined in a file named users.txt.

```
Ldifde -i -v -f c:\users.txt
```

Unlike the file required by the csvde utility an ldifde compatible file lists and defines each object attribute as an individual line item. Each object created repeats the list of attributes being defined.

3. VBScripting: allows for the creation of custom scripts to create, delete, and modify Active Directory objects. The syntax below creates a new organizational unit named sales, a user named Jane Doe with a login name of jdoe, and a group named sales all in the acme.com domain.

```
Set objDomain = GetObject("LDAP://dc=acme,dc=com")
Set objOU = objDomain.Create("organizationalUnit", "ou=sales")
objOU.SetInfo
Set objOU = GetObject("LDAP://OU=sales,dc=acme,dc=com")
Set objUser = objOU.Create("User", "cn=Jane Doe")
```

```
objUser.Put "sAMAccountName", "jdoe"  
objUser.SetInfo  
Set objOU = GetObject("LDAP://OU=sales,dc=acme,dc=com")  
Set objGroup = objOU.Create("Group", "cn=sales-users")  
objGroup.Put "sAMAccountName", "sales-users"  
objGroup.SetInfo  
objGroup.Add objUser.ADSPATH
```

 **NOTE:** For help with scripting visit the <http://www.microsoft.com/technet/scriptcenter/default.mspx> website. Microsoft provides an extensive library of customizable scripts for a number of situations.

### Troubleshoot computer accounts.

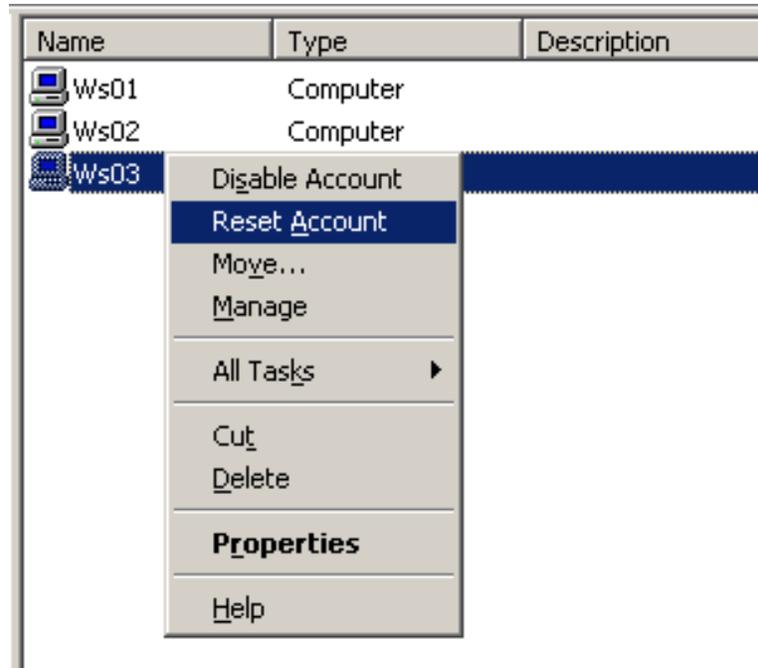
**Diagnose and resolve issues related to computer accounts by using the Active Directory Users and Computers MMC snap-in.**

The Active Directory Users and Computers management console is a fast and easy way to identify computer accounts that have been disabled. The figure below shows a computer account that was disabled and is consequently causing users to receive failed logons.

Name	Type	Description
 Ws01	Computer	
 Ws02	Computer	
 Ws03	Computer	

### Reset computer accounts.

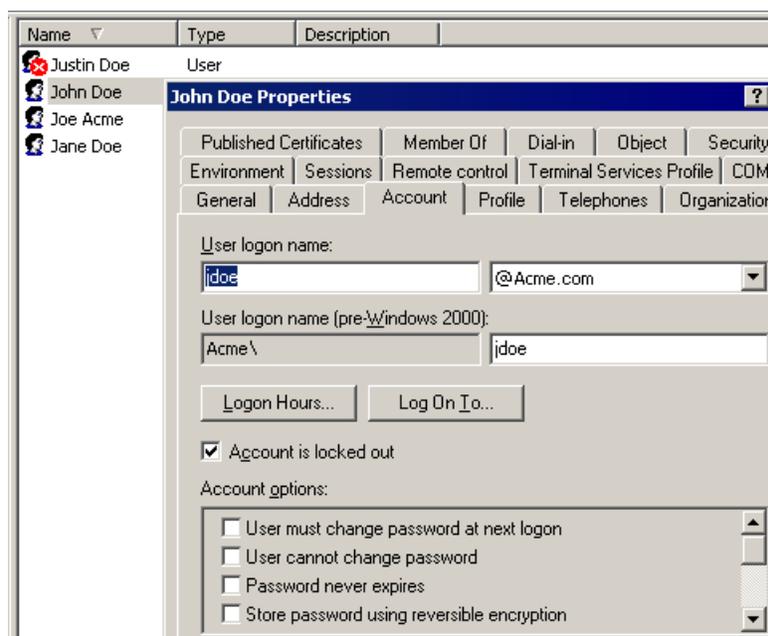
Computer accounts that lose their secure password with the domain database need to be reset. Resetting a computer account can be done through the Active Directory Users and Computers snap-in or via the nltest command line utility. In either case a computer account that is reset will prevent users from successfully logging in until the computer has rejoined the domain to establish its secure relationship with the domain. The following figure shows the administrative options for disabling and account vs. resetting an account.



### Troubleshoot user accounts.

#### Diagnose and resolve account lockouts.

User accounts, like computer accounts can be disabled. A disabled user account is not permitted to logon. User accounts, however can be locked out automatically depending upon the Account Lockout duration setting in the Account Policy settings for the domain or local system. An Account Lockout Duration set to 0 (zero) requires administrative intervention. The figure below shows the distinction between a disabled user account (Justin Doe) and a locked out (John Doe) user.



**Diagnose and resolve issues related to user account properties.**

Issues with user account can be easily diagnosed and resolved through the Active Directory Users and Computers management console. New features like drag-and-drop capability as well as multi-object selecting making account management much easier. For example using the saved queries node of ADUC you can easily find all accounts with non-expiring passwords. The entire result set of the query can then be selected and edited to force an expiring password.

**Troubleshoot user authentication issues.**

In any network user authentication problems are sure to arise. In order to successfully authenticate, a user or computer must successfully obtain an IP address, communicate with a DNS server to find a domain controller, and find a domain controller to submit credentials. Without any of these three pieces authentication problems are sure to arise. As discussed before disabling a user or computer account , resetting a computer account, or locking a user account can all result in failed authentication.

# Chapter 3: Managing and Maintaining Access to Resources

## Chapter 3

### Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5

### Configure access to shared folders.

#### Manage shared folder permissions.

As part of Microsoft's new security initiatives the default permissions for shared folders has been changed from an Everyone-Full Control to an Everyone-Read. This enhances the default security by not allowing users excessive access to resources by default. Shared folder permissions however are a moot point in the big picture of resource permissions. The configuration of NTFS permissions is the most important piece of the permissions puzzle. Shared folder permissions are only accounted for when a resource is being accessed over the network, while NTFS permissions are always taken into consideration. For this reason it is common practice for administrators to configure all share permissions as an Everyone-Change permission and then spend more time ensuring that the NTFS permissions are enforcing appropriate security level restrictions. A user's effective permission is equal to the least restrictive permission between the most restrictive share permission and the most restrictive NTFS permission.

**WARNING:** Remember that share permissions are not considered when logged on interactively to a system while NTFS permissions are always considered.. Therefore, it is most important to ensure that a resource's NTFS permissions are configured in a secure manner.

### Troubleshoot Terminal Services.

#### Diagnose and resolve issues related to Terminal Services security.

Terminal Services offers four level of security for the Remote Desktop Protocol (RDP) connections between client and server. Security can be set on the General tab of the RDP-TCP properties in the Terminal Services Configuration Management Console. The four options include:

- a) **Low:** all data sent from the client to the server is encrypted using 56-bit encryption. Data sent from server to client is not encrypted.
- b) **Client compatible:** All data sent between client and server, in either direction, is encrypted using the maximum key strength supported by the client.
- c) **High:** all data sent between client and server, in either direction, is encrypted using the maximum key strength supported by the server.
- d) **FIPS:** all data sent between client and server, in either direction, is encrypted using Federal Information Processing Standard 140-1 encryption method.

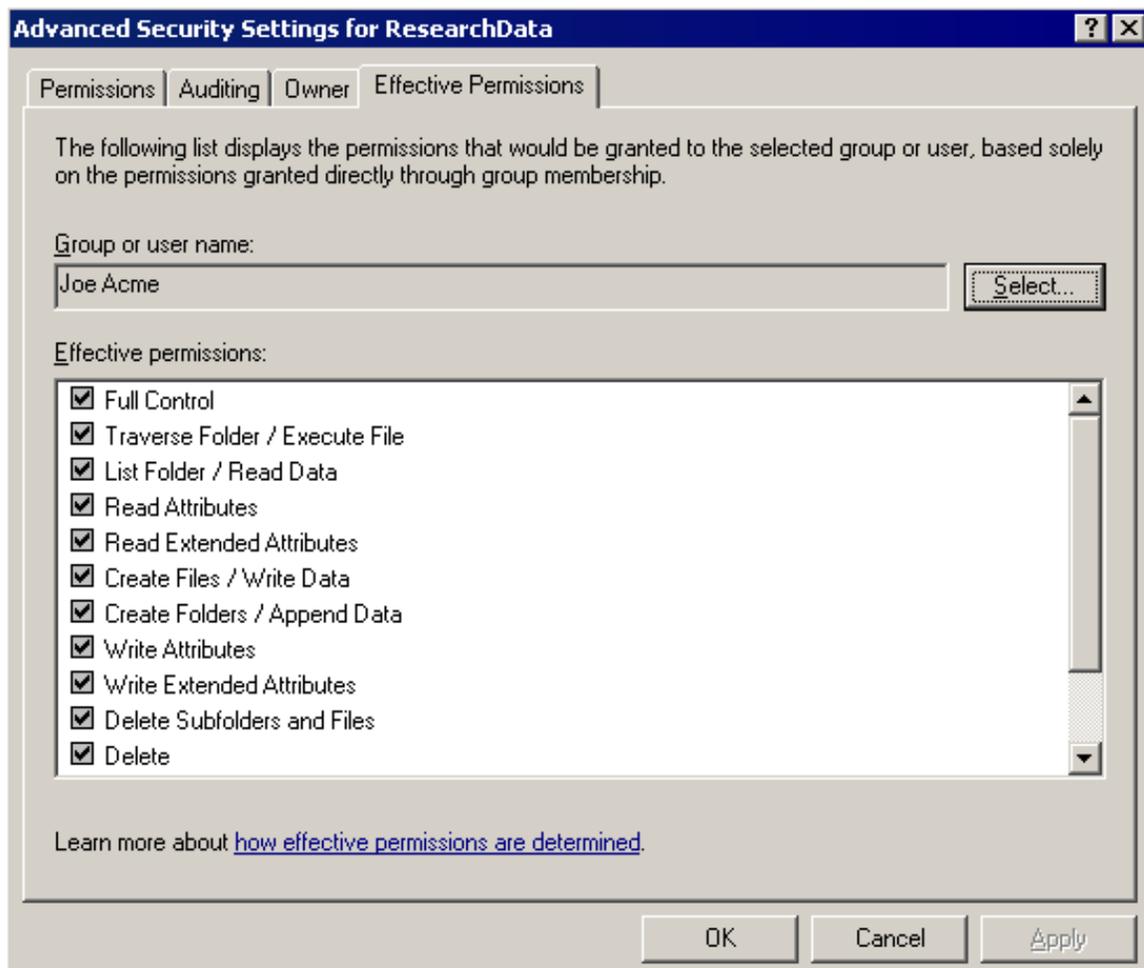
### Diagnose and resolve issues related to client access to Terminal Services.

Clients needing access to a Terminal Server must be provided with the appropriate privileges. Users in the Administrators or Remote Desktop Users groups are already provided with the right to access a system for Remote Desktop Administration.

### Configure file system permissions.

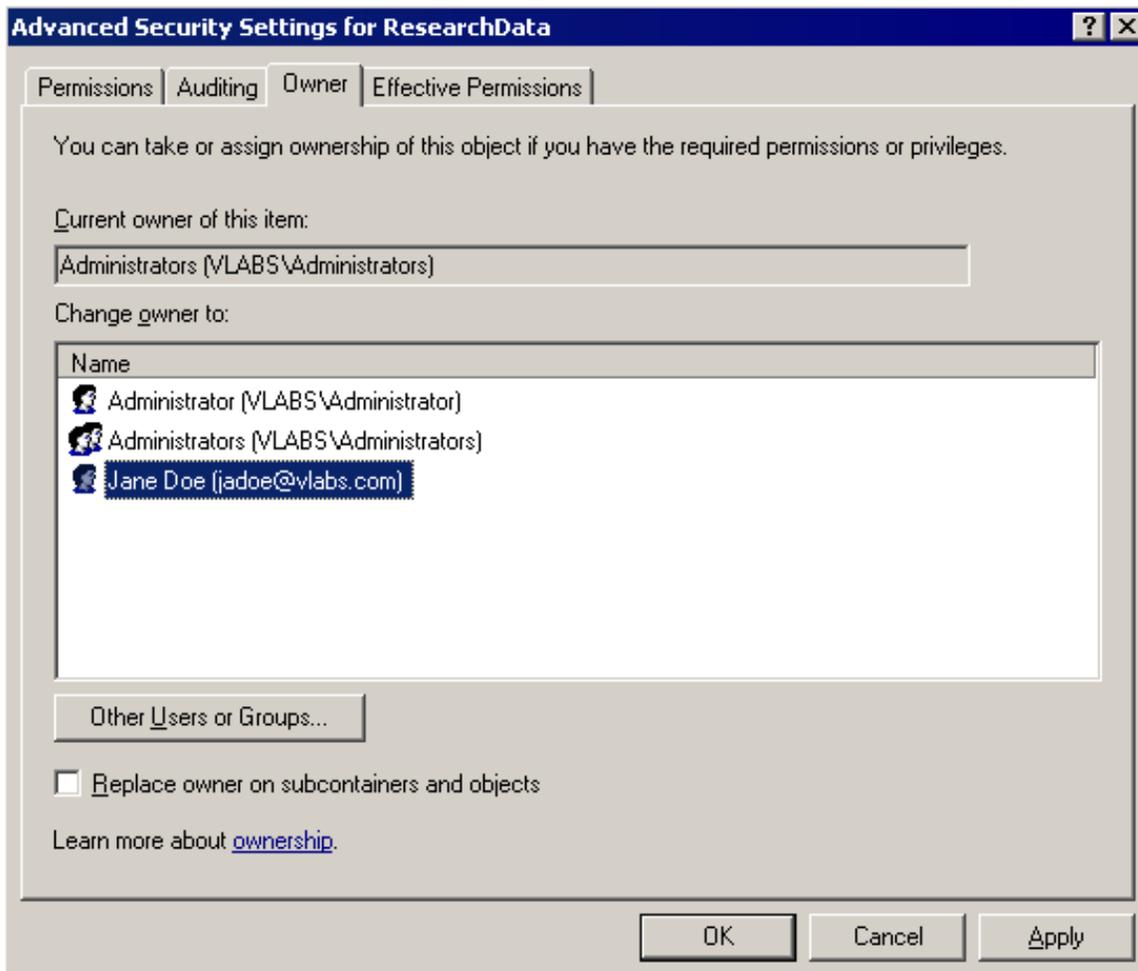
#### Verify effective permissions when granting permissions.

On the advanced properties of an NTFS resource a new tab named Effective Permissions provides a summary of a user's effective NTFS permissions by accumulating all permissions for all group memberships as well as the individual account. The figure below shows that the user named Joe has full control NTFS permissions. This identifies that if Joe is experiencing a problem accessing the ResearchData folder it must be due to a limitation existing within the Shared Folder permissions.



### Change ownership of files and folders.

Windows Server 2003 now provides an easy way to change the ownership of files and folders. Instead of having to provide a user with the Take Ownership permission for a resource, an administrator or current resource owner can directly transfer ownership through the advanced properties, Owner tab of a resource. The figure below shows the ability to directly transfer ownership of the ResearchData folder to any of the listed users.



## Chapter 4: Managing and Maintaining a Server Environment

### Chapter 4

#### Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5

### **Monitor and analyze events. Tools might include Event Viewer and System Monitor.**

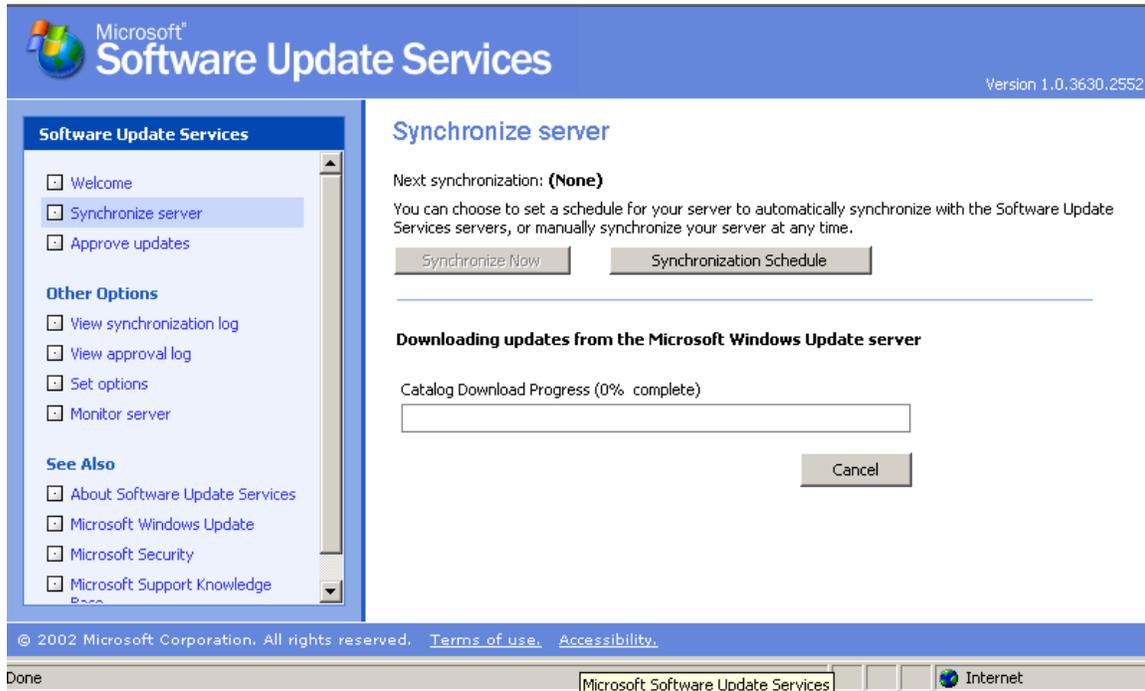
The Event Viewer and System Monitor are two common tools for managing a Windows Server 2003 system. The Event Viewer maintains three default logs of information; System log, Security log, and Application log. As new services are added to a system new logs are added to the list. For example, when the DNS service gets installed on a server a new DNS log is added. The System Monitor utility (more to come) is used to catch performance measurements of a Windows Server 2003 system.

### **Manage software update infrastructure.**

The Software Update Service (SUS) is an added service that allows for the creation of a simplified patch management and security update infrastructure. SUS is an http based service that provides administrators with a means of downloading and storing all available updates from the Windows Update servers. Using the <http://servername/susadmin> management page administrators can configure a number of settings including:

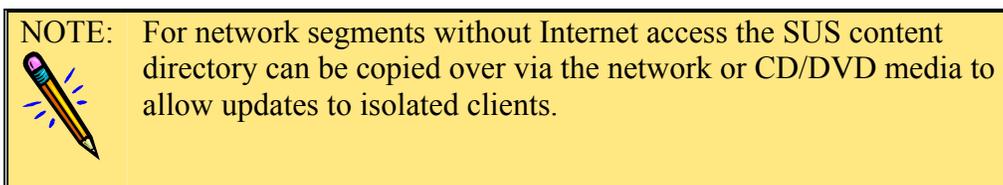
- 1) To download updates from the Windows Update servers or other SUS servers.
- 2) When to synchronize with the other servers
- 3) To automatically or manually approve updates
- 4) To download updates only for specific languages
- 5) To store updates in a local directory or maintain them on the Windows Update Site

The figure below shows the SUS administration page accessible as a virtual directory under the default website.



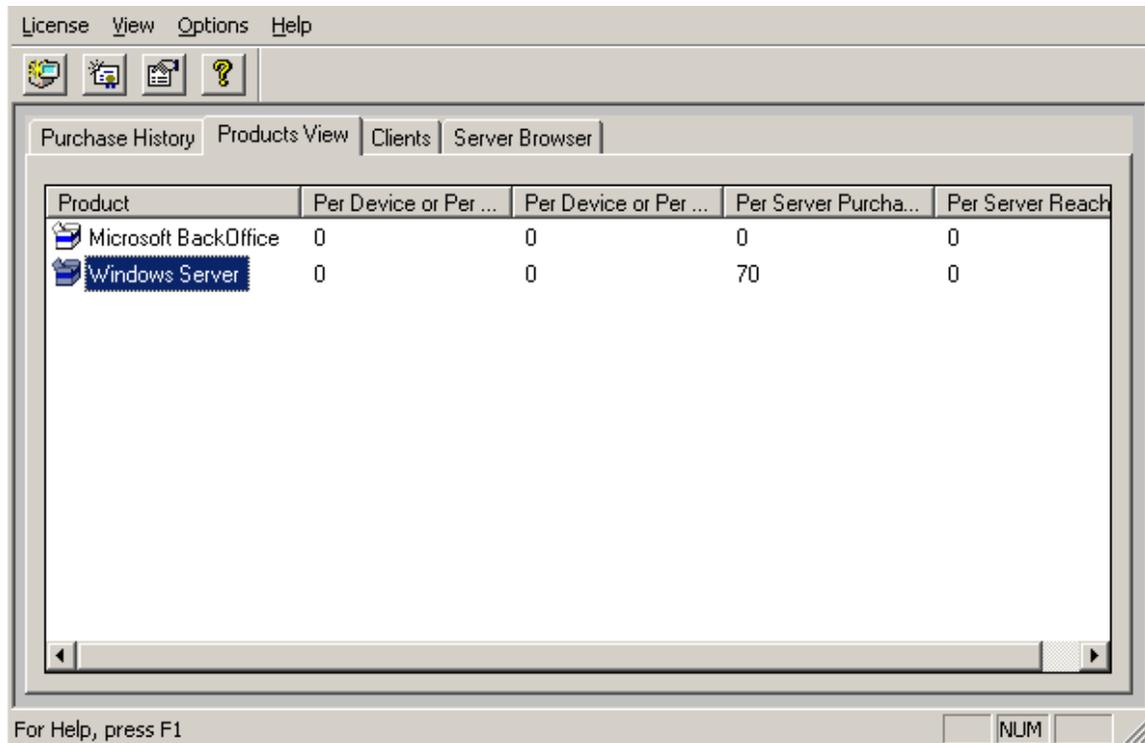
SUS stores a list of all approved updates and synchronizations in a pair of xml files appropriately named history-approve.xml and history-sync.xml.

Domain members can be configured as SUS clients using a Group Policy object that identifies the SUS server and schedule for downloading new updates. The combination of an internal SUS infrastructure with Group Policy and Active Directory makes for an administratively easy software update infrastructure.



### Manage software site licensing.

Licensing of the Windows Server 2003 product family is done through the licensing console. The figure below shows that there are 70 Per Server licenses purchased for the Windows Server product line.



The screenshot shows the Windows Server 2003 Licensing console. The 'Products View' tab is active, displaying a table with the following data:

Product	Per Device or Per ...	Per Device or Per ...	Per Server Purcha...	Per Server Reach
Microsoft BackOffice	0	0	0	0
Windows Server	0	0	70	0

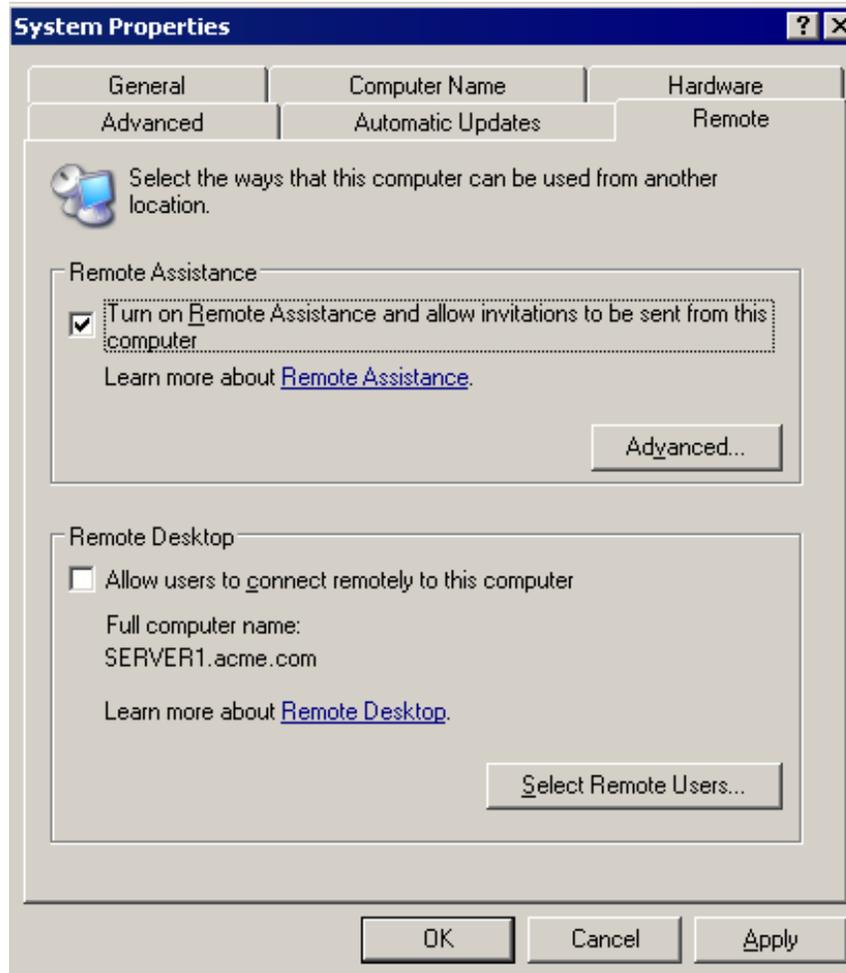
The interface includes a menu bar (License, View, Options, Help), a toolbar with icons, and a status bar at the bottom with the text 'For Help, press F1' and a 'NUM' button.

Licenses can be added and revoked as needed through the Licensing console.

### **Manage servers remotely.**

#### **Manage a server by using Remote Assistance.**

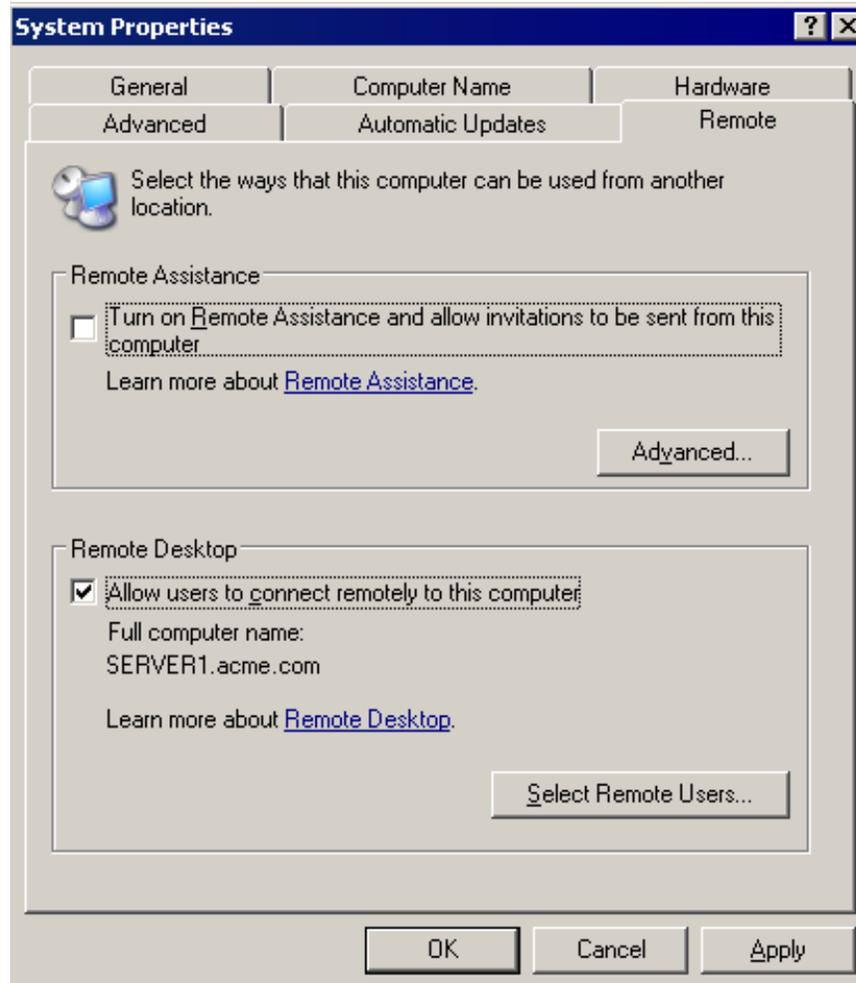
The Remote Assistance feature of Windows Server 2003 allows for “expert” users to assist “novice” users in times of need. Remote Assistance must be enabled on the system where the invitation for help is initiated. The figure below shows the portion of the system properties, Remote tab, where Remote Assistance is enabled.



Remote Assistance Invitations can be sent via e-mail, messenger, or even a saved file. In any case the user asking for help always has the option to deny the help upon the offering from the expert user. The Remote Assistance invitations can also be configured with an expiration to prevent an excessive delay in the request. This feature runs over the same protocol (RDP) and port (3389) as Terminal Services and Remote Desktop Administration. Windows Server 2003 also provides a Group Policy setting named Offer Remote Assistance that can be enabled to allow issuing unsolicited Remote Assistance offerings to users.

### **Manage a server by using Terminal Services remote administration mode.**

The Remote Desktop Administration feature of Windows Server 2003 is what used to be termed the Terminal Services Administration Mode. The new version is installed by default but not enabled as shown in the figure below.



Once enabled the only users who can access the system by default are members of the Administrators group and the Remote Desktop Users group.

	<p><b>WARNING:</b> When accessing a domain controller via Remote Desktop Administration the Remote Desktop Users group must be granted the Allow Logon through Terminal Services right through a Group Policy.</p>
---	--

### Manage a server by using available support tools.

Remote systems management does not always have to fall under the category of Remote Desktop or Remote Assistance. Administrative users can download install the adminpak.msi on their workstation to use the default management consoles for remote systems management. Management snap-ins like Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and more.

	<b>WARNING:</b> Installing the adminpak.msi from a Windows Server 2003 CD-ROM installs tools that default to a higher security level by using LDAP signing and encryption. Using these tools to manage domain controllers running an operating system other than Windows Server 2003 will fail unless a registry change is made to disable the enhanced security.
---	---

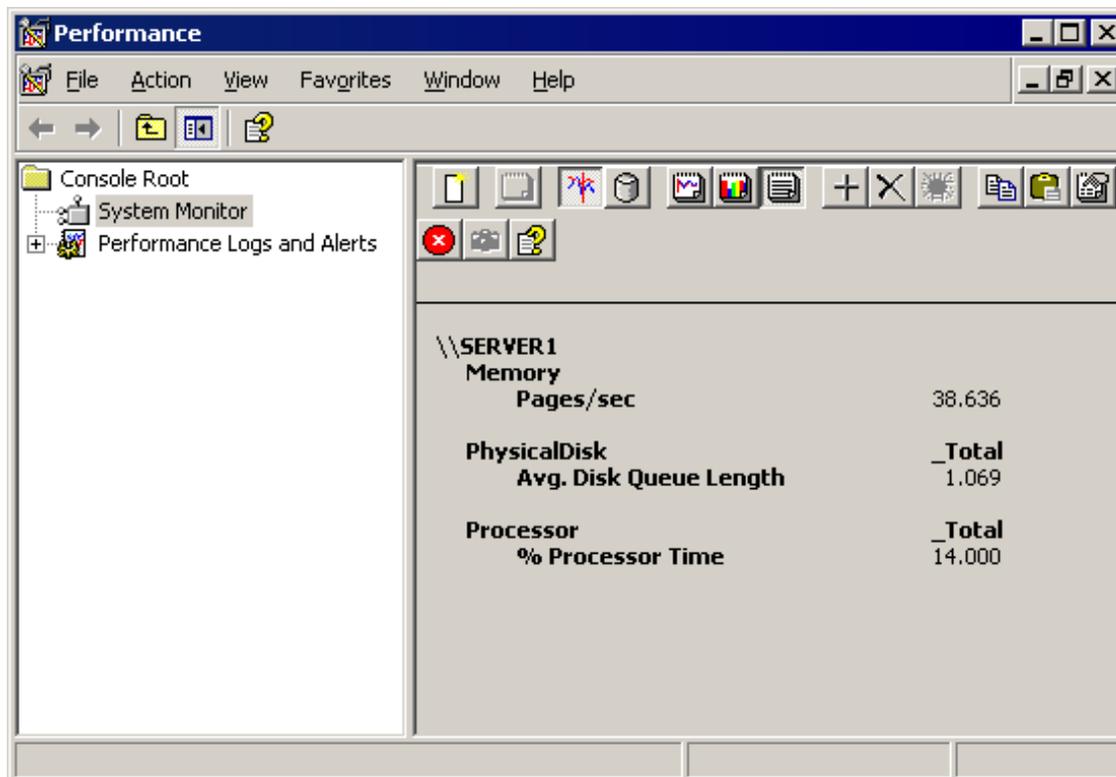
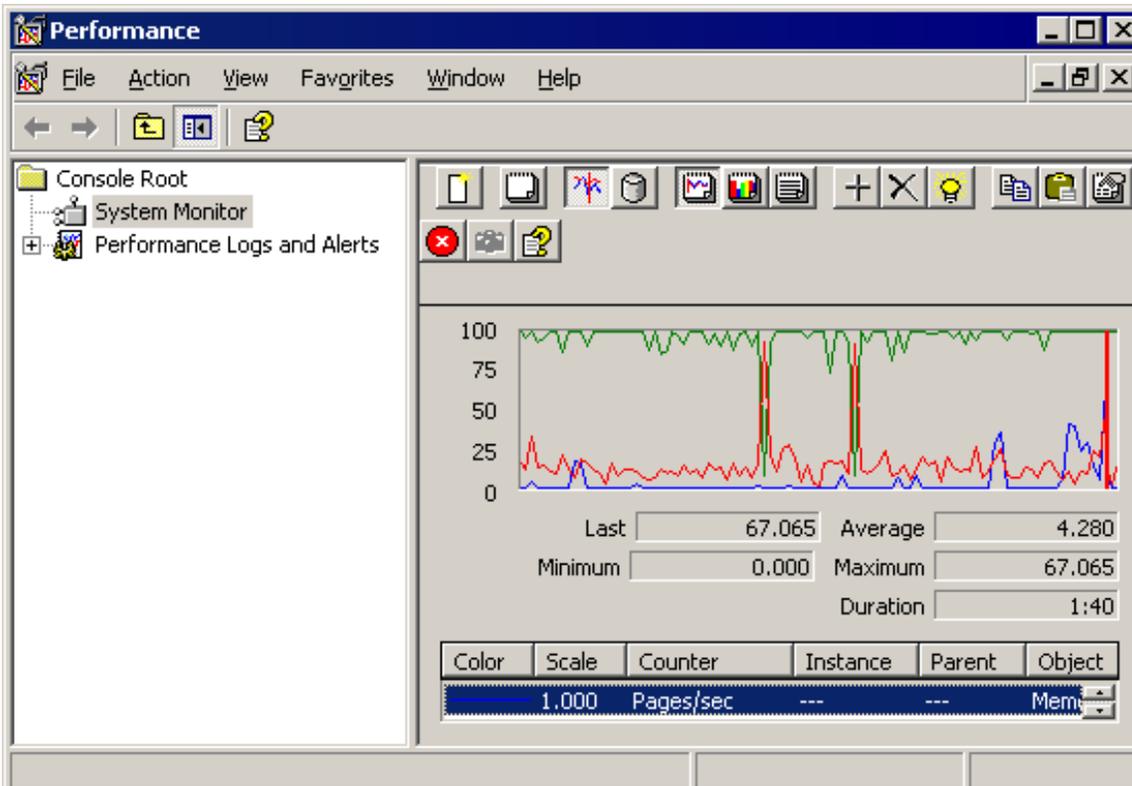
### **Troubleshoot print queues.**

Administrators can troubleshoot print queues by connecting to the printer in the traditional fashion of a UNC path or they can connect via Internet Explorer if Internet printing is installed and enabled.

	<b>WARNING:</b> Remember that IIS 6.0 is not installed by default and even once it is installed it does not support ASP pages, WebDAV, or Internet Printing. These features have to be enabled before they become functional.
---	---

### **Monitor system performance.**

Using the System Monitor (Performance Monitor) administrators can easily identify system performance and make decisions with regards to hardware upgrades to improve performance. The figures below show the Chart View and Report View of System Monitor.



## Monitor file and print servers. Tools might include Task Manager, Event Viewer, and System Monitor.

### Monitor disk quotas.

Disk quotas provide administrators with an easy way to limit the amount of data a user can store on a particular volume. Quotas cannot be configured on an individual directory nor can they be configured for groups.

**WARNING:**  Users who have previously saved data to a folder on a volume where quota is retroactively enabled will not be part of the quota restriction. An administrator will need to add a quota entry for each user account that had a already saved information.

### Monitor server hardware for bottlenecks.

Monitor a server for bottlenecks requires a time investment that most administrators find they don't have. The rewards however can be fantastic. By developing consistent and regular monitoring schedules administrators are able to identify trends in hardware performance. Those trends can turn into projections and expectations of system bottlenecks or worse yet system failure. Armed with this data, however, administrators are able to head off the bottlenecks by making system adjustments that reduce the increasing trends.

## Monitor and optimize a server environment for application performance.

### Monitor memory performance objects.

The performance of a server's memory is best monitored by looking at the Pages/sec counter in the Memory object. A high number of pages per second identifies that there is insufficient memory and thus the server is having to swap data out of the faster RAM memory into the slower hard drive storage location. The best way to mitigate a high number of Pages/sec is to add more RAM.

**NOTE:**  Each system is different and therefore it is difficult to determine an exact value that would indicate excessive paging. As a general rule of thumb Pages/sec should be under 20.

### Monitor network performance objects.

The performance of a server's network interface can be monitored by watching the Bytes/sec Total on the Network Interface object. Keep in mind that most network adapters are 100Mbps cards and therefore you will need to convert Mb to Bytes to identify poorly performing network adapters.

### Monitor process performance objects.

Arguably the most important counter to track is the %Processor time on the Processor object. All systems perform differently under different conditions and therefore it isn't possible to identify an exact value where %Processor time is considered excessive. For example, Server1 could run without

problems at a %Processor time of 75% while Server2 could display significant problems at 75%. Like the memory object, however, we can define a general rule of thumb.

### Monitor disk performance objects.

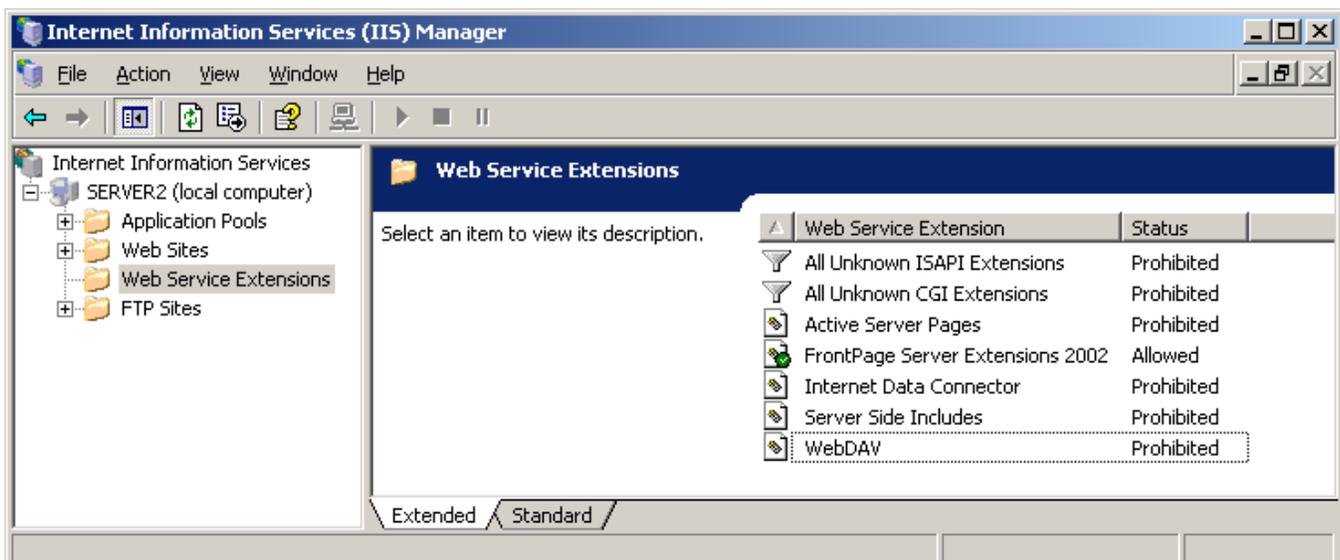
The last object of the big 4 is the Average Disk Queue Length for the Physical Disk counter. An excessive value for the Average Disk Queue length identifies that the hard drive is not processing requests fast enough and thus there are requests waiting. A general rule for the Average Disk Queue Length is that it should not exceed  $2 \times \#$  of disks.

**WARNING:** A high value for the Average Disk Queue Length could be a result of an excessive amount of paging and therefore mislead you into adding faster or more hard drives which would NOT remedy the excessive paging.

### Manage a Web server.

#### Manage Internet Information Services (IIS).

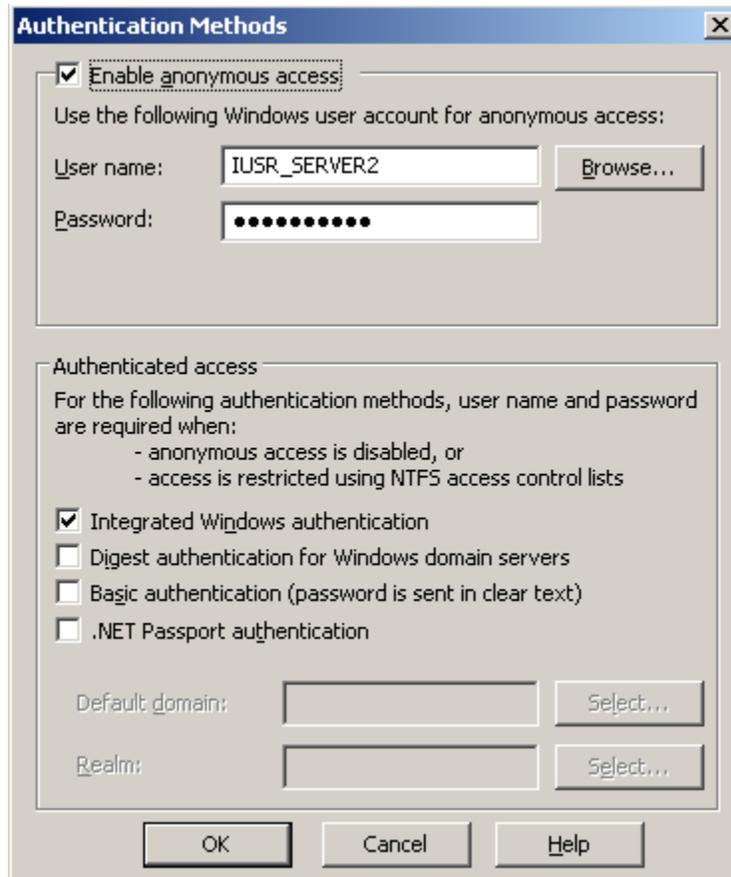
Windows Server 2003 includes the ability to install Internet Information Services 6.0. As part of Microsoft's initiative on building a secure computing environment IIS 6.0 is not installed by default. Even upon installation of IIS 6.0 it is not open for any services other than serving up static content. It is "locked down". The figure below shows the default configuration for the various web services available on IIS 6.0 with Front Page Server Extensions added in to the installation.



**WARNING:** With all of these services prohibited by default administrators will experience failure of their more common ASP applications and WebDAV feature until the feature has been changed to the Allow configuration.

### Manage security for IIS.

As shown in the figure below, IIS 6.0 provides several different methods of authentication including.



Anonymous authentication allows for public users to easily access web sites without requiring any form of authentication. If enabled none of the other authentication mechanisms will be used.

Integrated Windows authentication is best used for intranet sites accessed by internal Microsoft clients. Integrated Windows does not support firewall traversal or non-Microsoft operating systems.

Digest authentication supports Microsoft clients that need to traverse through a firewall.

## Chapter 5: Managing and Implementing Disaster Recovery

### Chapter 5

#### Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5

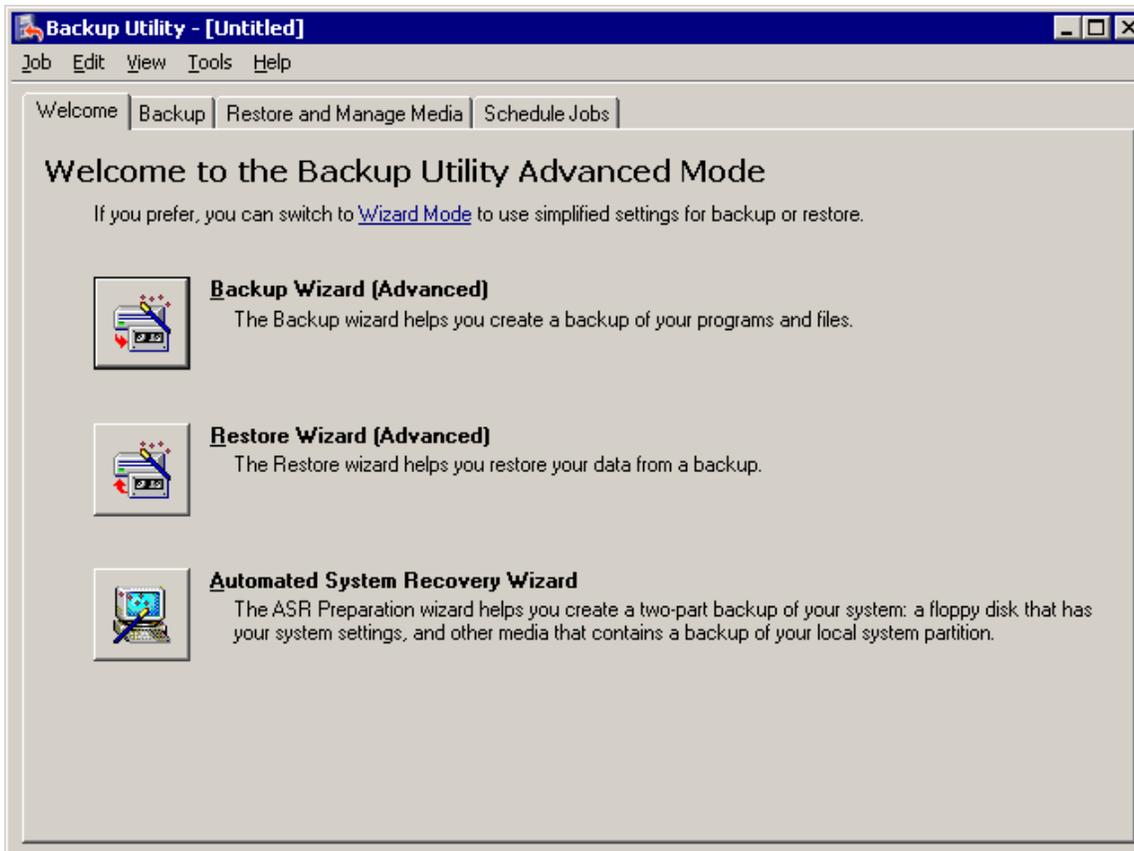
### Perform system recovery for a server.

#### Implement Automated System Recovery (ASR).

The Automated System Recovery is a new feature of Windows Server 2003 that provides complete system recovery in a timely fashion. Dating back to the NT 4.0 Server days there was the `rdisk.exe` utility which maintained a backup of the registry along with operating system configuration information. Moving into the Windows 2000 era the `rdisk.exe` went away and the Emergency Repair Disk was introduced. The ASR is the third evolution of the system repair chain. The ASR backup set is created from the Windows Backup utility and consists of an ASR floppy and an ASR backup file. The process for performing an ASR includes:

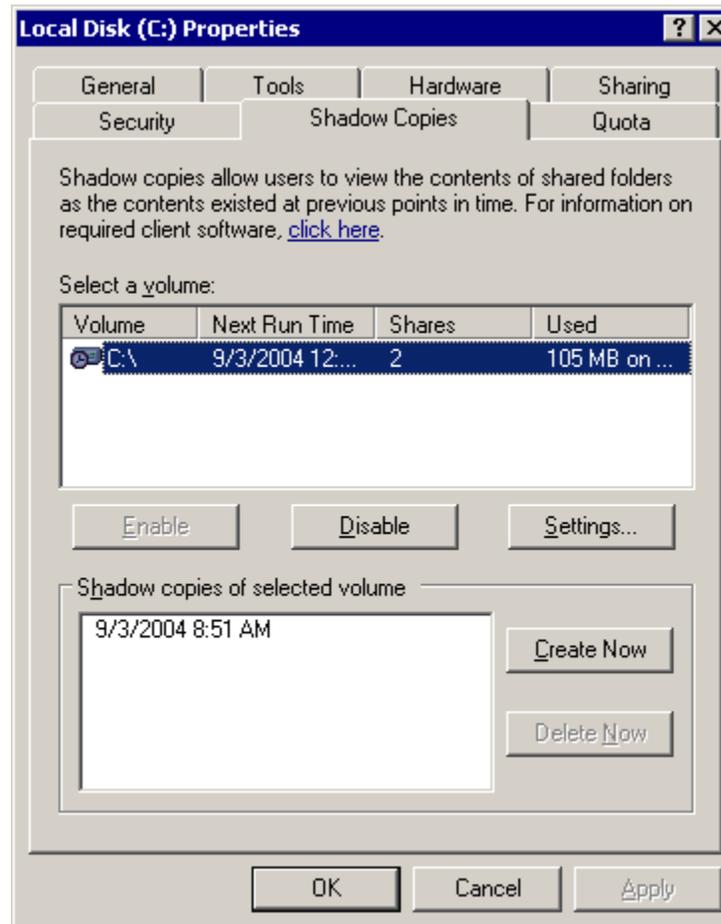
- a) Rebooting the system from the Windows Server 2003 CD-ROM.
- b) Press F2 when prompted and insert the ASR floppy.
- c) Follow the on-screen directions for instantiating the restore of the ASR backup.

The ASR Wizard utility can be seen in the figure below.



### Restore data from shadow copy volumes.

Volume shadow copy is a new feature of Windows Server 2003 that allows administrators to make scheduled copies of all shared files and folders. As shown in the diagram below shadow copies can be enabled and configured on the properties of the volume that stores the required data.

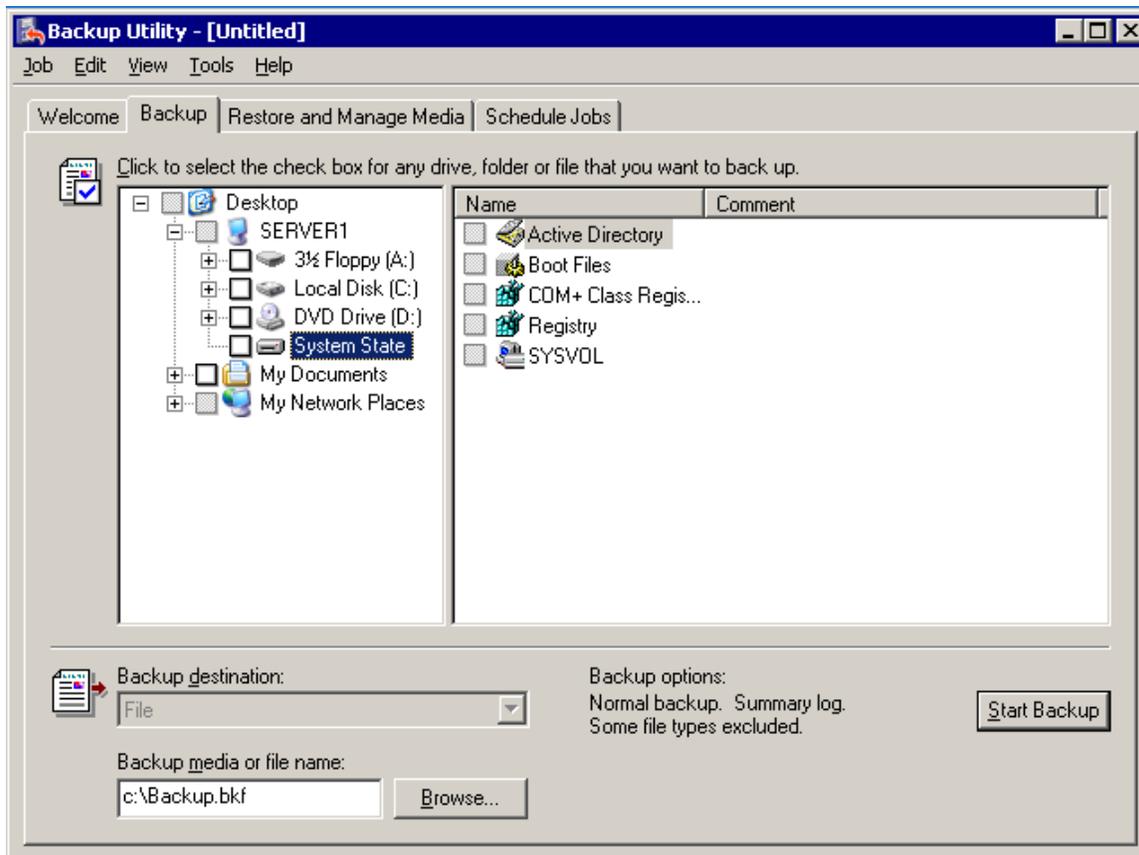


The clients that need to take advantage of Shadow Copies by restoring an older version of a document can do so from the Previous Versions tab of the properties of the file or folder.

<p><b>!</b></p>	<p><b>WARNING:</b> The Previous Versions tab is not available until the twcli32.msi, or Previous Versions Client Software, is deployed to the client systems. This package is available from the C:\Windows\system32\clients\twclient directory on a Windows Server 2003 system.</p>
-----------------	--

### Back up files and System State data to media.

The system state data is a special subset of information that can be backed up through the Windows Backup utility. By default the system state data includes the Boot Files, COM+ Registration Database, and Registry. On a domain controller it also adds in Active Directory and Sysvol while on a certificate server it adds in the certificates database and on a cluster node the cluster configuration information. The figure below shows the components of the system state data for a domain controller.



**WARNING:** ! The components of the system state data cannot be backed up individually. They must be backed up and restored as a complete unit. The system state data CANNOT be backed up or restored remotely.

### Configure security for backup operations.

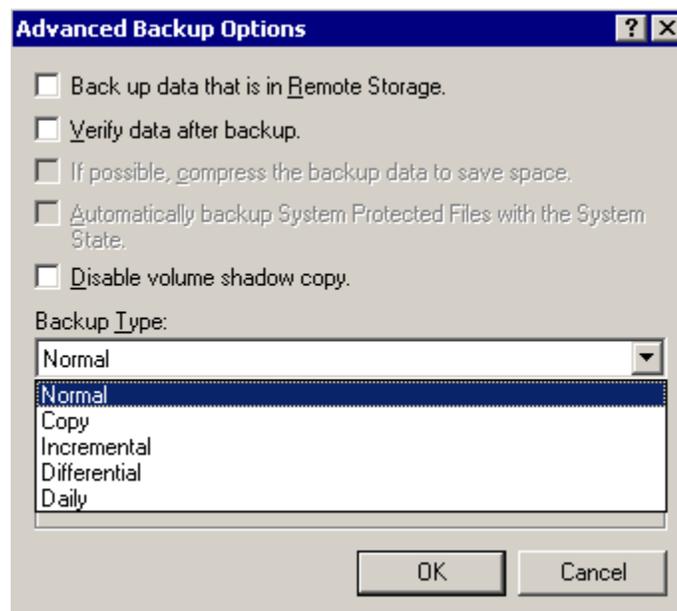
A built-in security group named the Backup Operators is hard-wired with the ability to backup and restore all files. Administrators should utilize this group to provide individuals with the ability to manage backup and restore procedures without having to provide more authority than is required. This group exists on each system and performing these actions on a system requires membership in the group for that system. Being a member of the Backup Operators group on a domain controller gives the rights to back up and restore files on any domain controller.

## Manage backup procedures.

Backups are an integral part of any server administration policy. Files on a system are marked with an archive bit to allow the backup utility to determine if a file has been changed. The different backup types below handle the archive bit in different ways thus changing the amount of time to backup and recover.

- 1) **Normal:** a full backup of all data. The archive bit is reset.
- 2) **Copy:** a full backup of all data. The archive bit is not reset.
- 3) **Differential:** a backup of all data that has changed since the last normal backup. The archive bit is not reset.
- 4) **Incremental:** a backup of all data that has changed since the last normal or incremental. The archive bit is reset.
- 5) **Daily:** a backup of all changes occurring on the day of the backup. The archive bit is not reset.

The figure below displays the Advanced Backup Options that allow for the enabling of remote storage backups, data verification, and disabling of volume shadow copy which would prevent the backup of any opened files during the duration of the backup.



 **NOTE:** The Windows Backup utility has a command line counterpart, ntbakup, which provides all the same functionality through command line switches accompanying the ntbakup utility

## Recover from server hardware failure.

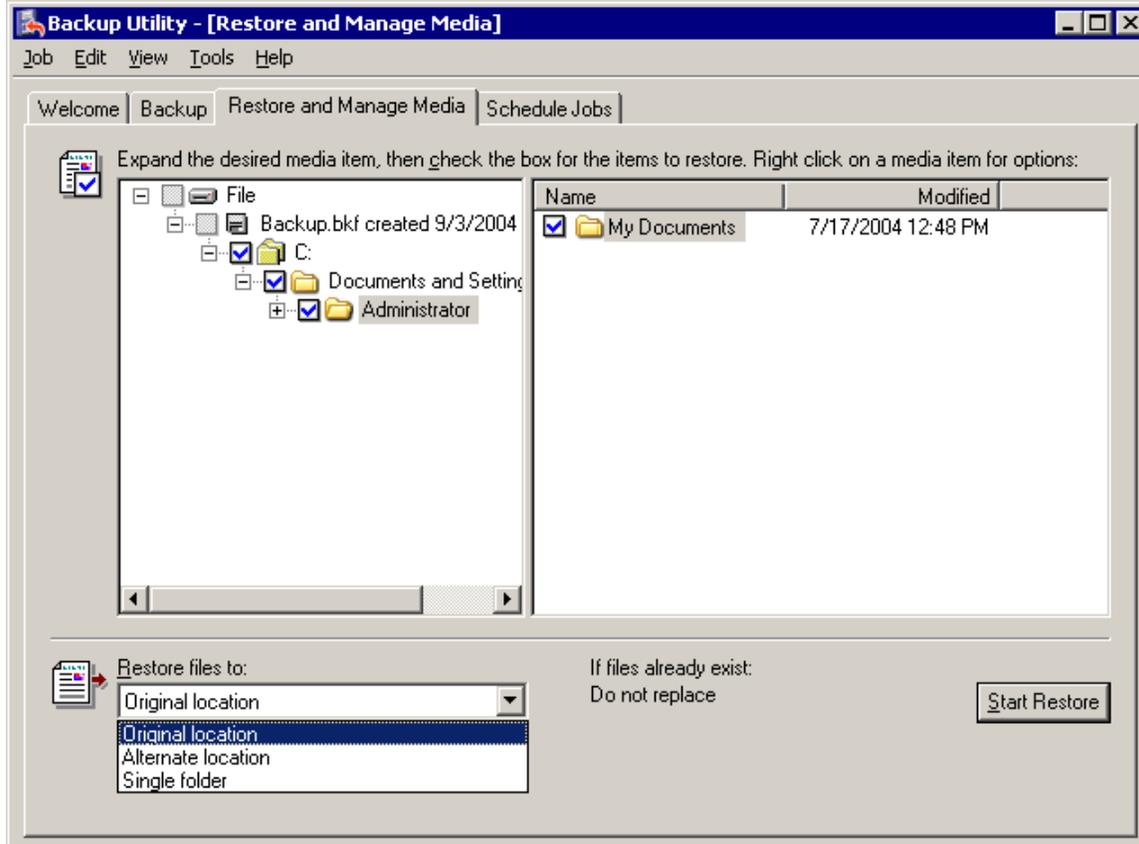
Recovering from server failure can be a cumbersome and timely process. When recovering from a system failure your first attempts at recovery should be that which entails the least amount of

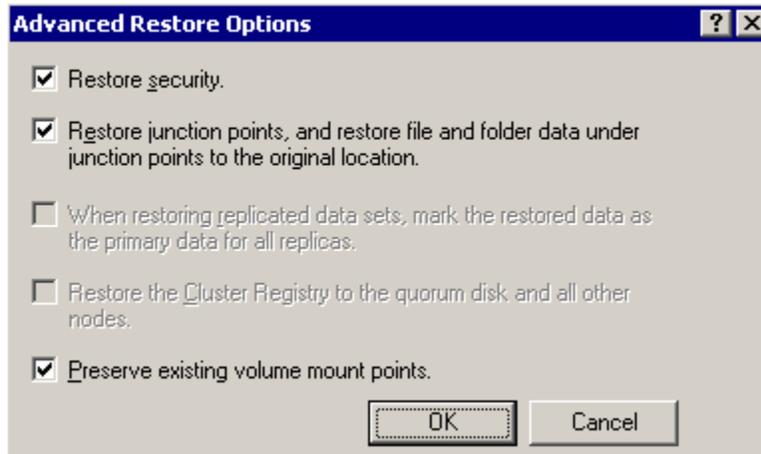
administrative effort. The following recovery techniques are available in Windows Server 2003 and should be attempted in this order when recovering a system provide an enhanced and simplified level of administrative control that includes the ability to upgrade, patch, alter, or remove software. These software packages can be published (deployed as an optional install) or assigned (deployed as a mandatory install). Published software requires a manual effort on the part of the user to install the software via Add/Remove Programs and thus can only be delivered to users. Assigned software is a mandatory install and can be delivered to both users and computers.

- 1) **Last Known Good Configuration:** an easy repair tool that boots off the registry values written during the last successful boot. This should be the first options since it requires the least amount of effort. Unfortunately it only works in cases when a successful logon has not occurred since the system failure.
- 2) **Safe Mode:** The Safe Mode option for Windows Server 2003 allows for access to the user interface with a limited number of drivers being loaded to the system. During this mode device drivers for tape backup devices are loaded to support the backup and restore of files without being able to boot into the full operating system.

### Restore backup data.

Restoring backup data of course is predicated on the successful implementation and completion of a backup strategy. The figures below display the restore windows and Advanced Restore Options available.





As seen in these figures administrators have several options with regards to the files and folders being restored. Data can be restored to its original location, a new location, or a single folder while at the same time administrators have the option to remove the existing security information (rights and permissions) by disabling the Restore security option.

### **Schedule backup jobs.**

Backup jobs can be scheduled through the Windows Backup utility or through the Scheduled Tasks utility. In either case it is imperative that the user context under which the job runs has the appropriate rights to perform the job. If the user account does not have these rights the scheduled backup job is sure to fail.