STUDY GUIDE

Microsoft

70-290

Managing and Maintaining a MS Windows Server 2003 Environment

Chris McCain

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.

Troubleshoot server hardware devices.

- Diagnose and resolve issues related to hardware settings.
- Diagnose and resolve issues related to server hardware and hardware upgrades.

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

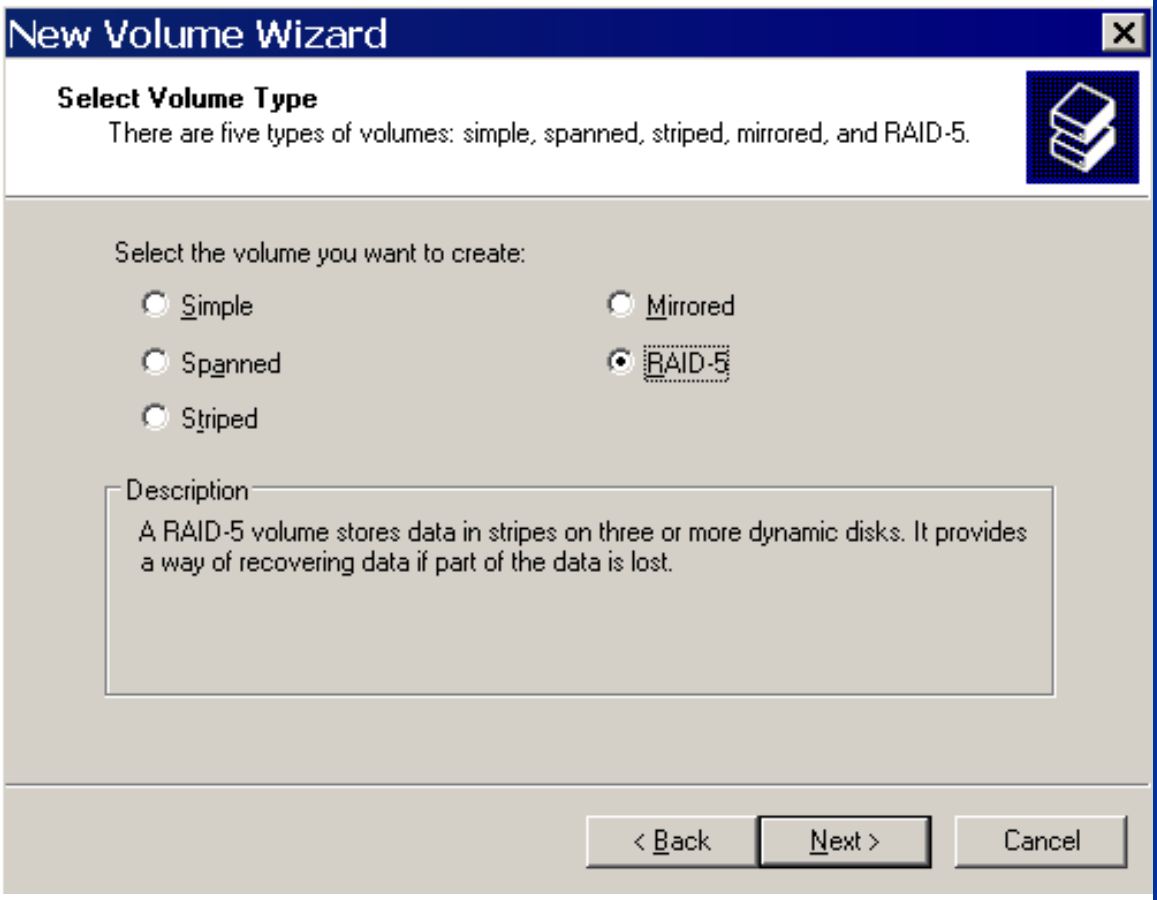
Chapter 1

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 known in 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. The DISKPART utility can be used from the command line to accomplish this. 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 Windows Server 2003 operating system.



Managing disks with the Computer Management snap-in requires the logical disk management service and the logical disk management administrative service.

Basic disks can have a total of 4 primary partitions or 3 primary partitions and 1 extended partition.

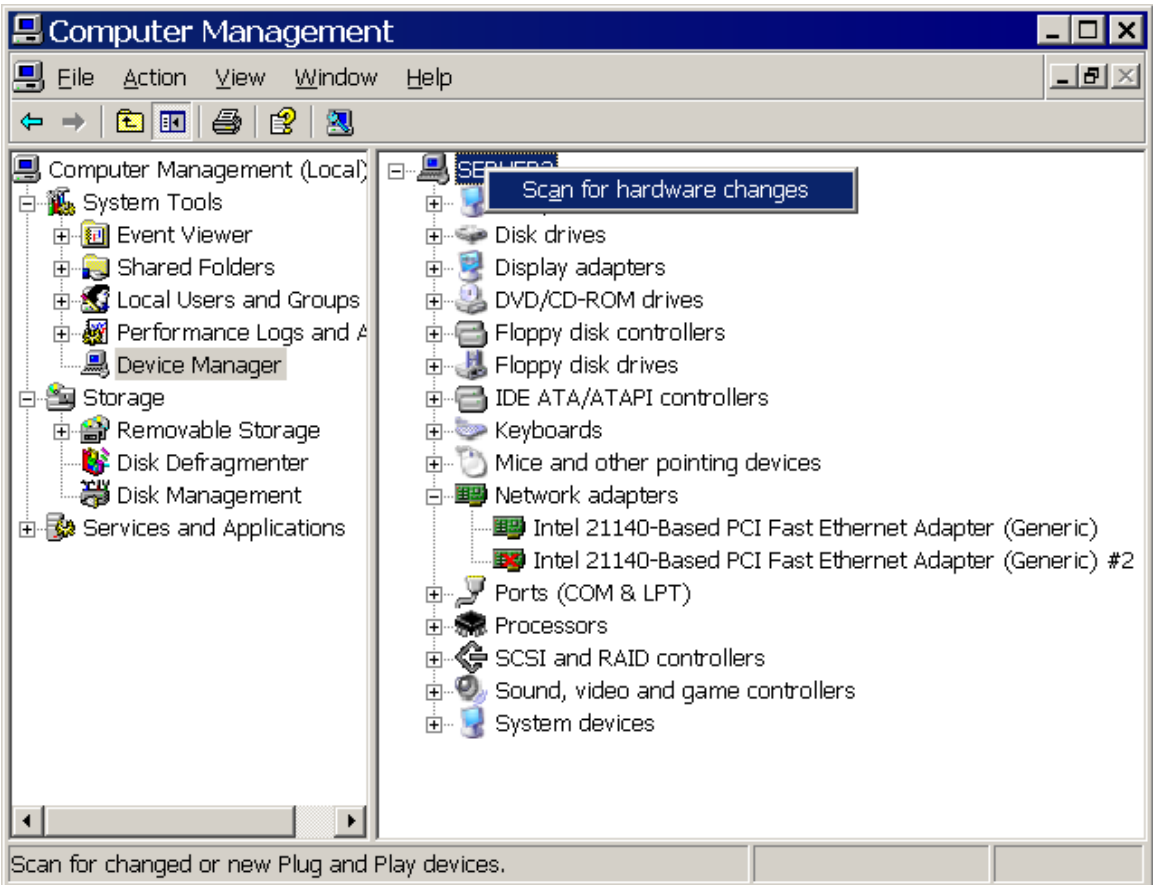
Dynamic disks support fault tolerant volumes and can be used to create any of the following volume types:

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 disk 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.

NOTE:	Dynamic disks do not support dual booting on the same disk and reverting back to basic requires deleting all of the partitions.

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 in a system. Device Manager offers a Scan for hardware changes option for locating and installing 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 adapters.

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.

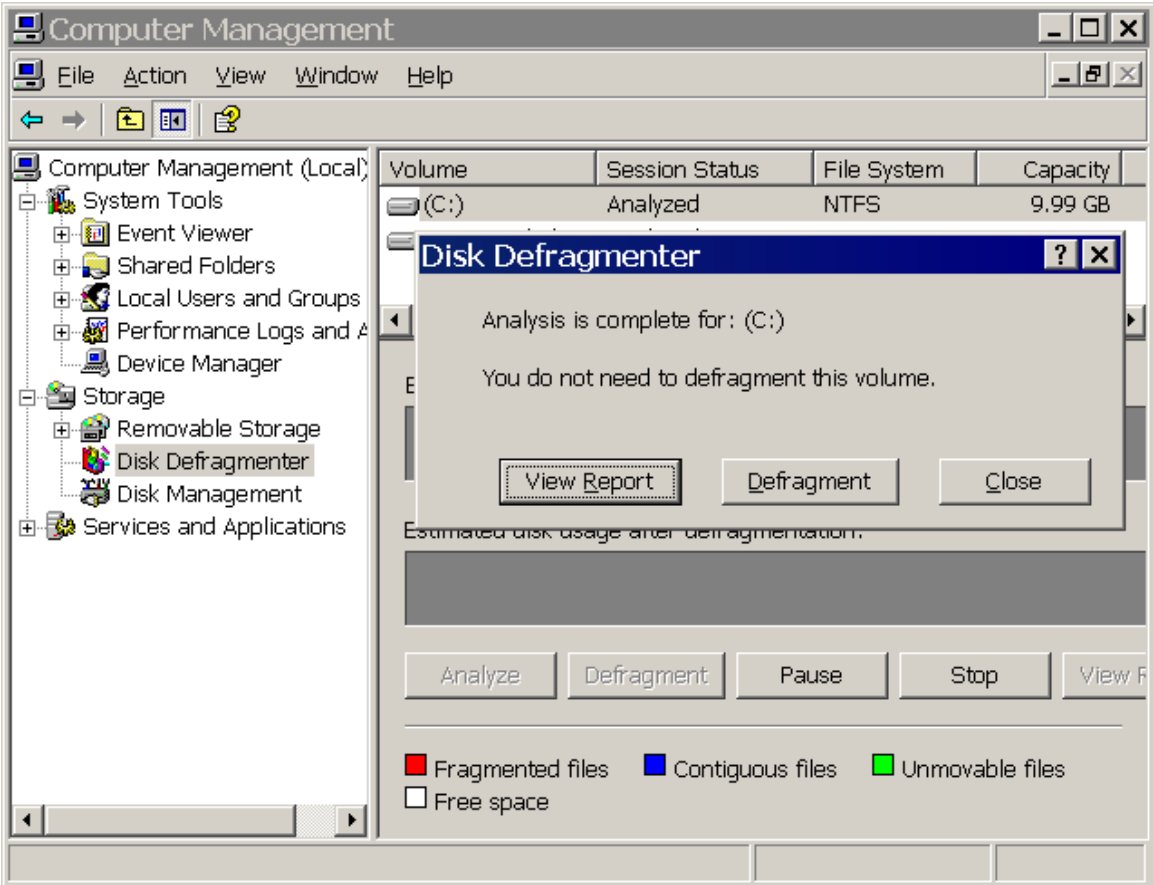
The RAID-1 (mirrored volume) type is better for providing fault tolerance of the system volume. This helps to minimize recovery time in the event of an operating system failure. By copying all operating system configurations and settings to a second volume, administrators can quickly reboot systems that 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, 3 or 32, in the RAID-5 volume it only supports the loss of a single drive.

Defragment volumes and partitions.

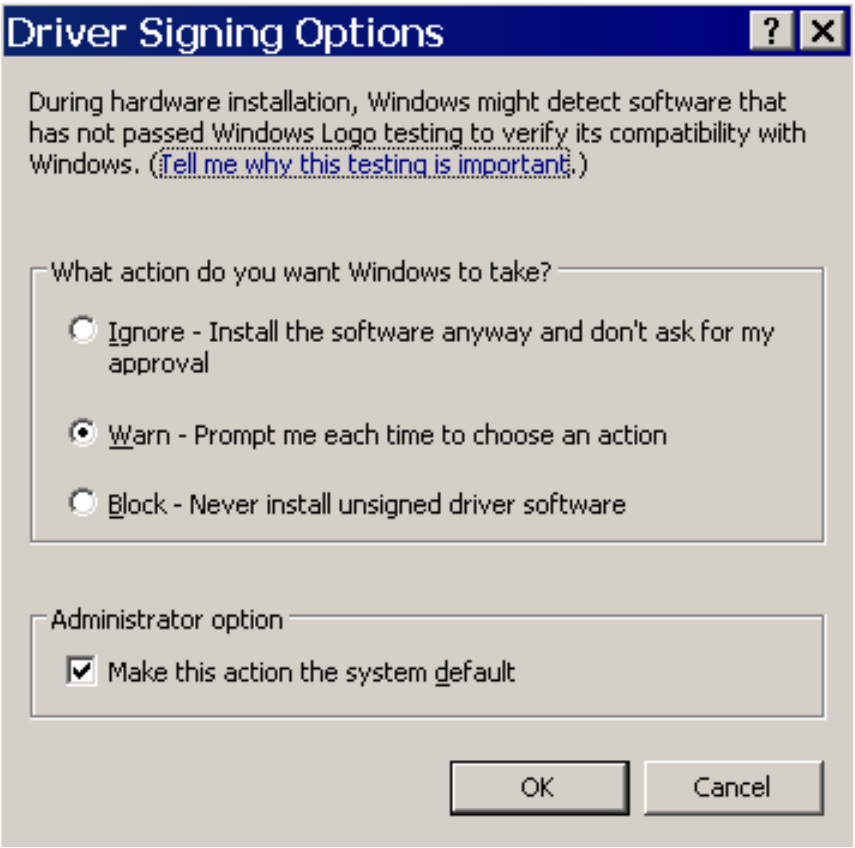
Over time hard drives become fragmented because data written to the physical disk cannot be written into contiguous blocks of space. When fragmented, needed information must be retrieved from multiple locations before being returned to the user. Users are often first to identify the need for defragmentation 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 a volume to determine if defragmentation is necessary.



Install and configure server hardware devices.

Configure driver signing options.

Windows Server 2003 provides Driver Signing Options for identifying devices drivers that have 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 Hardware tab in System Properties. There are three configuration options for Driver Signing, as well as the administrative option of making one of those options the system default.



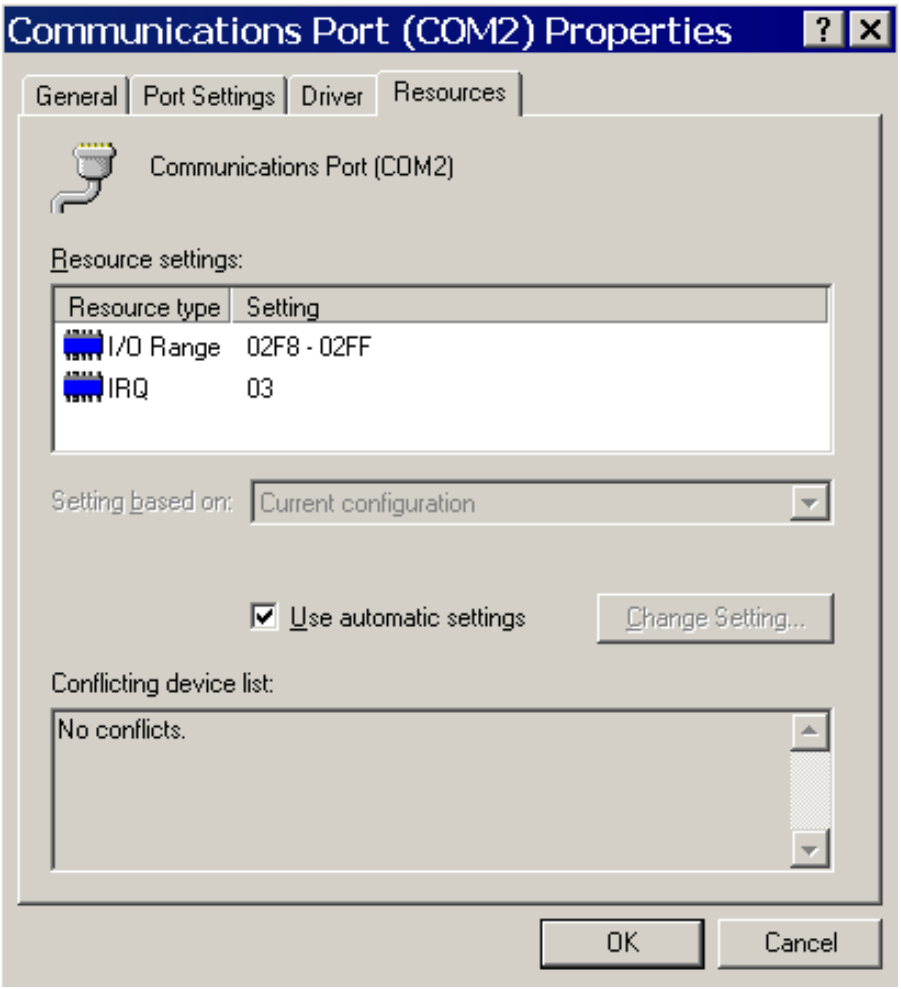
- **Ignore** – This option allows any driver to be installed without warning.
- **Warn** – This option will prompt a user that an unsigned driver is being installed.
- **Block** – This option will block any unsigned drivers from being installed.

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.

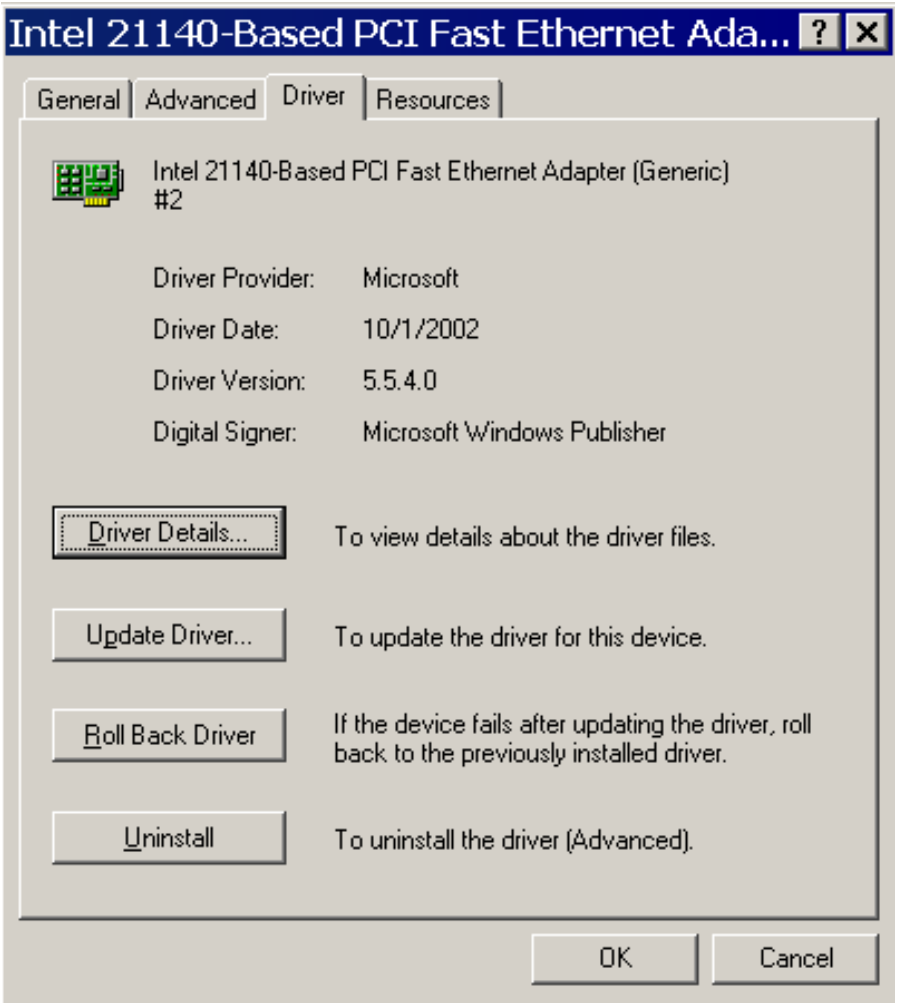
Configure resource settings for a device.

Identifying resource conflicts and device errors is easily done through the Device Manager. As shown in the figure below the properties of a device will display IRQ settings and conflicts. IRQ conflicts are not common anymore because of the introduction of IRQ sharing.



Configure device properties and settings.

The device properties and settings displays 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.

Configuring and troubleshooting Modems.

From the proerties sheet of a modem, a diagnostic query can be run to assist in troubleshooting the device. Older technologies may require lowering the modem's top speed setting to make it easier and more reliable to establish a connection.

Chapter 2: Managing Users, Computers, and Groups

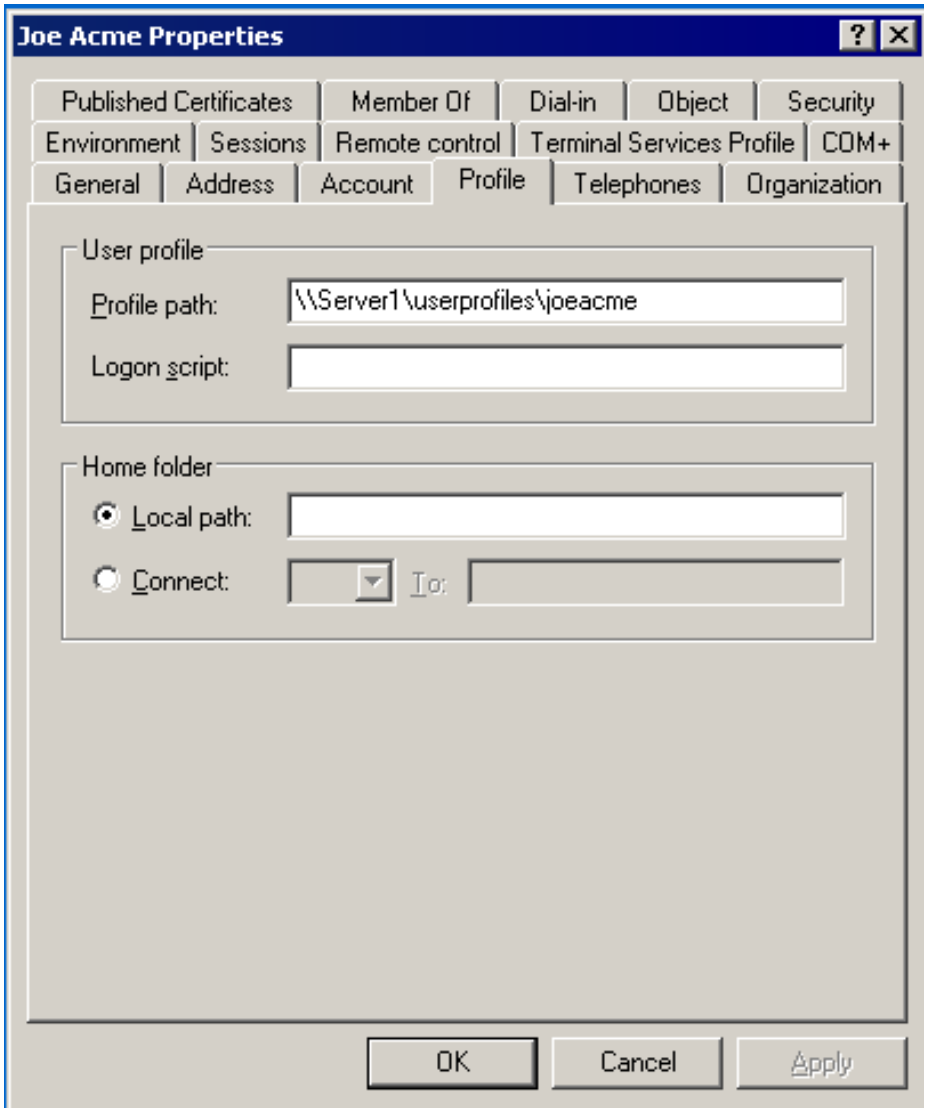
Chapter 2

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 on 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. Roaming profiles are stored in a centralized location to provide accessibility from any system. Profile configuration can be done from properties of a user account. The figure below shows location of the user profile path on the properties of a user account.



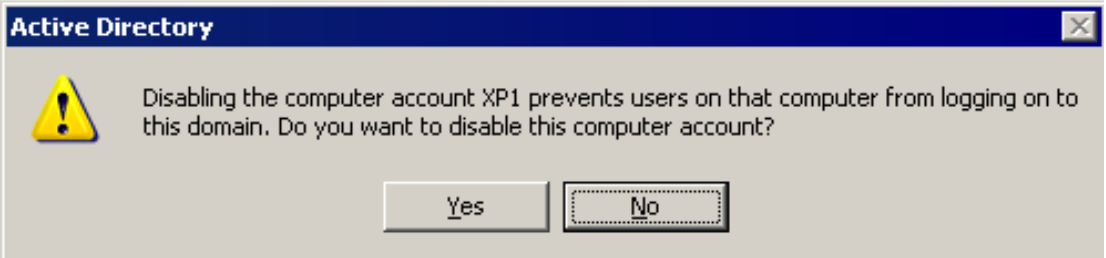
The mandatory profile is a means of locking the user environment. By changing the ntuser.dat file to an ntuser.man file extension the user is then prohibited from saving changes to the profile. Users logging on to the network can receive a default profile by placing the default user profile in the NETLOGON share on a domain controller.

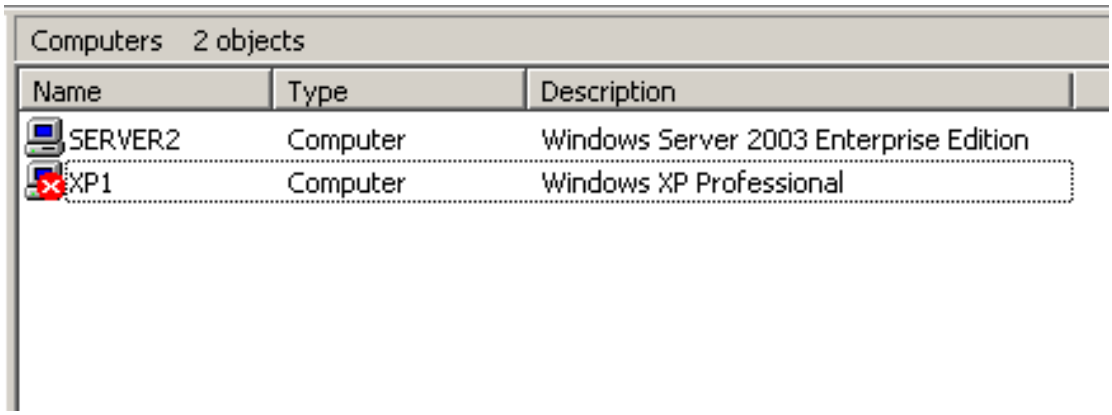
Create and manage computer accounts in an Active Directory environment.

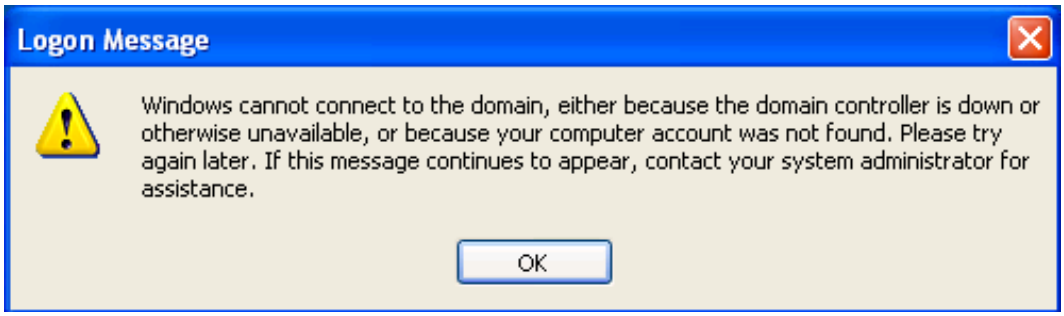
Computers added to a Windows Server 2003 domain are listed by default in the Computers container in the Active Directory Users and Computers management console. Administrators can relocate these computer accounts based upon the administrative and security model of their network. Computer accounts created before the physical system is introduced to the network environment are considered to be 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 Active Directory. This action places a large red X on the computer account. Computers that are disabled generate an error notifying the user that a logon is not available. The figures below show the administrative warning when disabling a computer account, a system indentified as disabled to prevent logon, and the error users receive after the logon attempt from a disabled system.







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 Server 2003 has different group types and group scopes used to accomplish different tasks. For example, the security group type is used anytime administrators are looking to establish resource permission tasks while the distribution group type is used for e-mail. The group scopes include domain local, global, and universal.

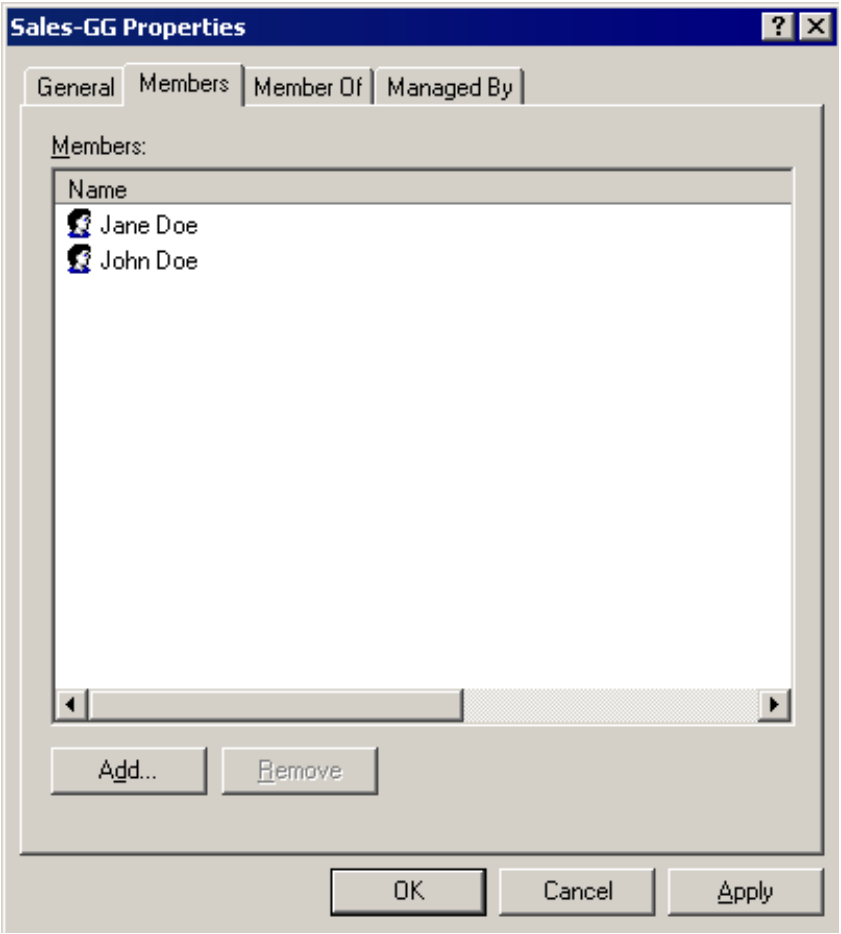
- Domain local groups are used by administrators to assign permissions to resources. A domain local group can contain members from any domain while only being visible for permission assignement in its own domain. Domain local groups are stored in the domain partition of the local domain.

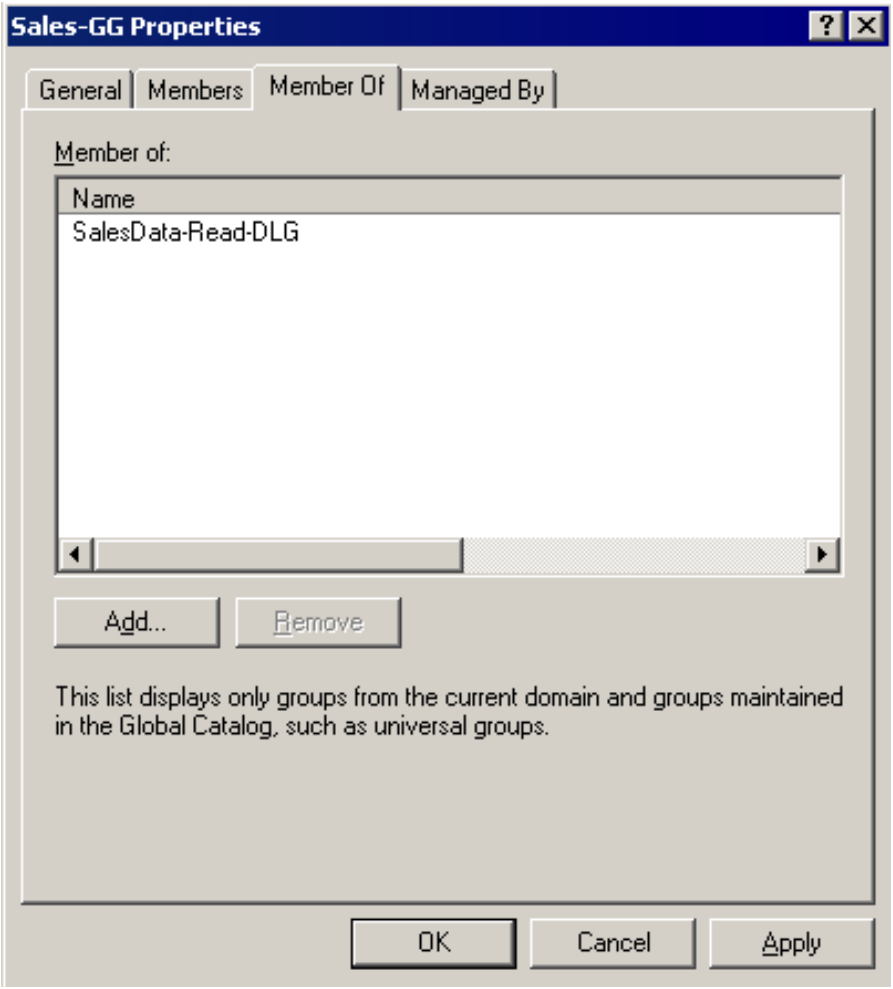
- Global groups are used for organizing users. A global group can only contain members from its own domain but is visible for permission assignment from any domain. Global groups are stored in the domain partition of the local domain.

- Universal groups are only available in Windows 2000 Native mode functional level 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. Universal groups share the best of domain local and global groups. They are able to be seen from any domain and can be accessed from any domain. Universal groups are stored in the global catalog which can be placed on any domain controller in the forest.

Find domain groups in which a user is a member.

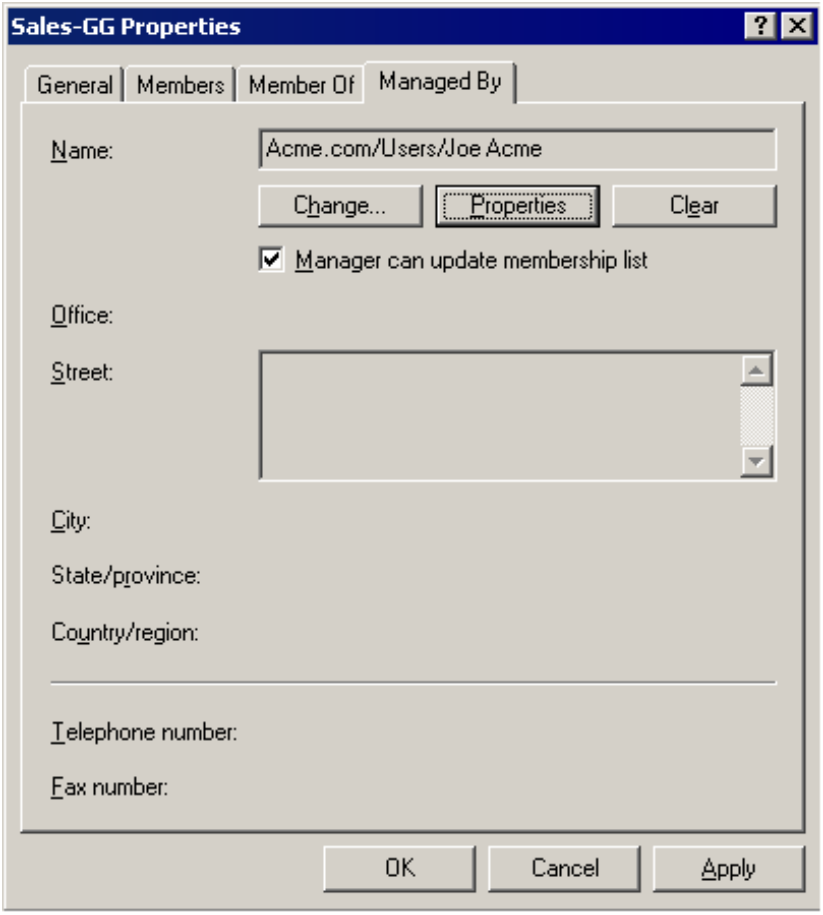
Membership in a group can be obtained from the “Member of” tab of the user account properties or the “Members” tab of the group properties. The figures below display the members that belong to the Sales-GG group as well as the domain local groups to which Sales-GG belongs.


Sales-GG Properties
General
Members
Member Of
Managed By
Members:
Name
Jane Doe
John Doe
Add...
Remove
OK
Cancel
Apply



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.

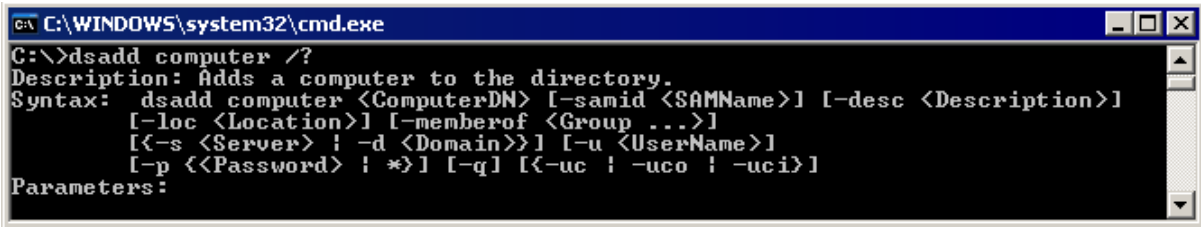


Create and modify groups by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.

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 easy viewing and creation capabilities using either context menus 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.



NOTE: To see more detail about the dsadd computer utility enter **dsadd computer /?** at a command prompt.

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. It also allows for multiple account management. Select multiple accounts of the same type to modify all at the same time.

Create and modify user accounts by using automation.

In large enterprise environments administrators are often tasked with creating or managing many objects. Using GUI methods such as context menus 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 an 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.

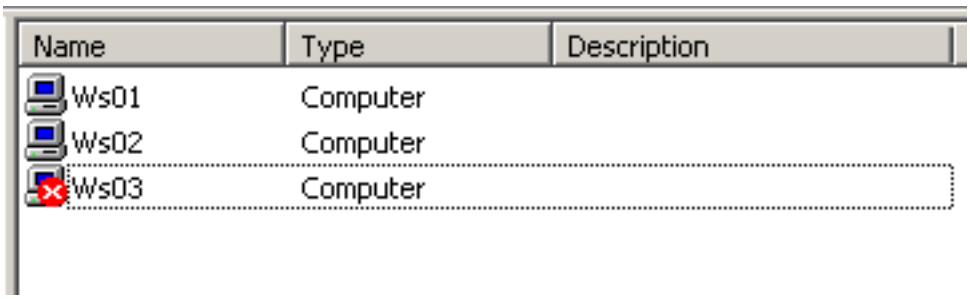
- **DSMOD** is a command line tool that can modify active directory objects.
- **DSQUERY** is a command line tool that can query for active directory objects.
- **DSMOVE** is a command line tool that can move and rename active directory objects.
- **DSADD** is a command line tool that can add active directory objects.

NOTE: When copying user accounts, remember that some attributes do not get copied over including dial-in permissions and terminal services settings.

Troubleshoot computer accounts.

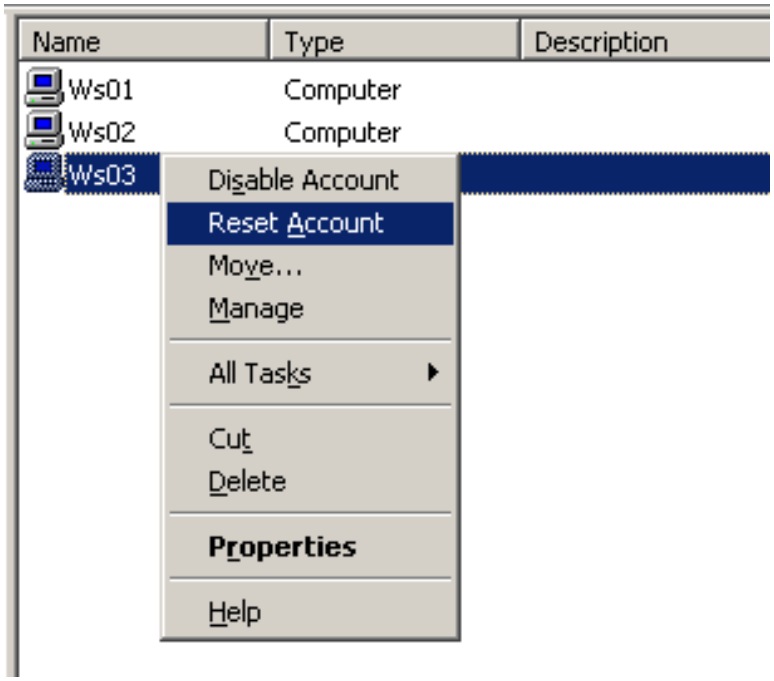
Diagnose and resolve issues related to computer accounts by using the Active Directory Users and Computers MMC snap-in.

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. The saved queries feature allows queries to the database to be saved and refreshed when needed.



Reset computer accounts.

Computer accounts that have lost their secure password relationship to the domain must be reset. This can be accomplished through the Active Directory Users and Computers snap-in or via the nltest.exe command line utility. In either case, a computer account that has been reset will prevent users from successfully logging in until the computer has rejoined the domain and re-established its relationship with the domain. The following figure shows the administrative options for disabling an account vs. resetting an account.

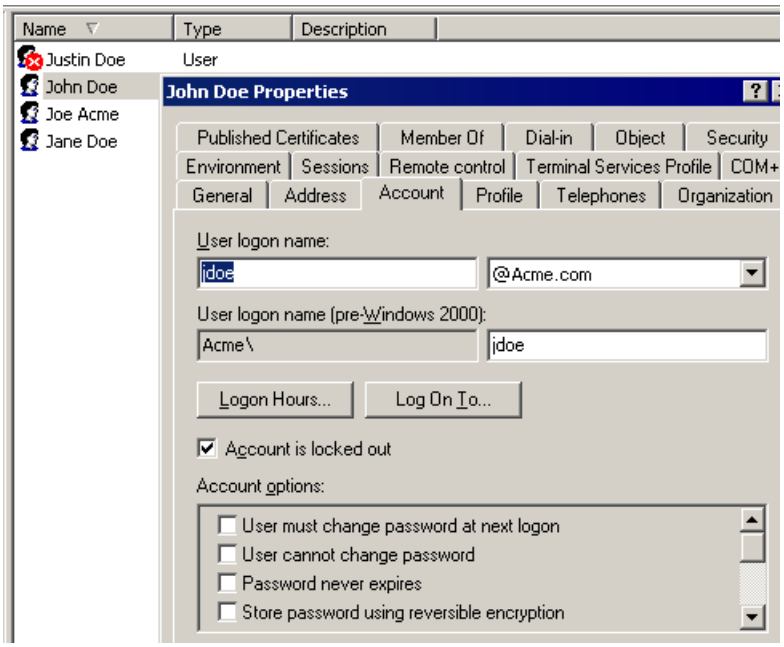


Troubleshoot user accounts.

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 account (Justin Doe) and a locked out account (John Doe). When a user account is

disabled, the user icon is overlaid with a large red X. When a user account is locked out, the Account is locked out box on the Account tab of the user account properties is checked.



Diagnose and resolve issues related to user account properties.

Issues with user accounts 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 resultant 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. In the absence of any of these three pieces, authentication problems will occur. As discussed before, disabling a user or computer account, resetting a computer account, or locking a user account can all result in failed authentication.

When forest trusts are set up, it is possible to authenticate across forests. If forest-wide authentication is enabled, the user only requires permission to the resource. If selective authentication is enabled, an additional configuration needs to be enabled for authentication. A user would need the Allowed to Authenticate permission enabled on the resource. This can be set using Active Directory Users and Computers.

Chapter 3: Managing and Maintaining Access to Resources

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 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.

By default, share permissions are set to Everyone-Read. The three share permissions choices are Allow or Deny the following:

- **Read** – This allows files to be viewed and applications to be executed.
- **Change** – This includes the Read permissions and also allows the user to change files or folders.
- **Full Control** – This includes all Change permissions and also allows the user to change the permissions on the file or folder.

Administrative shares are designated with a $ at the end of the share name. These are built-in shares for administrative use and are hidden when browsing for shares. Hidden shares can be created by adding the $ to the end of a share name. These shares will not be visible on the network.

WARNING: !	Remember that share permissions are not considered when logged on interactively to a system, whereas 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 levels 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.

If Remote Administration is disabled on the properties of the server, Terminal Services will not run on that server.

If users experience problems running legacy applications, change the Permissions Compatibility from Full Security to Relaxed Security. Do not make the user a member of the Power Users group; they have the ability to reboot the server.

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. To access a Terminal Server, standard users require the "Allow logon to Terminal Server" option enabled on their account.

Terminal Services and Group policy.

The easiest way to administer multiple Terminal Servers is through group policy. Settings precedence starts with the client settings, which would be overridden by the Terminal Server settings, which, in turn, are overridden by group policy settings. Group policy can be used to control almost all of the settings of a terminal server and session.

Terminal Server licensing.

Terminal Services licensing must be installed in order to govern licenses. Terminal servers are given a grace period of 120 days to install a licensing server before operations cease. Users have an additional 90 days before requiring a license. There are two licensing models:

- **Enterprise** – This model allows for one licensing server per forest.
- **Domain** – This model allows for one licensing server per domain.

There are two client licensing options:

- **Per user** – This model requires each user of a terminal server to have an individual license.
- **Per device** – This model gives the server a number of licenses and dictates the maximum number of users allowed to connect simultaneously.

NOTE: If users cannot gain access to resources and the permissions and configurations have been verified, check to ensure that sufficient licenses are available.

Configure file system permissions.

NTFS permissions provide for file and folder level security. NTFS permissions are always evaluated, whether being accessed remotely or locally. The default NTFS permission for a file is Read & Execute and Read. The default NTFS permissions for a folder are Read and Execute, List Folder Contents and Read. The following is a list of the common NTFS permissions:

- **Read** gives the ability to view files and folders.
- **Write** gives the ability to add files or folders.
- **List Folder Contents** gives the ability to see what is contained in a folder. (folders only)
- **Read and Execute** gives the ability to execute applications.
- **Modify** gives the same rights as all previous permissions in addition to being able to modify a folder or file.
- **Full control** gives all of the permissions of Modify and the ability to delete subfolders and files and change permissions.

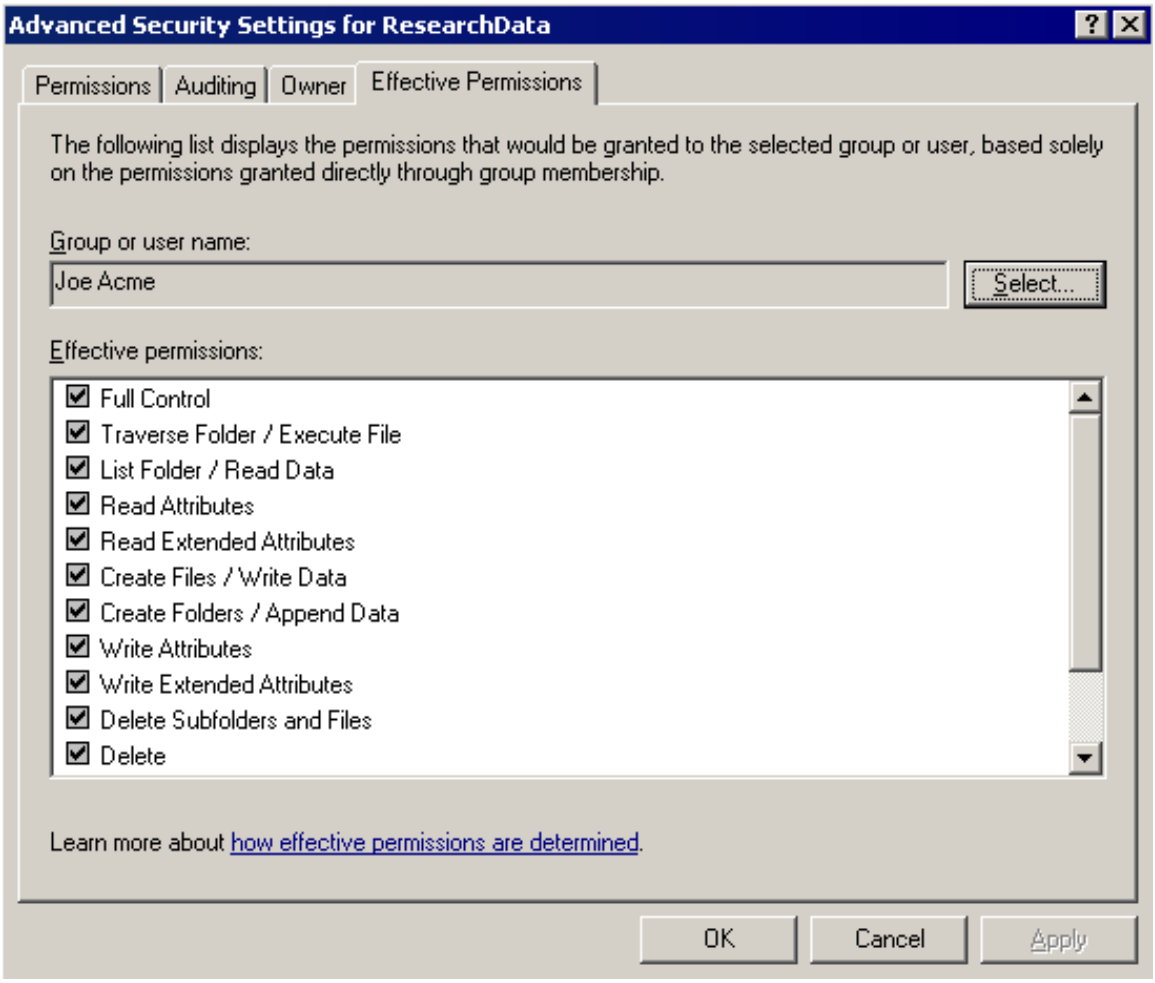
NOTE: Permissions options will differ depending on whether the object is a file or folder. List Folder Contents does not apply to files so would not be listed in the security control list of a file.

Permission Precedence is an important concept for determining permissions. There are three permissions that can be assigned.

- **Implicit Deny** is the absence of any permission designation. If no permissions are defined, no access is granted.
- **Explicit Allow** overrides Implicit Deny because permissiona are now being defined. It grants access to a given object. Allow permissions are cumulative in that they will build on each other and the greatest permissions will be granted.
- **Explicit Deny** is absolute. If an Explicit Deny is set, all other permissions are overridden.

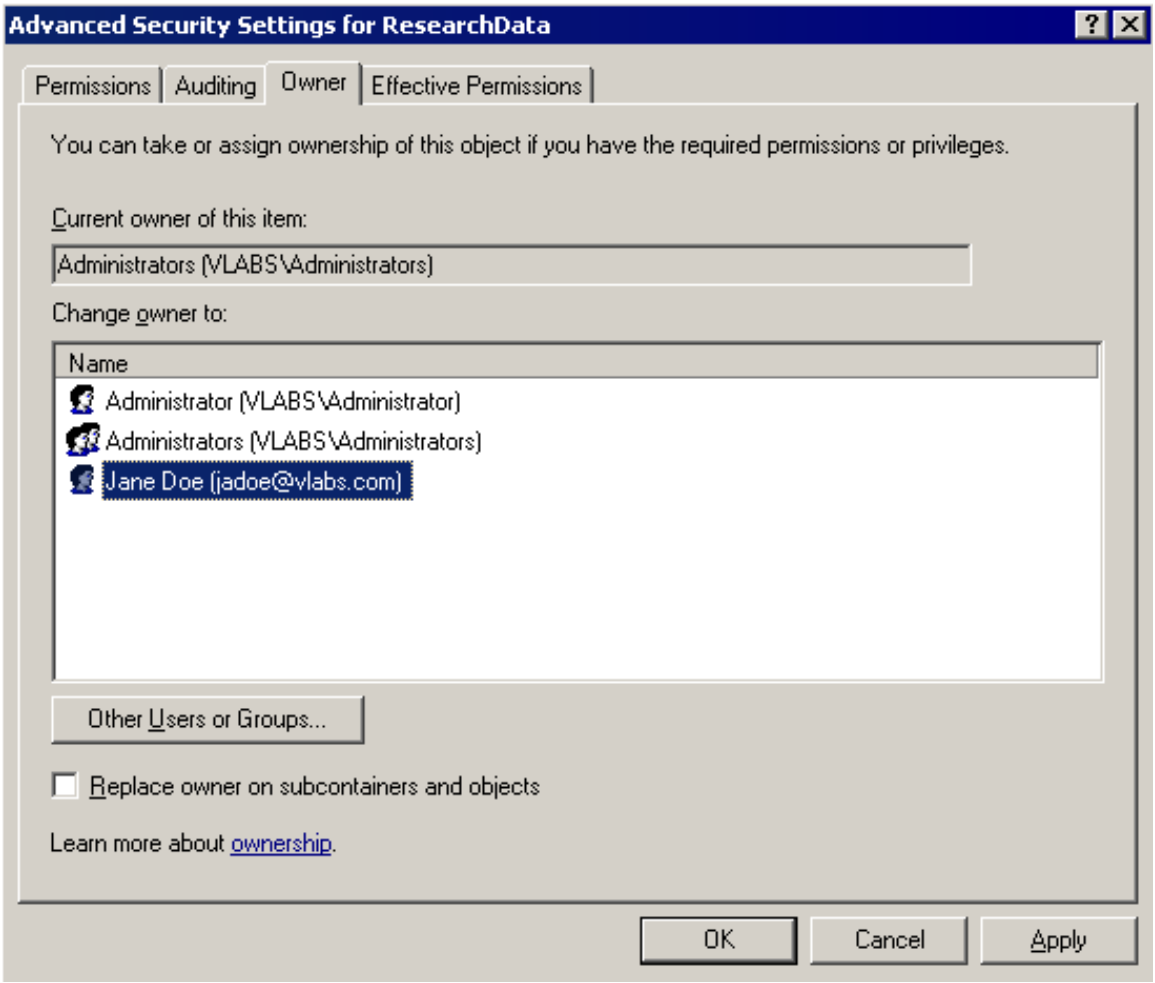
Verify effective permissions when granting permissions.

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. Effective permissions do not account for share permissions. The figure below shows that the user named Joe has Full Control. With this configuration, 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.



Assigning Permissions.
Permissions should be assigned using Microsoft's best recommended practice of AGDLP. Accounts go into Global Groups which go into domain local groups which get assigned permissions. ADLP and AGUDLP are acceptable solutions in different situations.

Chapter 4: Managing and Maintaining a Server Environment

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:

- The **system log** contains events logged by Windows system components. For example, if a driver fails to load during startup, an event is recorded in the system log. Windows predetermines the events that are logged by system components.

- The **security log** records events such as valid and invalid logon attempts. It also logs events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrators group or Server Operator group in order to turn on, use, and specify which events are recorded in the security log.

- The **application log** contains events logged by programs. For example, a database program may record a file error in the application log. Events that are written to the application log are determined by the developers of the software program.

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. When a server is promoted to a domain controller, the Active Directory log and the File Replication service logs are created.

There are five event types in Event viewer. The five types are:

- **Information** - An event that describes the successful operation of a task, such as an application, driver, or service. For example, an Information event is logged when a network driver loads successfully.

- **Warning** - An event that is not necessarily significant. However, it may indicate the possible occurrence of a future problem. For example, a Warning message is logged when disk space starts to run low.

- **Error** - An event that describes a significant problem, such as the failure of a critical task. Error events may involve data loss or loss of functionality. For example, an Error event is logged if a service fails to load during startup.

- **Success Audit (Security log)** - An event that describes the successful completion of an audited security event. For example, a Success Audit event is logged when a user logs on to the computer.

- **Failure Audit (Security log)** - An event that describes an audited security event that did not complete successfully. For example, a Failure Audit may be logged when a user cannot access a network drive.

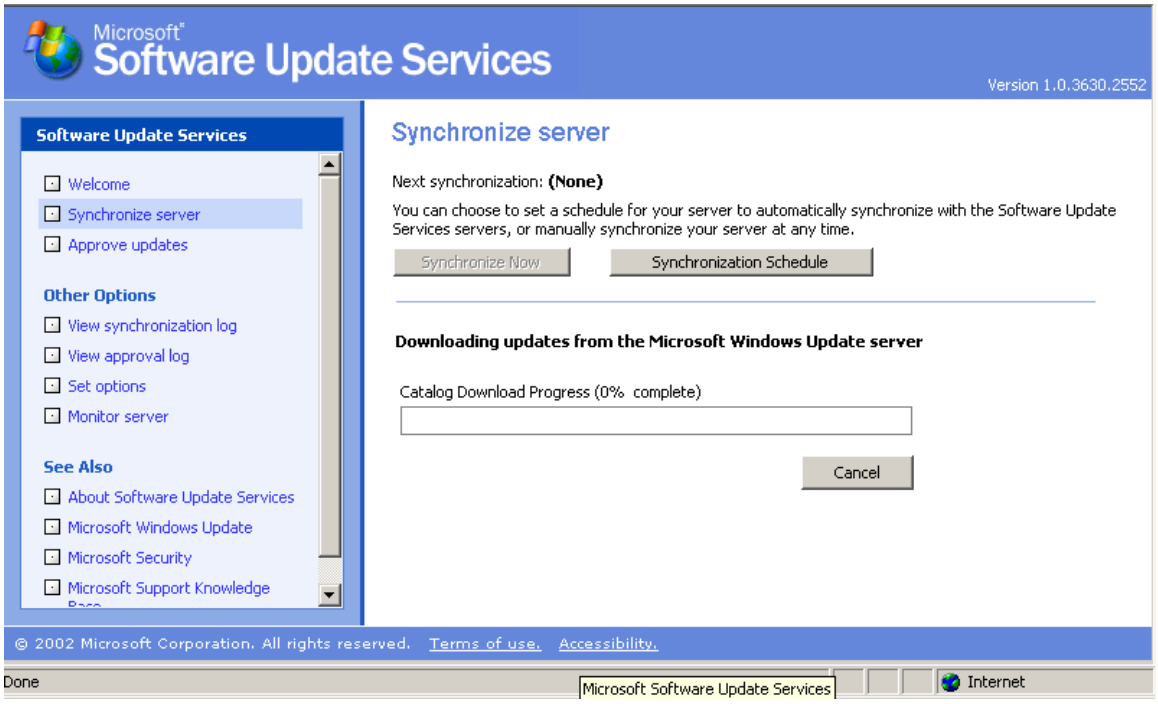
NOTE:	Event Viewer logs can be filtered for specific event types

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 service packs hot fixes and 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 is 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.

Software Update Service (SUS) backup and restore. The procedure for backing up SUS is as follows:

1. Backup the default website to the IIS metabase using the IIS console.
2. Backup the IIS metabase, the default website and the SUS content directory using the NTbackup utility.

Restoring a SUS server is the reverse process:

1. Use NTbackup utility to restore the IIS metabase, the default website and the SUS content directory.
2. In the IIS console, restore the metabase file.

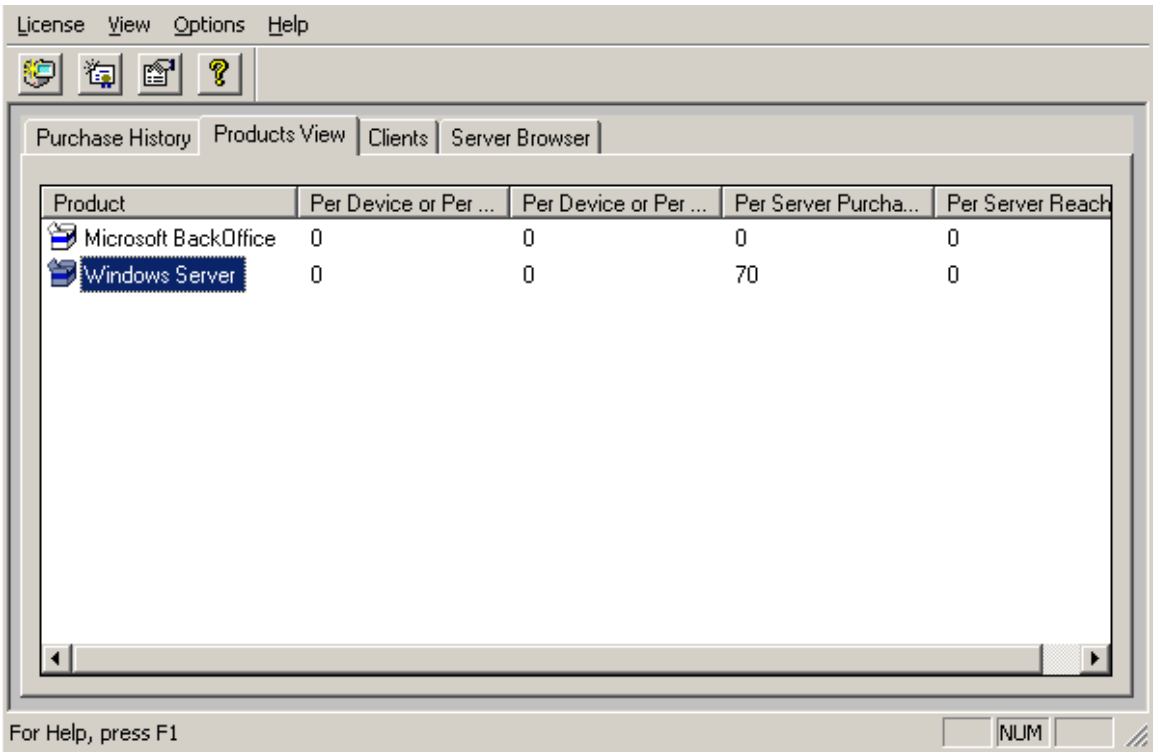
Software Update Service (SUS) clients can be configured individually on each machine or through a GPO. The Automatic Update service needs to be running on the clients for the update to work. The options for downloading and installing are as follows:

1. Notify for download, notify for install.
2. Auto download, notify for install.
3. Auto download, auto install (scheduled).

NOTE: For network segments without Internet access, the SUS content directory can be copied via the network or CD/DVD media to allow updates to isolated clients

Manage software site licensing.

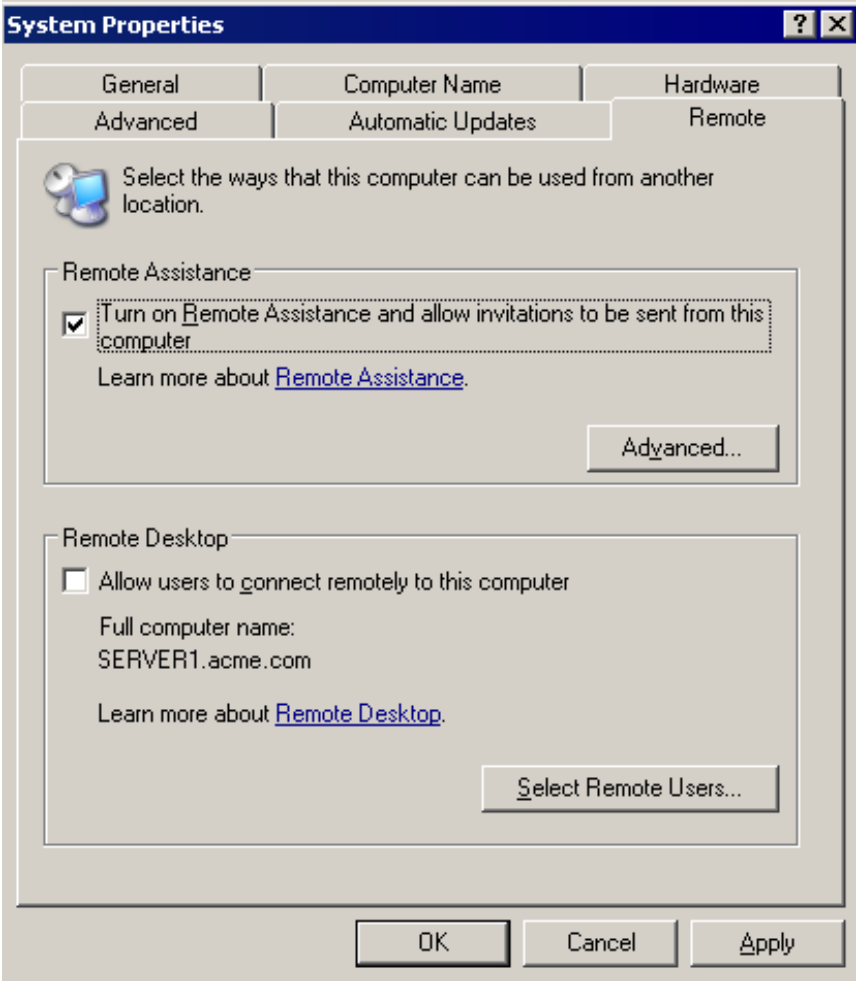
Licensing of the Windows Server 2003 product family is done through the Licensing console. Licenses can be added and revoked as needed through the Licensing console. A site licensing server needs to be designated per site and can be viewed or changed in Active Directory Sites and Services.



Manage servers remotely.

Manage a server by using Remote Assistance.

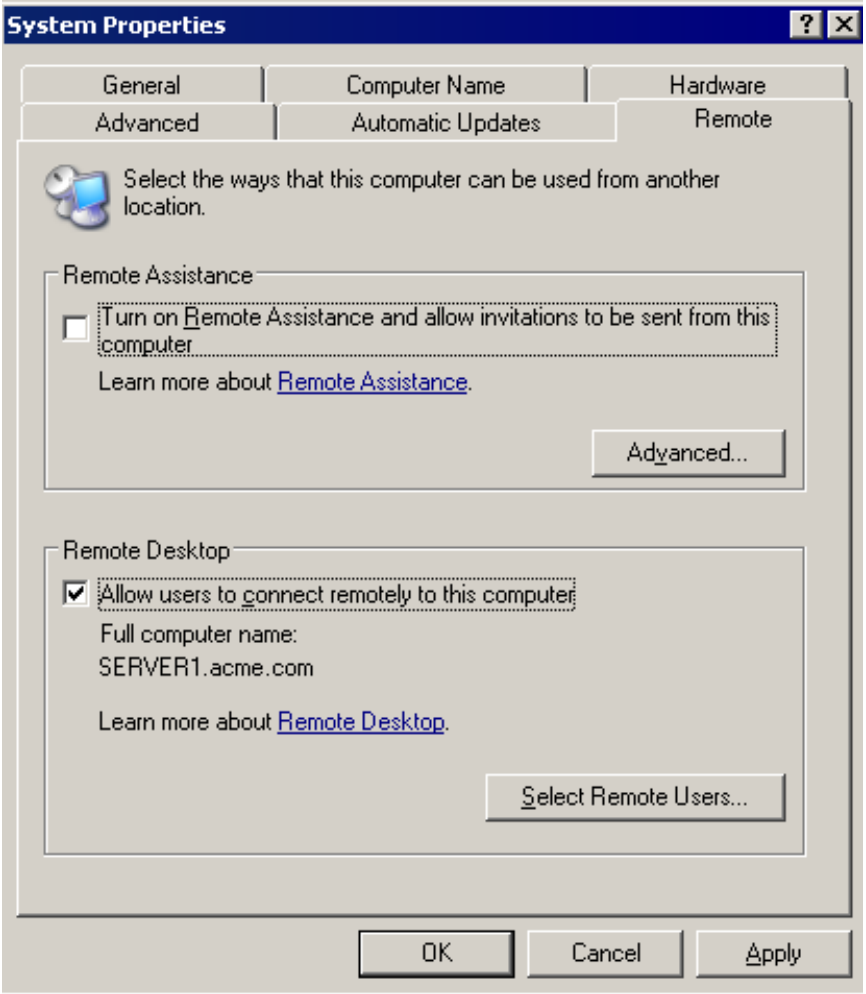
The Remote Assistance feature of Windows Server 2003 allows for “expert” users to assist “novice” users in times of need. Remote Assistance must be enabled on the system where the invitation for help is initiated. The figure below shows the portion of the System Properties, Remote tab, where Remote Assistance 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 offer of assistance from the expert user. The Remote Assistance invitations can also be configured with an expiration to prevent an excessive delay in the request, as well as a password for added security. 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 Remote Desktop Administration.

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



Remote Desktop Administration is enabled on the Remote tab of System Properties. Once enabled, the only users who can access the system by default are members of the Administrators group and the Remote Desktop Users group.

WARNING: !	When accessing a domain controller via Remote Desktop Administration, the Remote Desktop Users group must be granted the Allow Logon through Terminal Services right via Group Policy.

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 and install the adminpak.msi on their workstation to use the default management consoles for remote systems management. Management snap-ins such as Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and more. The remote registry service must be running to perform remote management.

These tools should be used in conjunction with a secondary logon using the Run As function to open the remote management tools. This will help to ensure server security is maintained.

WARNING: !	When installing the adminpak.msi from the Windows Server 2003 CD-ROM install tools, it defaults 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 the registry is edited to disable the enhanced security.

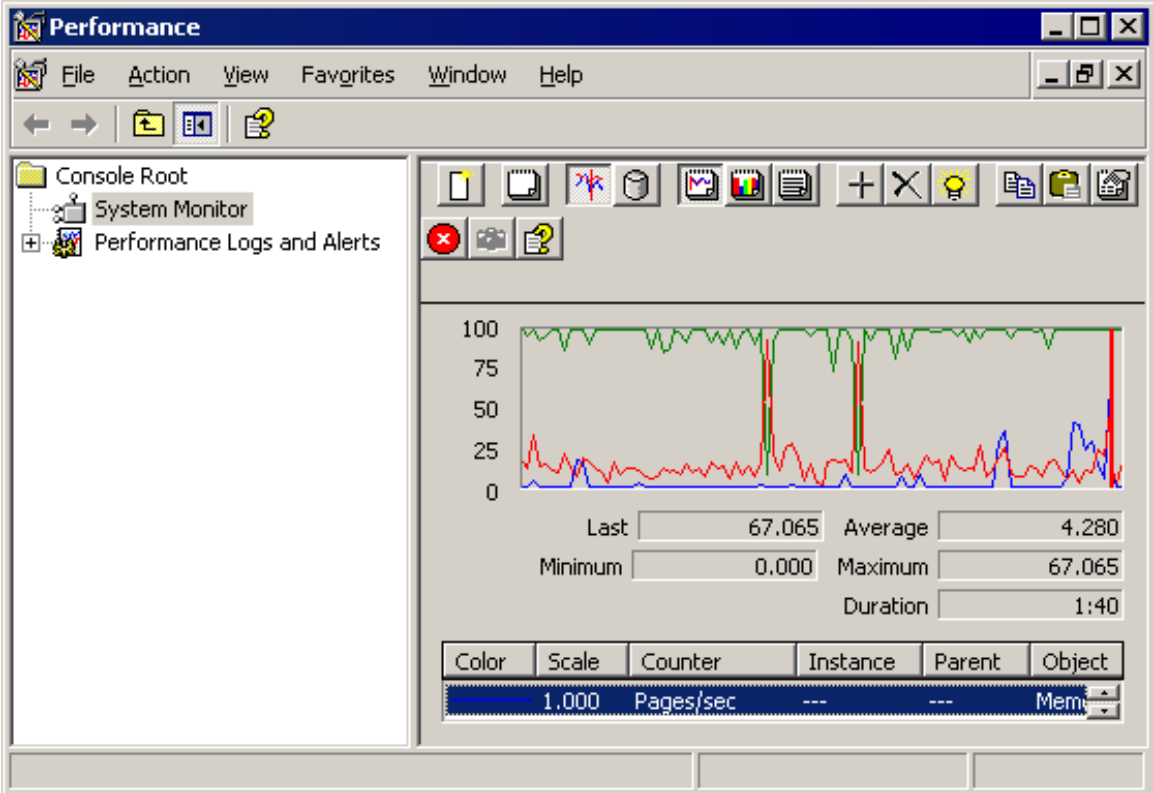
Troubleshoot print queues.

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.

WARNING: !	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 bottlenecks and make decisions with regards to hardware upgrades to improve performance. System Monitor can be viewed in Graph, Histogram and Report views. Baselines should be created for all servers to help diagnose a course of action when a problem occurs. A counter log is the best type of log for marking baselines. Storing logs on a central SQL database is the best method of log rentention for quick and easy searches. The types of logs are:



- **Counter logs** - record performance data on the selected counters at a specific sample interval. For example, you could sample performance data for the CPU every 15 minutes.

- **Trace Logs** - Trace logs record performance data whenever events for their source providers occur. A source provider is an application or operating system service that has traceable events.

    - Sequential Trace File Writes records events to the trace log sequentially up to the max file size (if any).
    - Circular Trace File Overwrites replacesold data with new data when the file reaches a specified size limit.

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 has already saved information.

Monitor server hardware for bottlenecks.

Monitoring 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 even system failure. Armed with this data, administrators may be able to pre-empt bottlenecks or failures 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, thus causing the server has to swap data out of the faster RAM memory into the slower hard drive paging file. The best way to mitigate a high number of Pages/sec is to add more RAM.

NOTE:	Each system is different and it is therefore 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 network adapters are measured in Mbps. Therefore it is necessary to convert Mbps to Bytes/sec 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%.

Monitor disk performance objects.

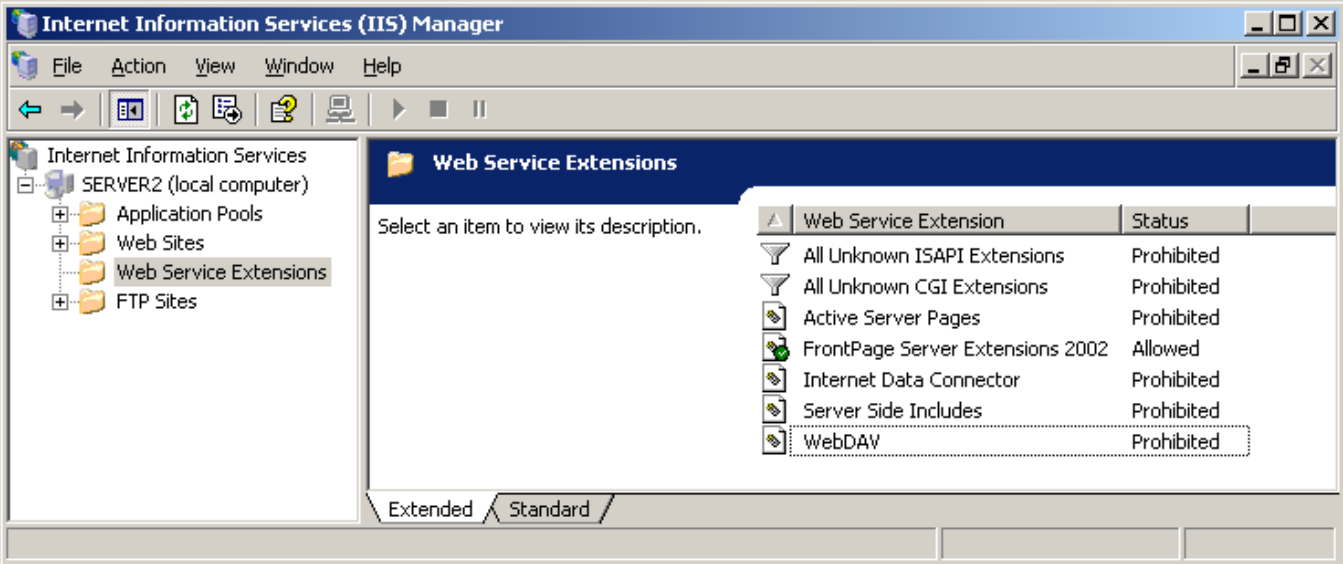
The last object of the big 4 is the Average Disk Queue Length for the Physical Disk counter. An excessive value for the Average Disk Queue length identifies that the hard drive is not processing requests fast enough and, thus, there are requests waiting. A general rule for the Average Disk Queue Length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

WARNING: !	A high value for the Average Disk Queue Length could be a result of an excessive amount of paging and possibly be misdiagnosed as a need for faster or more hard drives. This action, however, would NOT remedy the excessive paging.

Manage a Web server.

Manage Internet Information Services (IIS).

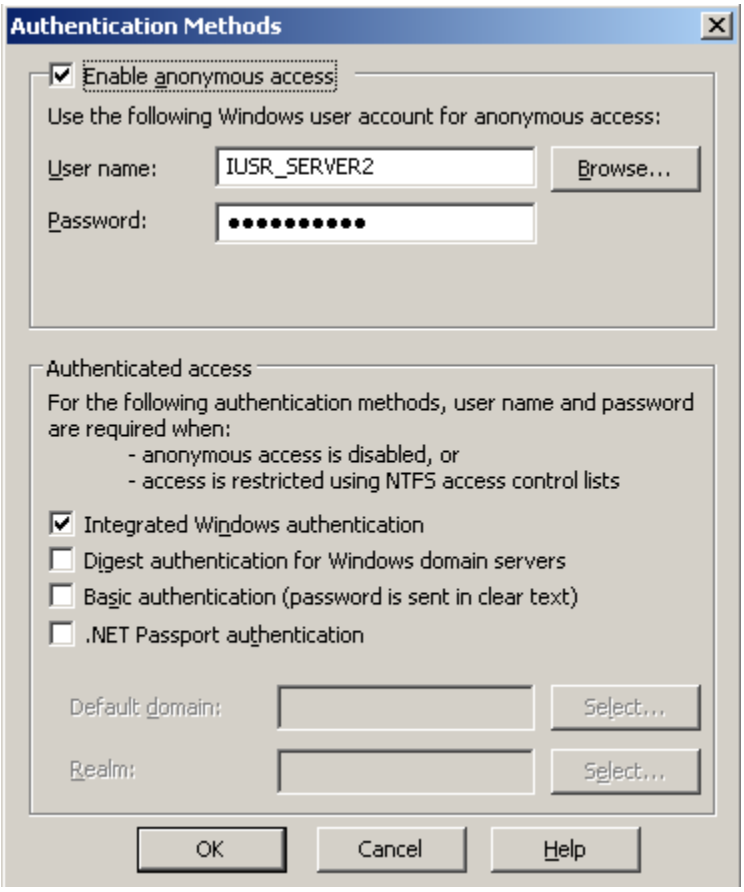
Windows Server 2003 includes the ability to install Internet Information Services 6.0. As part of Microsoft's initiative on building a secure computing environment, IIS 6.0 is not installed by default. Even upon installation of IIS 6.0 it is not open for any services other than serving static content; it is essentially "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. By default, all of the web service extensions are disabled, including ASP pages and WEBDAV.



WARNING: !	With all of these services prohibited by default, administrators will experience failure of their ASP applications and theWebDAV feature until the features have been changed to the Allowed configuration.

Manage security for IIS.

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



Anonymous authentication allows public users to easily access web sites without requiring any form of authentication. If this is 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 authenitication does not support firewall traversal or non-Microsoft operating systems.

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

Auditing is configured through the local security policy on an individual machine or through group policy for a group of machines. There are four different configurations for auditing. These include success, failure, success and failure or not defined. There are nine different auditing policies:

- **Audit account logon events:** auditing of network authentications.
- **Audit account management:** auditing of the creation, deletion, or modification of security principals.
- **Audit directory service access:** auditing of specific objects within the Active Directory database.
- **Audit logon events:** auditing of console logons and log offs.

- **Audit object access:** auditing of specific files, folders, printers, and registry keys.
- **Audit policy change:** auditing of modifications to policies regarding user rights or audit policy.
- **Audit privilege use:** auditing of users exercising their rights, for example backing up and restoring files.
- **Audit process tracking:** auditing of application activation or process termination.
- **Audit system events:** auditing of system events like starting, restarting, or shutting down a system.

WARNING: !	Although it is possible to configure auditing at the local system level, if the system is part of a domain environment it is best practice to use broader level Group Policies to manage multiple systems rather than micromanaging at the system level.

Chapter 5: Managing and Implementing Disaster Recovery

Quick Jump To:

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

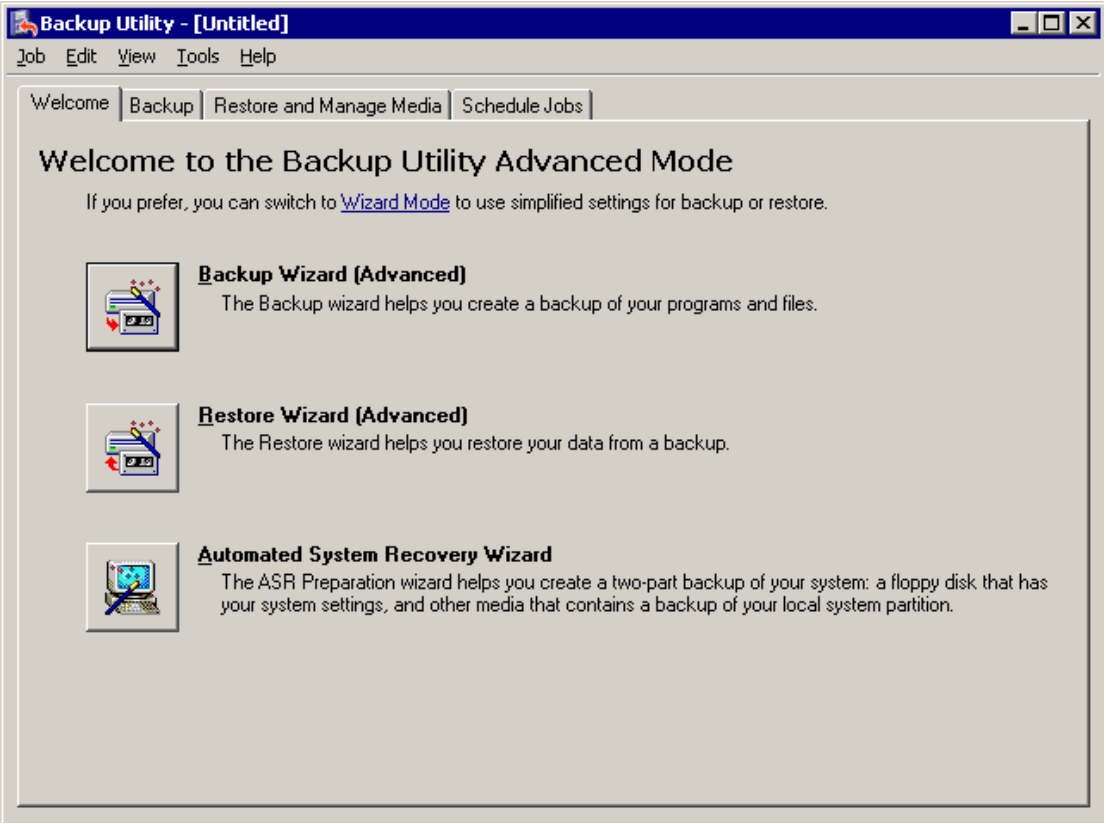
Perform system recovery for a server.

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, 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:

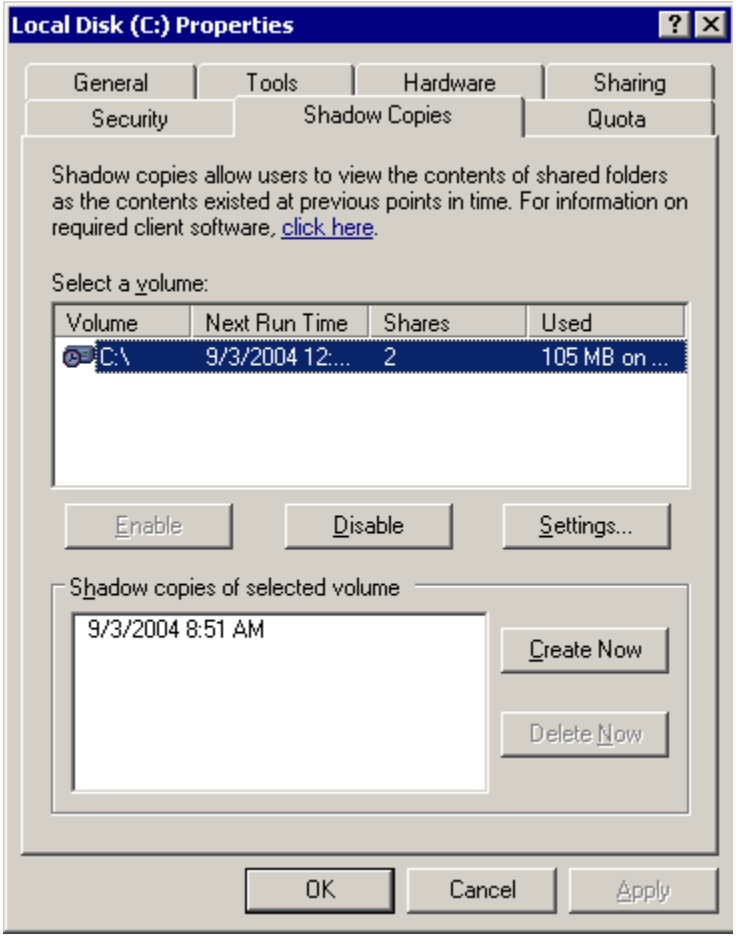
a) Rebooting the system from the Windows Server 2003 CD-ROM.
b) Press F2 when prompted and insert the ASR floppy.
c) Follow the on-screen directions for initiating the restoration of the ASR backup.

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.

WARNING: !	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.

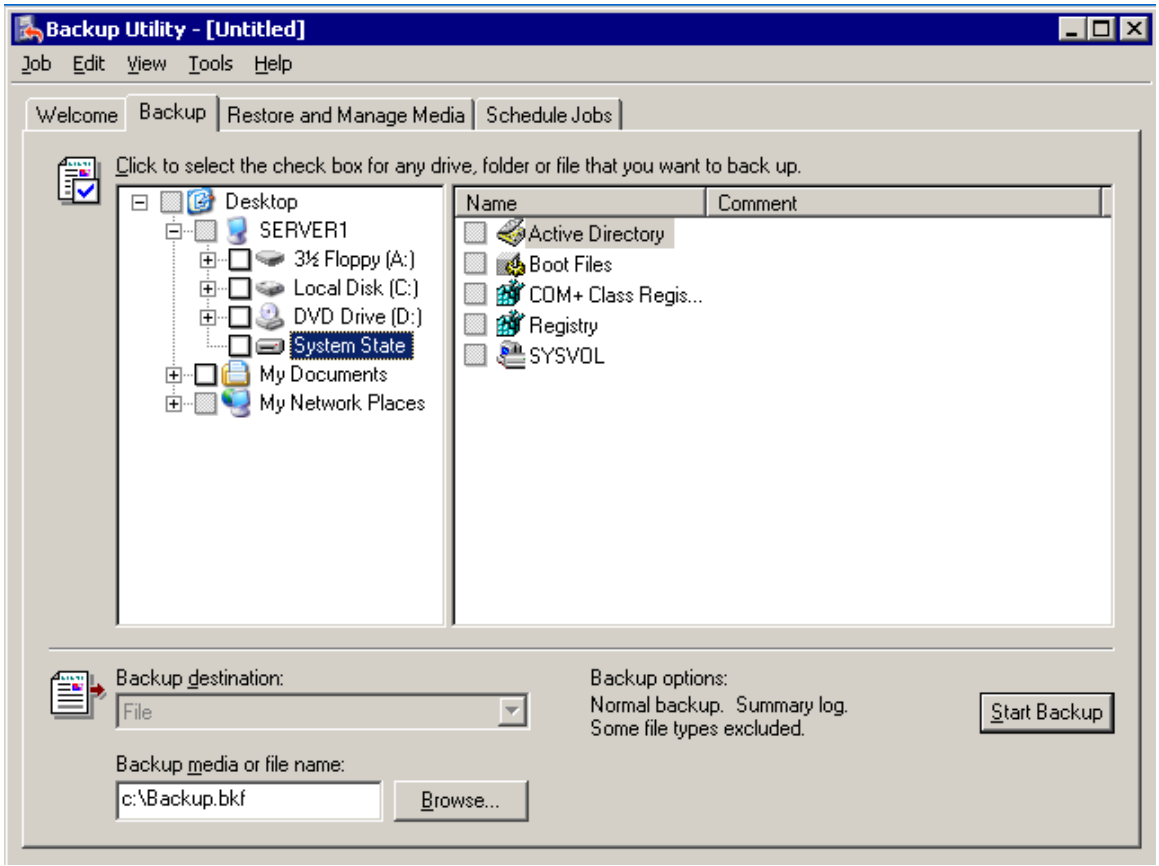
Shadow Copy allows for three types of restore:

- **Restore** is the normal function which overwrites the existing file.
- **Copy** allows the file to be restored to a different location so the current file is not lost.
- **View** allows viewing the document before making a decision to restore.

NOTE: If a file has been deleted, it is necessary to restore the entire folder in order to recover the missing file.

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 that the components of the system state data for a domain controller are the Active Directory database, Boot Files, COM+ files, the Registry and the SYSVOL.



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.

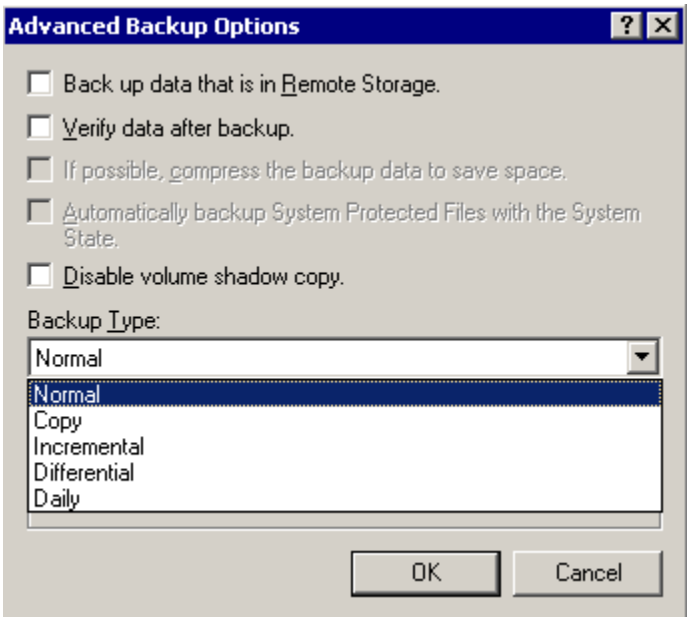
A built-in security group named the Backup Operators is hard-wired with the ability to backup and restore all files. Administrators should utilize this group to provide individuals with the ability to manage backup and restore procedures without having to provide more authority than is required. This 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, NTbackup, which provides all the same functionality through command line switches accompanying the NTbackup utility.

Recover from server hardware failure.

Recovering from server failure can be a cumbersome and timely process. When recovering from a system failure, the first attempts at recovery should be that which entail 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.

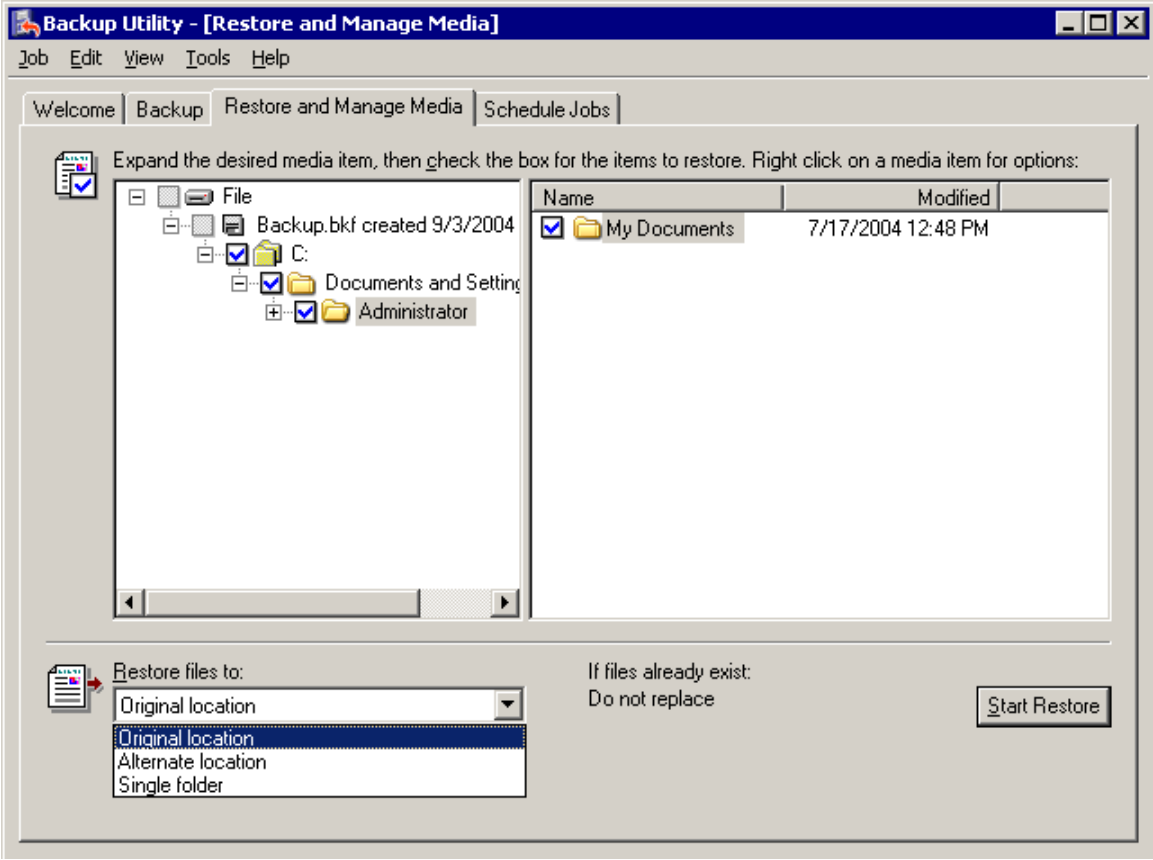
1) **Last Known Good Configuration:** an easy repair tool that boots off the registry values written during the last successful boot. This should be the first options since it requires the least amount of effort. Unfortunately it only works in cases when a successful logon has not occurred since the system failure.

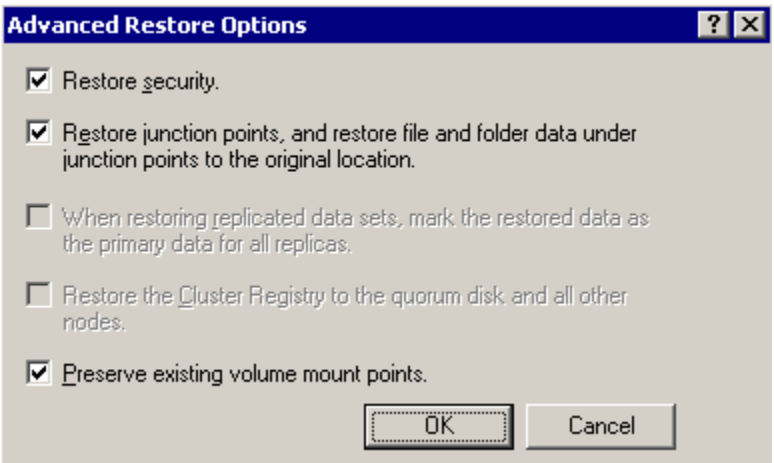
2) **Safe Mode:** The Safe Mode option for Windows Server 2003 allows for access to the user interface with a limited number of drivers being loaded to the system. In this mode, device drivers for tape backup devices are loaded to support the backup and restoration of files without having to boot into the full operating system.

3) **Recovery console:** The recover console allows for limited command prompt access to the operating system. The recovery console can be installed or can be reached using an installation CD.

Restore backup data.

Restoring data from backup is predicated upon 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. Administrators also have the option to remove the existing security information (rights and permissions) by disabling the Restore Security option.

Restoring backup data to a domain controller requires booting into a special form of Safe Mode called Directory Services Restore Mode. This is only available on domain controllers and is access the same way as Safe Mode. It boots the operating system without loading the Active Directory database so that it can be manipulated.

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 will fail.