070-218

TEST KING

LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

Managing a Microsoft Windows 2000 Network Infrastructure

Version 1.4

Important Note
Please Read Carefully

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of just cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

We are constantly adding and updating our products with new questions and making the previous versions better so email us once before your exam and we will send you the latest version of the product.

Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that particular pdf file being distributed by you. Testking will reserve the right to take legal action against you according to the International Copyright Law. So don't distribute this PDF file.

Q. 1
You are the administrator of your company's Windows 2000 file servers. Users on the network secure some of their files by using Encrypting File System (EFS).

An employee named Marc leaves the company. An employee named Maria needs access to some of Marc's files. The files are in a shared folder for which all users have permission to read these files. However, some of Marc's files are protected EFS.

You need to allow Maria access to all of Marc's files. What should you do?

A. Move the files to a partition that is formatted as either FAT or FAT32.
B. Use an EFS Recovery Agent to decrypt the files.
C. Take ownership of the files and assign Maria the **Allow-Read** permission for the files.
D. Assign Maria the **Allow-Take Ownership** permission for the files.

Answer: B
Explanation: Windows 2000 uses private key-based cryptographic schemes for file encryption. Therefore, when a user encrypts a file, only that user will be able to use the file. If the file owner's private key is not available, a person designated as the Recovery Agent can decrypt the file using his or her own private key. After the files are decrypted other users can access the files if they have the required NTFS permissions to those files. In this scenario Maria would be able to access the files as all users have permission to read these files.

Note: To decrypt a file of folder you must clear the **Encrypt Contents To Secure Data** check box in a folder's or file's **Advanced** Attributes dialog box. You can access a folder's or file's **Advanced** Attributes dialog box from the **Properties** dialog box for the folder or file.

Incorrect Answers:
A: File encryption is only supported on NTFS volumes, therefore, by moving encrypted files to a FAT or FAT32 partition the encryption would be lost. This would then enable Maria to read the files if they are moved to a shared folder. Maria will not require any additional permissions as NTFS permissions are not supported on FAT or FAT32 partitions. However, before we can move the files we must have the Modify permission for the source files because Windows 2000 deletes the files from the source folder after it is copied to the destination folder. We must therefore first take ownership of the files.
C: Maria already has read permission to the files as all users have permission to read these files; however, Marc's files are encrypted. Only the owner of the file can use the file once it has been encrypted, regardless of read permission. It is because of the encryption that Maria cannot access the files.
D: The **owner** of the file or any user with **Full Control** permission can assign the Full Control standard permission or the Take Ownership special access permission to another user account or group, allowing the user account or a member of the group to take ownership of the file. An **administrator** can also take ownership of a folder or file, regardless of assigned permissions and then grant another user or group the take ownership permission. Therefore the administrator must first take ownership of the files before he or she can transfer that ownership to another user.

Q. 2
You are the administrator of a Windows 2000 Server computer named ServerA. ServerA has Internet Information Services (IIS) installed and is used to host your company's public Internet web site.

The company is developing a new web site where business partners can exchange information about customer purchases, order history, and credit card information.

You are asked to ensure that all information transmitted between ServerA and each business partner's computers is encrypted. What should you do?

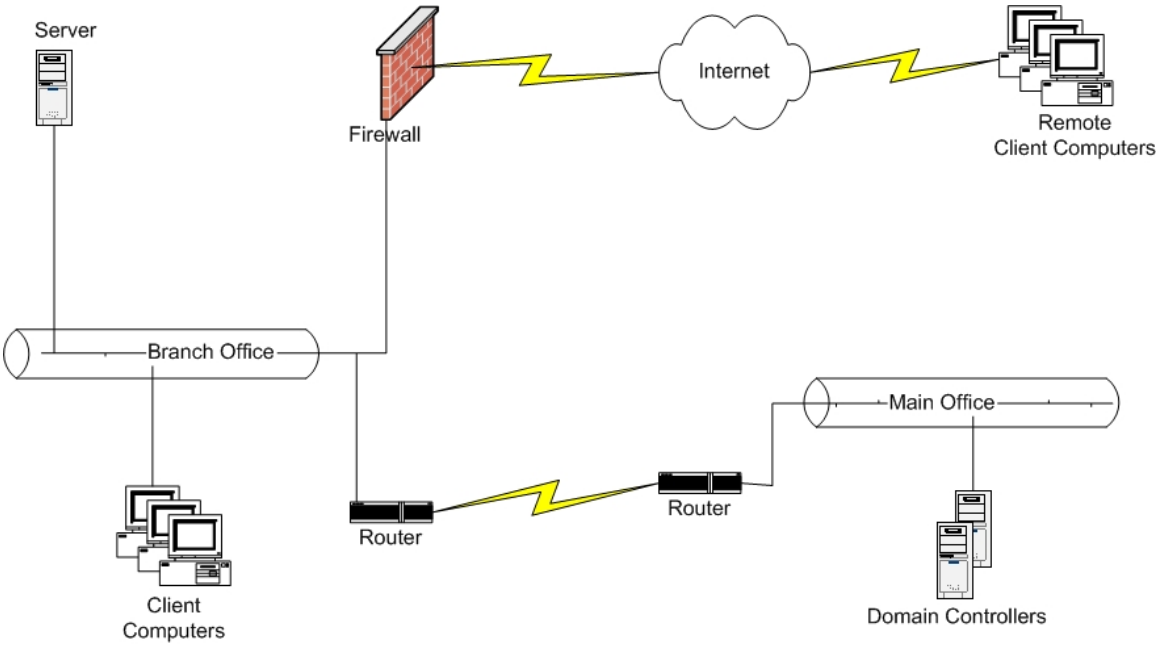
A. Install a Web server certificate and enable Digest authentication.
B. Install a Web server certificate and enable SSL for the new Web site.
C. Configure the new web site to use Integrated Windows authentication.
D. Configure the new Web site folder to enable Encrypting File System (EFS).

Answer: B
Explanation: Secure Sockets Layer (SSL) security protocols are used by most popular Internet browsers and servers to provide authentication, message integrity, and confidentiality. SSL encrypts the content and the data transmitted between a client and a server and relies upon certificates. The certificate-based SSL features in IIS consist of a server certificate, an optional client certificate, and various digital keys.

Note: Certificates are digital identification documents that allow both servers and clients to authenticate each other. Server certificates usually contain information about your company and the organization that issued the certificate.

Incorrect Answers:
A: Digest authentication encrypts client-supplied passwords in compatible browsers (Internet Explorer), but it does not encrypt the content and data.
C: Integrated Windows authentication would not, by itself, secure the connections.
D: Encrypting the Web Site folder on the server would protect the information for anyone gaining access to that folder. However, it would not secure the data when it is sent out from the Web server to the clients. The data would be unencrypted when it leaves the server.

Q. 3
You are a network administrator for your company. The company has 10 branch offices and has plans to add at least 25 more branch offices during the next 12 months. The network is configured as shown in the exhibit.



Each branch office has only one server. These servers are multifunction servers that are domain controllers and application-based Terminal servers. The users of the remote client computers connect to these servers by using Terminal Services over the internet so that they can access a financial application.

You need to ensure that remote users can log on to the Terminal servers and not to any other domain controllers at the main office. You must also ensure that remote users cannot log on to any other domain controller that is not an application-based Terminal Server. When new application-based Terminal servers are added to the domain, you want the servers to automatically configure settings to meet these requirements.

You create a new group named Terminal Server-Users, and you make the user accounts of all the users who need access to these application-based terminal servers members of this group.

What should you do next?

A. Create a new Group Policy Object and link it to the domain level. Configure this GPO by assigning the Terminal-Server-Users group the **Log on locally** right.
B. Create a new Group Policy Object and link it to the domain Controllers Organizational unit (OU). Configure this GPO by assigning the Terminal-Server-Users group the **Log on locally** right.
C. Create a new OU and move all terminal servers into this organizational unit (OU). Create a Group Policy Object and link it to this new OU. Configure this GPO by assigning the Terminal-Server-Users group the **Log on locally** right.
D. Modify the local security policy on all of the application-based Terminal servers by assigning the Terminal-Server-Users group the **Log on locally** right.

E. Modify the Domain Controller security policy on one of the application-based Terminal servers by assigning the Terminal-Server-Users group the **Log on locally** right.

Answer: C
Explanation: In this scenario each branch office has only one multifunctional server that is both a domain controller and an application-based Terminal server. For security purposes we must ensure that the remote users can only log on to the Terminal Server and not to any other server. To accomplish this we must create an OU and place all the Terminal Servers in this OU. We must then create a Group Policy Object that is configured to assign the Terminal-Server-Users group the right to **Log on Locally** and link this to the OU. This way the remote users would only be allowed to log on to the Terminal Servers.

Note: Terminal Server clients use the Terminal Server remotely but need the right to log on locally in order to use it.

Incorrect Answers:
A: A GPO is applied at the level at which it is linked. Therefore, a GPO that is linked to the domain level and that is configured to allow the Terminal-Server-User group log on locally would allow the remote users to log on to any computer in the domain.
B: If we link the GPO to the Domain Controllers OU the remote users would be allowed to log on to any domain controller. We however only want to allow them to be able to log onto the Terminal Servers.
D: Part of the requirements in this scenario is that the configuration of Terminal Servers that are to be added to the domain must be accomplished automatically. However, modifying the local security policy is done on the local computers and we would be required to perform this modification on each additional domain controller. In other words, this solution does not provide for an automatics centralized configuration of the new domain controllers.
E: By modifying the Domain Controller security policy on one of the Terminal Servers, we will allow remote users to log on to only that Terminal Server. The other Terminal Servers and the Terminal Servers that are to be added to the domain would thus not be used. This would thus be an inefficient use of resources and is thus not the best answer.

Q. 4
You are the administrator of a Windows 2000 web server named ServerA. ServerA is a member of a Windows 2000 Domain. A folder on ServerA named I:\\WebData\Public_Information is shared as a virtual directory named Public.

You also want users to be able to access the virtual directory named Public.
You also want users to be able to access the virtual directory by using the URLs http://serverA/PI and http://ServerA/Information.

What should you do?

A. In the Web sharing properties for the folder, add the aliases PI and information.
B. Create two new shares for the folder and name them PI and information.
C. Create two new folders name PI and Information. Copy the files from the existing folder to the new folders. Share each of the new folders with the default settings.
D. Create two new Web sites named PI and Information. Configure I:\\WebData\Public_Information to be the root directory for both web sites.

Answer: A
Explanation: Through the use of Virtual directories we can store Web content in locations other than the default directory. This is done by mapping an alias to the physical location. In this scenario the alias Public is already mapped to the folder I:\\WebData\Public_Information. We just have to add another alias which maps the name PI to the I:\\WebData\Public_Information folder.

Steps to configure a virtual directory (for a folder that already has a virtual directory):

1. Open Windows Explorer and browse to the appropriate folder (here I:\\WebData\Public_Information).
2. Right click on the folder and choose Properties.
3. Select the Web sharing tab.
4. Click the Add button.
5. Enter the first virtual directory name of the alias (here PI) in the Alias field. Click OK.
6. Enter the second virtual directory name of the alias (here information) in the Alias field. Click OK.
7. Click OK.

After this procedure we have three virtual Directory aliases pointing to the same folder.

Reference: HOW TO: Reference Folders Stored on Other Computers from Your Web Site (Q308150).

Incorrect Answers:
B: We can only create one share per folder. We thus cannot create additional shares for the same folder. We should instead create aliases for the two new virtual directories.
C: We do not need to create new folders for the virtual directory as we can map aliases to the new virtual directories.
D: We do not need to create any new Web sites. A virtual directory has already been set up therefore a web site already exists. What we should do is create aliases to point to the same folder.

Q. 5
You are the administrator of a Windows 2000 file and web server named ServerA. ServerA is a member of a Windows 2000 Domain. A folder on ServerA named: I:\Data\Accounting_vacation_requests is shared as AcctVac with default NTFS and share permissions.

Users in the domain local group named AcctGrp save vacation requests as Microsoft Word documents to AcctVac by using a mapped drive.

You want other users in the domain to be able to view the vacation requests by using the URL http://ServerA/Vacation. What should you do?

A. Rename the folder to I:\Data\Vacation. Modify NTFS permissions for the folder to assign the Everyone group the **Allow-Read** permission and to assign the AcctGrp group the **Allow-Full Control** permission.
B. Create a new share named Vacation for the folder. Modify NTFS permissions for the folder to assign the Everyone group the **Allow-Read** permission and to assign the AcctGrp group the **Allow-Full Control** permission.
C. Configure the folder as virtual directory with the alias of Vacation. Assign the **Read** and the **Directory browsing** access permissions for the virtual directory.
D. Create a new Web site named Vacation on ServerA. Create a virtual directory with the default settings in the new Web site.

Answer: C
Explanation: We must set up a Virtual directory to the network share. The Virtual Directory should use the alias Vacation. We also need to configure the appropriate NTFS permission on the folder. Assigning **Read** and **Directory browsing** permissions would allow the users read only access and they would also be able to see contents of the folder.

Steps to configure a virtual directory:

1. Open Windows Explorer and browse to the appropriate folder (in this scenario it would be I:\Data\Accounting_vacation_requests).
2. Right click on the folder and choose Properties.
3. Select the Web sharing tab.
4. Select **Share this folder.**
   Note: by default the Virtual Directory will be put in the Default Web site.
5. Click the Add button.
6. Enter the first virtual directory name of the alias (here Vacation) in the Alias field.
7. Click OK.

We have now created a Virtual Directory in the default Web site.

Reference: HOW TO: Reference Folders Stored on Other Computers from Your Web Site (Q308150).

Incorrect Answers:

A: To allow users in the domain to be able to view the vacation requests by using the URL http://ServerA/Vacation, a Virtual directory must be set up that map the alias 'Vacation' to the actual folder.

B: To allow users in the domain to be able to view the vacation requests by using the URL http://ServerA/Vacation, a Virtual directory must be set up that map the alias 'Vacation' to the actual folder.

D: We do not need to create a Web site to solve this problem as we can configure the folder as a Virtual Directory in the Default Web Site that is mapped to the actual folder and assign appropriate permissions to the Virtual Directory.

Q. 6

You are a network administrator for your company. The network consists of a single Windows 2000 Domain. All servers run Windows 2000 Server. All client computers run Windows 2000 Professional.

The manager of the accounting department reports that files located in shared folders on a server named ServerA are being deleted and must continually be restored from backup.

You are asked to configure the local security policy on ServerA to find out who is deleting the files. You enable auditing on the affected files and folders for all users in the domain.

Which audit policy or security policy should you enable on ServerA?

A. **Audit Access of Global System Objects** security policy.
B. **Account Logon Events-Success** audit policy.
C. **Logon Events-Success** audit policy.
D. **Object Access-Success** audit policy.
E. **Privilege Use-Success** audit policy.

Answer: D

Explanation: By auditing Object Access we will be able to track user access to network objects. These include access to files, folders, and printers. Furthermore, we want to track the user or users that are deleting the shared files. As the user or users are able to delete the files, they are gaining access to the shared files and folders. We should therefore audit for success since we want to find out who is successfully deleting the files.

Incorrect Answers:

A: In this scenario we must use an audit policy, not a security policy, as we want to audit events.

B: When we audit **Account Logon Events**, Windows 2000 logs or records information when a domain controller received a request to validate a user account. However, in this scenario we want to audit files that are being deleted. As files are network objects, we should audit Object Access instead.

C: When we audit **Logon Events**, Windows 2000 logs or records information related to when a user logs on or logs off the domain. In this scenario, however, we are not interested in this kind of information. Instead we are interested in information pertaining to the deleting of shared files. As files are network objects, we should audit Object Access.

E: When we audit **Privilege Use**, Windows 2000 logs or records information related to the use of privilege a right. We are however not interested in this type of information. Furthermore, the deleting files is not a privileged right. It is an object access event. We should therefore audit Object Access.

Q. 7

You are the desktop administrator for your company. The client computers you administer are either Windows 95 or Windows 98 desktop computers. The network consists of a single Windows 2000 Active Directory domain.

The company is implementing a fault-tolerant distributed file system (DFS). You need to ensure that users on all of your client computers can access the resources on the fault-tolerant distributed file system.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Install the Active Directory client on all of the Windows 95 computers.
B. Install the standard DFS client on all of the Windows 95 computers.
C. Install the Windows 2000 Administration Pack on all of the Windows 95 computers.
D. Install the Active Directory client on all of the Windows 98 computers.
E. Install the standard DFS client on all of the Windows 98 computers.
F. Install the Windows 2000 Administration Pack on all of the Windows 98 computers.

Answer: A, D

Explanation: The Active Directory client for Windows 95, Windows 98 and Windows NT 4.0 includes a Dfs component. This component is the Dfs fault tolerance client which provides access to Windows 2000 distributed file system (Dfs) fault tolerant and fail-over file shares specified in Active Directory.

Note: In order for Windows 95 clients to access Domain Based DFS folders the client for Dfs 4.x and 5.0 add-on can be installed. In order for Windows 98 clients to access Domain Based DFS folders client for Dfs 5.0 add-on must be installed.

Reference: How to Install Distributed File System (Dfs) on Windows 2000 (Q241452).

Incorrect Answers:

B: The standard DFS client, Dfs 4.x and 5.0 add-on, would allow Windows 95 clients to accesss Dfs shares on the network. However, they would not be able to access fault-tolerant Dfs shares since they are included in the Active Directory and Windows 95 isn't Active Directory aware.

C: The Windows 2000 administration pack allows Windows 2000 to be administered from downlevel clients such as Windows 95. It wouldn't, however allow the clients to use DFS.

E: The standard DFS client, Dfs 5.0 add-on, would all Windows 98 clients to access Dfs shares on the network. However, they would not be able to access fault-tolerant DFS shares since they are included in the Active Directory and Windows 98 isn't Active Directory aware.

F: The Windows 2000 administration pack allows Windows 2000 to be administered from downlevel clients such as Windows 98. It wouldn't, however allow the clients to use Dfs.

Q. 8

You are a domain administrator for your company. The network consists of a single Windows 2000 Domain. All client computers run Windows 2000 Professional.

Each department has its own Organizational Unit (OU) structure. Each department has departmental administrators who are responsible for the administration of the OU structure. Top-level departmental OUs are created by the domain administrators, and the departmental administrators are delegated full control of these OUs. Child OUs are created by the departmental administrators as necessary.

The departmental administrator for the finance department is out of the office. The manager of the finance department asks you to publish a shared folder named FinanceDocs on a server named ServerA to Active Directory so that users can easily find the folder.

When you attempt to create the shared folder in the Finance OU, you receive the following error message:

You need to publish the shared folder. What should you do?

A. Assign the Domain Admins group the **Allow-Full Control** share permission for FinanceDocs.
B. Assign the Domain Admins group the **Allow-Read & Executive** NTFS permission for FinanceDocs.
C. Assign the Domain Admins group the **Allow-Create Child Objects** permission for Finance OU.
D. Assign the Domain Admins group the **Allow-Modify Owner** share permission for Finance OU and then take ownership.

Answer: C

Explanation: The exhibit in this scenario indicates that there is an access problem on the Finance OU, not an NTFS problem. You must be given access to the OU in order for you to be able to publish the folder. The Permission **Create Child Objects** would allow you to publish the share in the OU.

Incorrect Answers:
A: This is not an NTFS permission problem. You must be given access to the Finance OU.
B: This is not an NTFS permission problem. You must be given access to the Finance OU.
D: The Modify Owner permission allows the current owner, or any user with the Full Control permission, to give another user the right to take ownership of the object. You wouldn't be able to use this permission since you are not the owner of the OU and you don't have Full Access (we know this from the exhibit).

Q. 9
You are a network administrator for your company. The network contains 200 Windows 2000 Professional computers.

One of the client computers is named Client1. Client1 contains a shared folder named Public that is configured with the default settings. The employee who uses Client1 wants all users on the network to map a persistent drive to Public. However, many users report that they cannot map a persistent drive to Public.

What should you do to resolve the problem?

A. Enable the Guest account on Client1.
B. Modify the user limit for Public to allow 200 or more users.
C. Relocate the share and the folder to a Windows 2000 Server computer.
D. Assign the Authenticated Users group the **Allow-Full Control** permission for Public.

Answer: C
Explanation: The problem in this scenario is related to the maximum number of concurrent connections that are supported to resources on a Windows 2000 Professional computer. In this scenario these connections are made via persistent drive mapping. However, the maximum number of concurrent connections to a shared resource on a Windows 2000 Professional computer is 10. If more connections are requires, as is the case in this scenario where up to 200 users could connect simultaneously to the share resource, the share resource must reside on a Windows 2000 server which does not limit the number of concurrent connections.

Incorrect Answers:
A: The guest account is a built-in user account that is installed and enabled by default during the installation of Windows 2000. The problem in this scenario is related to the maximum number of concurrent connections that are supported to resources on a Windows 2000 Professional computer. In

this scenario these connections are made via persistent drive mapping. However, the maximum number of concurrent connections to a shared resource on a Windows 2000 Professional computer is 10 and not 200 as is required in this scenario.

B: The maximum number of concurrent connections to a share on a Windows 2000 Professional computer is 10. This maximum number cannot be set higher than 10. We therefore cannot set it to 200 users as 200 users cannot be simultaneously connected to a share on a Windows 2000 Professional computer.

D: the problem in this scenario is not related to folder permissions. Users can connect to the share as long as no more than 10 users connect at a time.

Q. 10

You are a domain administrator for your company. You are installing a new Windows 2000 Server computer named ServerA, which has Internet Information Services (IIS) installed.

You want to use ServerA to provide a corporate intrasite to your employees. You create a Web site on ServerA.

You want to enable users to access the intrasite by using the URL http://CLInfo. You want to accomplish this task with the least amount of administrative effort.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Create a DNS entry for CLInfo that specifies the TCP/IP address of ServerA.
B. Create a WINS entry for CLInfo that specifies the TCP/IP address of ServerA.
C. Create a Hosts file entry for CLInfo that specifies the TCP/IP address of ServerA. Then copy the Hosts file to each network computer.
D. Create the CLInfo Web site as virtual directory.
E. Configure hosts headers on ServerA to include CLInfo.

Answer: A, E

Explanation: IIS allows us to assign any number of sites to a single IP address and distinguish them by using host headers. First we must add the hosts headers name CLInfo using the IIS console. We configure it for the created Web site. Then we must register the host header name with the appropriate name resolution system. This is a Windows 2000 Domain so there must be a DNS server. So we should create an A (host) record mapping CLInfo to the TCP/IP address of ServerA (E).

Note: Each Web site has a unique, three-part identity it uses to receive and to respond to requests: a port number, an IP address, and a host header name.

Reference:

HOW TO: Use Host Header Names to Configure Multiple Web Sites on a Single IP Address in Windows 2000 (Q308163)
HOW TO: Use Host Header Names to Host Multiple Sites from One IP Address in IIS 5.0 (Q190008)

Incorrect Answers:

B: We could create WINS entries to solve this problem but this would require the presence of a WIN server. However, there is no WINS server present in this scenario. We therefore cannot solve the problem by creating a WINS entry for CLInfo that specifies the TCP/IP address of ServerA.

C: Copying a Hosts file to every computer would require an extensive amount of administrative effort. In this scenario this is not necessary as we could use a DNS server to automate this name resolution process. Furthermore, Hosts file is only used in special circumstances these days.

D: A Virtual Directory allows us to store Web content in locations other than the default directory. This is done by mapping an alias to the default directory's physical location. However, in this scenario CLInfo is the physical Web site. We therefore do not need to create an alias to the Web site.

Q. 11

You are the administrator of a Windows 2000 Server computer named ServerA. ServerA has Internet Information services (IIS) installed and is used to host your company's public internet web site.

The company plans to create a secure web site where customers can access their account and billing information. Customers will access this web site by using a variety of web browsers. A new web site has been created and configured to use Basic authentication.

You are asked to ensure that all information transmitted between ServerA and the customers' computers is encrypted. How should you configure the new web site?

A. Enable the web site to use Integrated Windows Authentication.
B. Enable the web site to use Digest authentication for Windows domain servers.
C. Enable the web site to use a web server certificate and enable SSL for the web site.
D. Enable the web site to use a web server certificate and enable IPSec on ServerA.

Answer: C

Explanation: Secure Sockets Layer (SSL) encrypts the content and the data that is being transmitted. Most popular browsers have built-in SSL support. Certificates are required for the server and client's browser to set up an SSL connection over which encrypted information can be sent. The certificate-based SSL features in IIS consist of a server certificate, an optional client certificate, and various digital keys.

Note: Certificates are digital identification documents that allow both servers and clients to authenticate each other. Server certificates usually contain information about your company and the organization that issued the certificate.

Incorrect Answers:

A: Integrated Windows authentication would not, by itself, secure the connections. It would only prevent access to anonymous users and would only authenticate and provide access to users who have valid domain user accounts. This would thus provide for the authenticity of the clients that access the server but would not provide for the encryption of the data that is transmitted between the client and the server.

B: Digest authentication encrypts client-supplied passwords in compatible browsers (Internet Explorer), but it does not encrypt the content and data that is transmitted between the client and the server.

D: To be able to use IPSec both the server and the clients must be enabled for IPSec. We however do not have control over the client computers as they belong to the customers. We therefore cannot ensure that IPSec is enabled on the client computers and therefore cannot implement IPSec.

Q. 12

You are the administrator of your company's file servers. An employee named Maria is promoted to the new position of manager in the marketing department. Maria needs to be able to review all the documents that are used by other employees in the marketing department. However, she does not need to make changes to these documents.

All the marketing documents are stored in subfolders in a single marketing folder, which is shared as Marketing. Each employee in the marketing department has a subfolder in the Marketing folder. Currently, only the employee, the Administrators group, and the Power Users group have permissions for each employee's subfolder. Permissions inheritance is enabled on the Marketing folder. The resources and permissions are shown in the following table.

Resource	Type of permission	Effective permission
Marketing share	Share	Everyone-Full Control
Marketing folder	NTFS	Administrators-Full Control Power Users-Modify
Peter's folder	NTFS	Peter-Modify Administrators-Full Control Power Users-Modify
Andrea's folder	NTFS	Andrea-Modify Administrators-Full Control Power Users-Modify
Marc's folder	NTFS	Marc-Modify Administrators-Full Control Power Users-Modify

You need to allow Maria to review the documents of all of the other marketing employees without giving her unnecessary permissions. What should you do?

A. Make Maria a member of the Power Users group.
B. Share each existing subfolder and assign Maria the **Allow-Read** permission for each of the new shares.
C. Assign Maria the **Allow-Read** NTFS permission for the Marketing folder.
D. Assign Maria the **Allow-Read** permission for the Marketing share.

Answer: C
Explanation: We need to allow read access for Maria. She must be able to read the files but must not be able to change them. She already has full Share permission to the Marketing share. We must give Maria NTFS permissions as well as her effective permission is a combination of the sum of her Share Permissions and a sum of her NTFS permissions. By giving Maria NTFS Read Permission on share her permission on the folders would be read as her effective permission is the most restrictive of her accumulative Share permissions and her accumulative NTFS permissions.

Note: To calculate a user's effective permission on a share:

1. Calculate the NTFS permissions. They are accumulative except for DENY that overrides all permissions.
2. Calculate the Share permission. They are accumulative.
3. Combine the calculated NTFS and Share permissions. The result is the most restrictive permission.

Incorrect Answers:
A: Adding Maria to the Power Users group would give her modify permission (NTFS: modify + Share: Full = Modify) on the all the file and folders on the share. This would provide her with more permissions than is the required.
B: By creating shares for each subfolder and give Maria the read share permission would not give Maria access to the files, since she does not have any NTFS permissions (NTFS: none + Share: read = none).
D: Giving Maria Read permissions on the share would not give Maria any more rights since she already has Full Control Share permission as a member of the Everyone group. Maria would have no permission to the folders (NTFS:none + Share:Full = none).

Q. 13
You are the administrator of a Windows 2000 file server named ServerA. ServerA is a member of a Windows 2000 Domain. On a volume that is formatted as NTFS, you create and share folders for the sales department. Managers in the sales department need to read and modify files in all of the department's folders. Users named Peter, Maria, and Marc need to read files in the G:\Sales\Reports folder, and they need full control of files in their personal folders.

You configure folder and share permissions as shown in the following table.

Folder	Share name	Share permission	NTFS permission for folders and files
G:\Sales	**Sales**	**Mangers-Full Control**	**Managers-Full control**
G:\Sales\Reports	**Reports**	**Everyone-Read**	**Managers-Full control Everyone-Read**
G:\Sales\Reports\Peter	**Peter$**	**Peter-Full Control**	**Managers-Full control Peter-Full Control**
G:\Sales\Reports\Maria	**Maria$**	**Maria-Full Control**	**Managers-Full control Maria-Full Control**
G:\Sales\Reports\Marc	**Marc$**	**Marc-Full Control**	**Managers-Full control Marc-Full Control**

A user in the Managers group informs you that she can read the files in Marc's folder but cannot update them.

You need to allow all users in the Managers group to update all of the files in the sales department's folder. What should you do?

A. Instruct the users in the Managers group to access the files by using the Sales share.
B. Assign the Managers group the **Allow-Full Control** permission for the Marc$ share.
C. Re-create the Marc$ share as Marc.
D. Ensure that the Managers group has the **Allow-Full Control** permission for the published share object in Active Directory that is associated with the Sales share.

Answer: A
Explanation: The Managers has full Share Permissions on the Sales share and full NTFS permissions the Sales folders and all its subfolders. The combined permission is also full permission (Share:Full + NTFS:Full=Full).

Note: The calculation of effective permission on a share can be done by:

1. Calculate the NTFS permissions. They are accumulative except for DENY that overrides all permissions.
2. Calculate the Share permission. They are accumulative.
3. Combine the calculated NTFS and Share permissions. The result is the most restrictive permission.

Incorrect Answers:

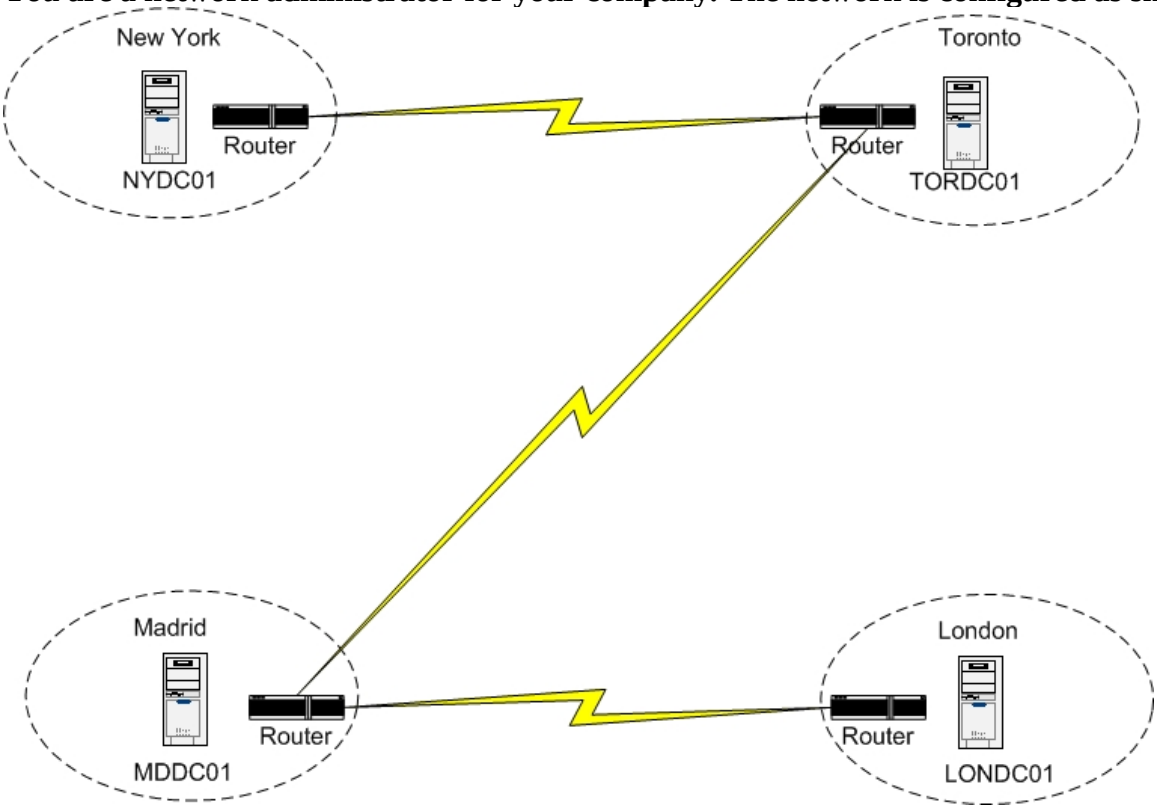
B: Assigning Full Control permission to the Managers group on Marc$ share would solve the problem for this particular share. Managers would still be denied access if they connected to the Maria$ or the Peter$ share though.

C: A share that ends with a $ sign is a hidden share, which means it cannot be seen while browsing the network. A hidden share uses the Share permissions in exactly the same way as a non-hidden share. Recreating the Marc$ share as Marc wouldn't change anything.

D: Access to a share is decided by NTFS and Share permissions, not by permissions assigned in the Active Directory. The Active Directory can be used to publish a share to users to make it more convenient for them to access the share.

Q. 14

You are a network administrator for your company. The network is configured as shown in the exhibit.



You notice that connectivity from the New York office to the London office is inconsistent. You need to find out where the network packets are being dropped and what percentage of packets is being dropped.

What should you do?

A. On NYDC01, run the **tracert LONDCO01** command. View the results and find out where the results time out.
B. On LONDC01, run the **tracert NYDCO01** command. View the results and find out where the results time out.
C. On NYDC01, run the **ping LONDC01** command. View the results.
D. On LONDC01, run the **ping NYDC01** command. View the results.
E. On NYDC01, run the **pathping LONDC01** command. View the results.
F. On TORDC01, run the **pathping LONDC01** command. View the results.

Answer: E
Explanation:

We must troubleshoot the connection from New York to London. We should issue any troubleshooting from source location New York.
The pathping combines features of the ping and tracert commands to identify which routers are on the path. It also provides additional information that neither of those commands provides. It sends pings periodically to all of the routers over a given time period, and computes statistics based on the number returned from each. Since pathping shows the degree of packet loss at any given router or link, you can determine which routers or links might be causing network problems.

Incorrect Answers:
A: Tracert doesn't provide as much useful information as pathping.
B: Tracert doesn't provide as much useful information as pathping.
The command should be issued at New York not at London.
C: The ping command only provides a result of either success or failure (and ping time). It will not provide any information on where the problem is located.
D: The ping command only provides a result of either success or failure (and ping time). It will not provide any information on where the problem is located.
The command should be issued at New York not at London.
F: The command should be issued at New York not at London.

Q. 15
You are a network administrator for Fabrikam, Inc. The network consists of a Windows 2000 Domain named ad.fabrikam.com. The domain contains two DNS servers that host an Active Directory integrated zone for ad.fabrikam.com. A Windows 2000 web server named ServerA is a member of ad.fabrikam.com.

An intranet web site was recently created on ServerA. You want users to access the new Web site by using the URL home.portal.fabrikam.com.

What should you do?

A. Create a new domain record named portal in the ad.fabrikam.com zone. In portal, create CNAME (canonical name) record named home and specify ServerA.ad.fabrikam.com as the target host.
B. On one of the DNS severs, create a new zone named portal.fabrikam.com. In portal.fabrikam.com, create a CNAME (canonical name) record named home and specify ServerA.ad.fabrikam.com as the target host.
C. In ad.fabrikam.com, create CNAME (canonical name) record named home and specify home.portal.fabrikam.com as the target host.
D. In ad.fabrikam.com, create CNAME (canonical name) record named home.portal and specify ServerA.fabrikam.com as the target host.

Answer: B
Explanation: A DNS zone can only provide host to IP resolution within the namespace of the zone. It cannot provide name resolution for host names that are not included in the zone.
In this scenario we have a zone ad.fabrikam.com and we want to use the name home.portal.fabrikam.com as an alias for the resource ServerA.ad.fabrikam.com. We do this by creating a new zone portal.fabrikam.com, add a CNAME (alias) record which maps the host name home (which in the zone equals home.portal.fabrikam.com) to ServerA.ad.fabrikam.com.

Incorrect Answers:
A: Adding a CNAME record portal in the ad.fabrikam.zone with ServerA.ad.fabrikam.com target host would map portal.ad.fabrikam.zone to ServerA.ad.fabrikam.com, but we want to map home.portal.fabrikam.com to ServerA.ad.fabrikam.com.
C: Adding a CNAME record portal in the ad.fabrikam.zone with home.portal.fabrikam.com target host would map portal.ad.fabrikam.zone to home.portal.fabrikam.com. But no source with that name exists.
D: A CNAME record home.portal in the ad.fabrikam.com would map the home.portal.ad.fabrikam.com to the destination host, but we want to map home.portal.fabrikam.com.

Q. 16
You are a network administrator for your company. The network contains a DNS server. All client computers are configured to use the DNS server for name resolution. The network also includes four Windows 2000 Server computers, which function as file and print server; 100 Windows 95 client computers; and 100 Windows 2000 Professional computers

The network is currently configured as a single logical subnet. The company adds two additional subnets, which are connected to the original subnet by routers. All client computers are distributed between the two new subnets. The servers remain on the original subnet.

Users of the Windows 95 computers now report that they cannot access server-based files and printers. Users of the Windows 2000 Professional computers can successfully access the servers. You verify that the Windows 95 computers are configured with the correct DNS server address.

You need to ensure that all users can access server-based files and printers. What should you do?

A. Create an Lmhosts file on each Windows 95 computer. In the file, include the name and IP address of the DNS server.
B. Install WINS on a Windows 2000 Server computer. Configure all computers to use the WINS server in addition to the DNS server for name resolution.
C. Configure the Windows 95 client computers to use b-node for NetBIOS name resolution.
D. Install a WINS Proxy Agent on each of the new subnets. Configure the WINS Proxy Agents to use the DNS server's IP address for WINS name resolution.

Answer: B
Explanation: Downlevel clients, like Windows 95 and Windows NT 4.0, use WINS, not DNS, for name resolution. On the other hand Windows 2000 computers only use DNS for name resolution by default. We must provide the Windows 95 clients with a method of resolving NetBios names to IP addresses. The most practical solution with least administration would be to configure one Windows 2000 server as a WINS server.

Incorrect Answers:
A: Lmhosts files do provide host name to IP address resolution, and an appropriate lmhosts will on each Windows 95 computer would allow the Windows 95 clients to use the DNS server. This would require a lot of administrative effort.
C: By default Windows 95 clients are configured for H-mode Wins resolution; first they use Wins server and then they use broadcasts to resolve NetBios names. Changing the node type to b-node would make the clients only try broadcasts, so this is not an improvement.
Note: there are four Wins Node types. They are:

- B-node, broadcast mode, only tries to resolve NetBios names with broadcasts.
- P-node, peer-peer node, only tries to resolve NetBios names through WINS server.
- M-mode, mixed mode, first use broadcast then in use broadcasts.
- H-mode, hybrid node, is the default Wins node type. H-mode first tries the WINS server then it tries broadcast.

D: WINS Proxy agent is used to enable non-WINS clients to communicate with WINS-clients. Windows 95 is a WINS client so a WINS proxy agent would not be any improvement.
UNIX clients, for example, could benefit from a Wins proxy agent.

Q. 17
You are a domain administrator for your company. The network contains two TCP/IP subnets that are connected by a router. The router is configured to forward BOOTP packets. The two subnets contain a total of 180 Windows 2000 Professional computers.

A Windows 2000 Server computer named ServerA provides DHCP services for the network. The DHCP scope on ServerA is configured as shown in the following table.

Scope	IP address range
172.30.10.0/24	172.30.10.1 to 172.30.10.100
172.30.11.0/24	172.30.11.1 to 172.30.11.100

You are adding a new Windows 2000 Server computer named ServerB. You install the DHCP service on ServerB. You want ServerB to provide load balancing and redundancy for ServerA.

How should you configure DHCP on ServerB?

A. Configure one scope with an IP address range of 172.30.10.1 to 172.30.10.100. Configure a second scope with an IP address range of 172.30.11.1 to 172.30.11.100.
B. Configure one scope with an IP address range of 172.30.10.101 to 172.30.10.200. Configure a second scope with an IP address range of 172.30.11.101 to 172.30.11.200.
C. Configure one scope with an IP address range of 172.30.10.1 to 172.30.10.200. Configure an IP address exclusion of 172.30.10.1 to 172.30.10.100.
D. Configure one scope with an IP address range of 172.30.11.1 to 172.30.11.200. Configure an IP address exclusion of 172.30.11.1 to 172.30.11.100.

Answer: B
Explanation: For redundancy, two (or more) DHCP servers must split the DHCP scope into two non-overlapping IP address ranges. Typically they are split with the 75/25 rule (or 80/20 etc.) that specifies that the local DHCP server will use 75% of the DHCP scope and the remote DHCP server will use 25% of the DHCP scope. The other scope is split in the same fashion: the local DHCP server use 75% of the scope and the remote DHCP server use 25% of the scope. This provides redundancy and load balancing as required.

In this scenario the solution would use a 50% split. This is not the optimal solution but it would provide redundancy and load balancing.

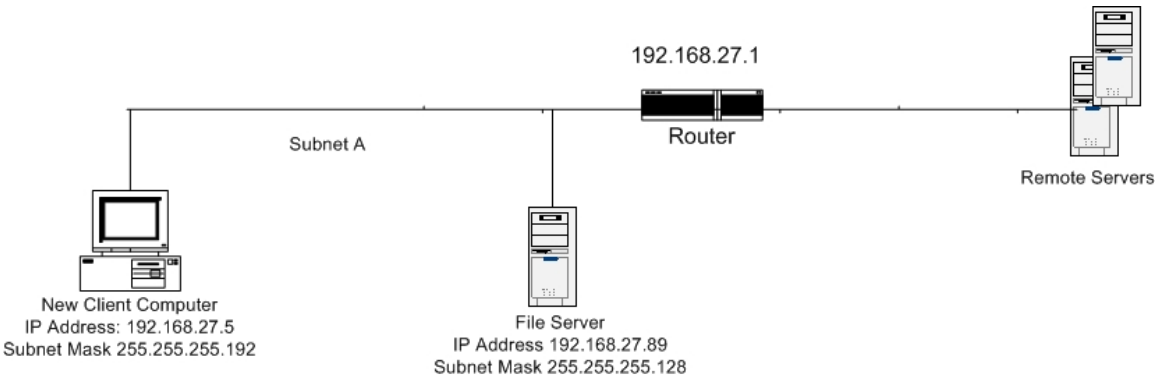
Incorrect Answers:
A: Two DHCP servers leasing IP addresses in the same range must not have overlapping scopes. Server a already uses the 172.30.10.1 to 172.30.10.100 range so ServerB cannot lease IP addresses in this range.
C: Redundancy and load balancing must be provided for both scopes. ServerB must be configured to lease address in the 172.30.11.0/24 scope as well.

D: Redundancy and load balancing must be provided for both scopes. ServerB must be configured to lease address in the 172.30.10.0/24 scope as well.

Q. 18
You are a network administrator for your company. The network uses static IP addresses on servers and client computers.

You add a new client computer to subnet A of the network. Your router administrator informs you that the new client computer is incorrectly configured.

The relevant portion of the network is shown in the exhibit.



You need to configure the client computer so that it can connect to all local and remote computers. What should you do?

A. Modify the IP address of the client computer so it is the same as the IP address of the file server.
B. Modify the IP address of the client computer so it is the same as the IP address of the router.
C. Modify the subnet mask of the client computer so it is the same as the subnet mask of the file server.
D. Modify the subnet mask of the file server so it is the same as the subnet mask of the client computer.

Answer: C
Explanation: In order to be able to communicate with other computers using the TCP/IP protocol a computer must have a unique address and an appropriate subnet mask. The new client must be given an IP address in the same subnet as the other clients on subnet. By studying the exhibit we see that this is the case. The subnet mask of the new client is not correct however. It must be configured with the same subnet mask as the file server.

Note: In order for the new client to connect to the remote servers the default gateway setting must be set to the IP address of the Router.

Incorrect Answers:

A: All computers using the TCP/IP protocol must use a unique IP address. The new client cannot be configured with the same IP address as the File server.

B: All computers using the TCP/IP protocol must use a unique IP address. The new client cannot be configured with the same IP address as the router.

D: Changing the subnet mask of the file server to the same subnet mask as the new client would allow these two computers to communicate. However, they would not be able to communicate with other computers on the local subnet or with clients on the remote subnet.

Q. 19

You are a network administrator for your company. The network contains Windows 2000 Professional computers and Windows 2000 Server computers. A server named ServerA provides DNS, WINS, and DHCP services. DHCP is configured to issue ServerA's IP address for DNS and WINS name resolution. ServerA's DNS zone is configured to use DNS dynamic update protocol. All other computers on the network are configured to use DHCP to obtain IP addressing information.

Your company purchases another company and relocates the new employees to your company's main office. The new employees use Windows 98 client computers that are configured to use static IP addresses.

You need to ensure that the Windows 98 computers obtain dynamic IP addresses, and that they register themselves with ServerA by using DNS dynamic update protocol. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Configure the Windows 98 client computers to use ServerA for DNS name resolution.
B. Configure the Windows 98 client computers to use ServerA for WINS name resolution.
C. Configure the Windows 98 client computers to use DHCP to obtain IP addressing information.
D. Configure the DNS server service on ServerA to perform lookups by using WINS.
E. Configure the DHCP service on ServerA to register clients by using DNS dynamic update protocol.

Answer: C, E

Explanation: We have downlevel Windows 98 clients that are not able to use DNS as the only way to resolve host names. However by integrating WINS and DNS they would be able to use host names to connect resources.

C: The Windows 98 clients are configured with static IP address configuration. We must change this configuration so that the clients use DHCP to obtain addressing information.

E: The downlevel Windows 98 clients don't handle the dynamic registration in DNS the same way as the Windows 2000 clients. In order to allow them to register dynamically we must:

1. Enable the DNS zone to allow dynamic updates. This has already been done in this scenario.

2. Configure the DHCP server to **Enable updates for DNS clients that do not support dynamic updates.** This setting is disabled by default and must be enabled to allow the Windows 98 clients to be registered in DNS dynamically.

Note: In a network with only Windows 2000 computers WINS would not be required.

Incorrect Answers:

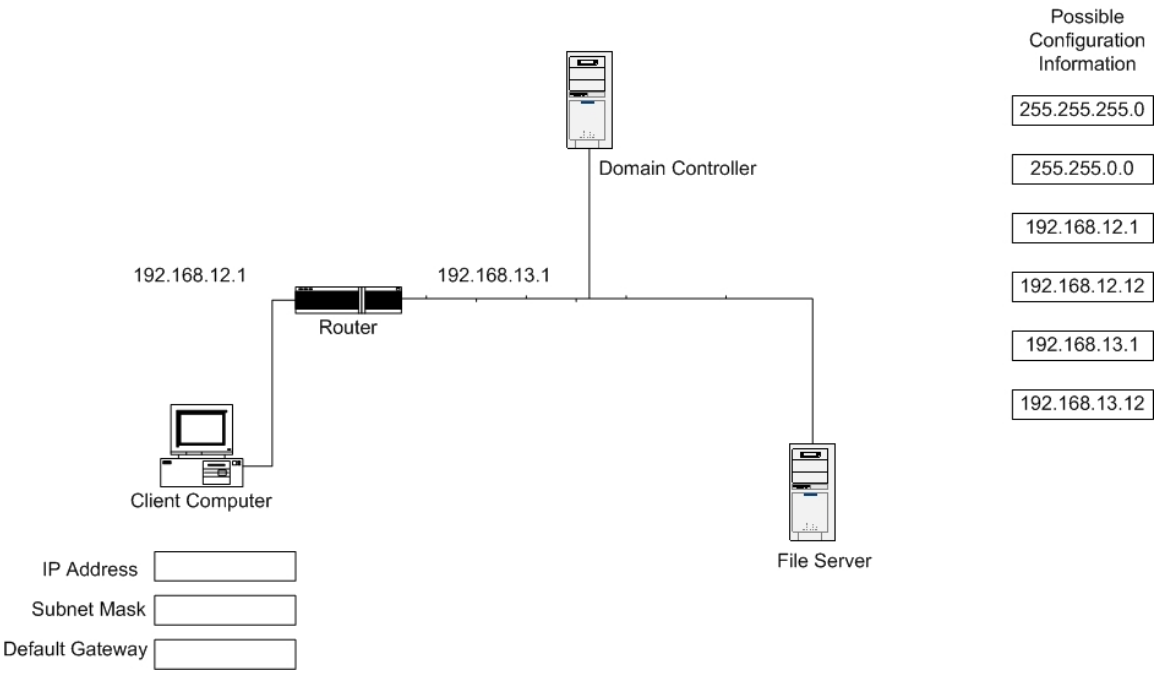
A: Name resolution is not required in this scenario. We only want to be able to register the Windows 98 clients dynamically in the DNS zone.

B: Windows 98 computers are configured to be WINS clients by default. They do not have to be configured to be able to use the WINS server.

D: Integrating WINS and DNS is a good idea and would provide name resolution for the downlevel Windows 98 clients. However, the scenario only requires us to setup up dynamic registrations of the Windows 98 clients in DNS. Integrating DNS and WINS will not accomplish this.

Q. 20

You are the network administrator for one of your company's branch offices. The network is your office consists of two subnets. One subnet contains client computers and one subnet contains servers. You are using standard, classful subnet mask on the subnets. The relevant portion of the network is shown in the exhibit.



You need to configure the client computer so that it can connect to the file server and the domain controller on the network. How should you configure the computer?

To answer click the select and place button, and then drag the appropriate configuration information to the client computer

Select And Place

Answer:
IP address: 192.168.12.12
Subnet mask: 255.255.255.0
Default gateway: 192.168.12.1

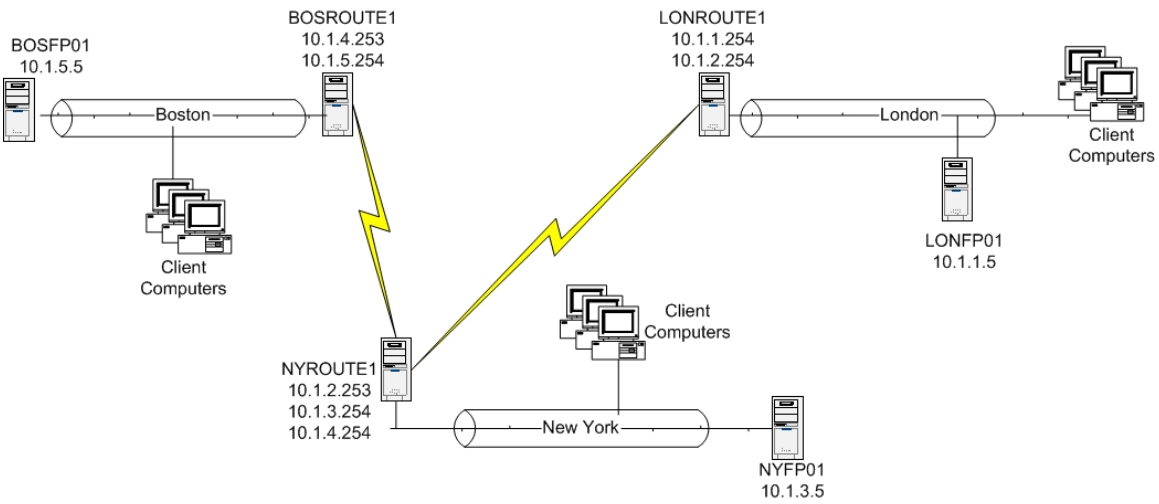
Explanation:
Subnet mask: A classful subnet mask uses a subnet mask in one of the address classes A, B, or C. The IP address of the local interface of the Router is 192.168.12.1. This IP address belongs to a Class C network. Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet.

IP address: The IP address must be included in the same subnet as the local IP address of the router (192.168.12.1) so it must have the pattern 192.168.12.xx (the subnet mask is 255.255.255.0). The only available choice is 192.168.12.12 since we cannot choose the same address as the router.

Default gateway: The default gateway must be set to the IP address of the local router interface which is 192.168.12.1.

Incorrect Answers:
The subnet mask 255.255.0.0 is used for Class B networks. The first octet of an IP address in a class B network must be in the 128-191 range.
The IP address 192.168.12.1 cannot be used since all computers must have a unique IP address and the router is already using the 192.168.12.1 address.
The IP addresses 192.168.13.1 and 192.168.13.12 cannot be used since they belong to another subnet than the router.

Q. 21
You are a network administrator for your company. The network is configured as shown in the exhibit.



Users in the London office report that they cannot connect to BOSFP01. You run the ping 10.1.4.253 command on NYROUTE1 and receive a reply. You run the tracert command on a client computer in the London office. The results are shown in the Tracert exhibit.

Tracert

```
Tracing route to 10.1.5.5 over a maximum of 30 hops

1  <10ms  <10ms  <10ms  LONROUTE1 [10.1.1.254]
2  <10ms  <10ms  <10ms  NYROUTE1 [10.1.2.253]
3    *      *      *    Request timed out
4    *      *      *    Request timed out
```

You need to ensure that users in the London office can connect to BOSFP01. What should you do?

A. On all client computers in the London office, run the following command:
route add 10.1.5.0 mask 255.255.255.0 10.1.1.254 -p

B. On NYROUTE1, run the following command:
route add 10.1.5.0 mask 255.255.255.0 10.1.4.253 -p

C. On LONROUTE1, run the following command:
route add 10.1.5.0 mask 255.255.255.0 10.1.2.253 -p

D. On BOSROUTE1, run the following command:
route add 10.1.1.0 mask 255.255.255.0 10.1.5.254 -p

Answer: B

Explanation: The Tracing route exhibit shows LONROUTE1 is trying to use NYROUTE1 to reach BOSROUTE1. Put the trace go no further than NYROUTE1. It is clear that routing stops at NYROUTE1. One possible solution is to add a static route on NYROUTE with the target of BOSROUTE1.
Note that the ping from NYROUTE1 to BOSROUTE1 only shows that BOSROUTE1 is up and running, not that the routing table on NYROUTE1 is correct.

Note: The route command with the –p switch adds a persistent route to the routing table.
Syntax: route -p add [network] mask [netmask] [gateway]

Incorrect Answers:
A: The problem is at NYROUT1 at the New York office, not at the London office.
C: The problem is the routing table on NYROUT1 at the New York office, not at LONROUTE1 at the London office.
D: We most configure the source location, not the destination location BOSROUTE1 which is unreachable.

Q. 22
You are a domain administrator for your company. The network contains 75 Windows 2000 Server computers and 1,000 Windows 2000 Professional computers. The network also contains 50 UNIX client computers. The UNIX computers run applications with hard-coded IP addresses for each of the servers.

One of the servers is configured to provide DHCP services for the network. All of the Windows 2000 computers are configured to use DHCP.

Users of the UNIX client computers reports that on some days that cannot connect to various servers.

You want to ensure that users of the UNIX client computers can successfully connect to the servers. What should you do?

A. Create a DHCP client reservation for each UNIX client computer.
B. Create a DHCP client reservation for each server.
C. Create a DHCP scope for the servers that specifies a six-month lease time-out.
D. Create a DHCP scope for the servers that includes a vendor option for the UNIX client computers.

Answer: B
Explanation: The UNIX computers are not always able to connect to the servers. We must make sure that the servers always use the same IP address in order for the UNIX application to be able to reach the servers. We do this by creating a DHCP client reservation for each of these servers.

Note: A good solution, not listed here, would be to use static addresses on the servers.

Incorrect Answers:

A: Creating client reservations for the UNIX client computers would ensure that these clients would use the same IP address. But the problem is the hardcoded IP addresses of the Servers. The servers, not the UNIX clients, must have client reservation in DHCP.

C: Create a separate DHCP scope for the servers would require a lot of administrative effort. A six-month lease time would not solve the problem; only make it happen more seldom.

D: The servers, not the clients, must use the same IP addresses.

Q. 23

You are the server and network administrator for a computer lab. The computer lab contains two multiple-subnet networks that do not have routing between them. The computer lab also contains a multihomed Windows 2000 Server computer that provides the DNS server service for both networks. Each network also contains a DHCP server.

The initial network adapter configuration of the DNS server is shown in the following table:

Adapter name	IP address	Subnet mask	DHCP enabled
LAN1	10.10.5.1	255.255.255.0	No
LAN2	10.10.6.1	255.255.255.0	Yes

At any given time, the client computers in the computer lab might be running Windows 2000 Professional, Windows NT workstation 4.0, or a third-party operating system. All of the DNS clients in the computer lab receive their IP configurations from DHCP servers. After functioning successfully for several months, the DNS clients on the 10.10.6.0/24 network can no longer resolve host names.

You want all computers in the computer lab to be able to resolve DNS names. What should you do?

A. Configure the DHCP servers to dynamically update DNS for DHCP clients.
B. Configure the DNS server service to listen only on LAN1.
C. Enable DHCP on LAN1.
D. Manually configure the IP address for LAN2 as 10.10.6.1.

Answer: D

Explanation: The DNS name resolution on LAN2 stopped working. The most probable cause is that the IP address on the LAN2 interface has changed.

The LAN2 interface is DHCP enabled, which means that it assigned DHCP configuration settings dynamically from the DHCP Server on LAN2. It would be better to use a static IP address on LAN2 in order to avoid any changes of the IP address on the LAN2 interface.

Incorrect Answers:

A: DNS has been working flawlessly for a while. There should be no reason to reconfigure the DNS server.
B: The LAN2 clients must have access to the DNS server as well.
C: Enabling dynamic IP configuration, DHCP, on LAN1 would only make matters worse. LAN2 could eventually be hit by same problem as LAN1, if the IP address of the LAN1 interface would change.

Q. 24
You are a network administrator for your company. The network consists of a single Active Directory domain. The network contains one Windows 2000 Server computer, which runs the DNS server service, and 200 Windows 2000 Professional computers. All of the Windows 2000 Professional computers use DHCP to obtain IP addressing information. The network is connected to the internet through an internet service provider.

On Monday, the ISP informs you that its network will be unavailable on Tuesday evening because of maintenance and changes. On Wednesday morning, all of your company's network uses report that they cannot access internet web sites. When they attempt to access internet web sites, they receive the following error messages; "Server not found or DNS error." Users can successfully log on to the domain and access resources on the company's network, including the intranet web site.

You contact the ISP and are informed that it has changed the IP address of its primary DNS server. The ISP informs you that the new IP address is 192.168.167.100. You need to reconfigure your company's network so that users can access internet web site.

What should you do?

A. Configure your company's DHCP server to configure client computers to use 192.168.167.100 for DNS name resolution.
B. Configure your company's DNS server to forward requests to 192.168.167.100
C. Configure your company's Windows 2000 Professional computers to use 192.168.167.100 for DNS name resolution.
D. Configure your company's DNS server to use 192.168.167.100 for DNS name resolution.

Answer: B
Explanation: The local DNS server must be configured to forward name resolution requests to the DNS server of the ISP. Then the clients would be able to access both local and external resources such as the internet web sites.

Incorrect Answers:
A: The clients must still use the local DNS server for name resolution on the local network. If the clients would be configured to use the DNS Server at the ISP for name resolution they would, theoretically, be able to access the internet web site but they wouldn't be able to access local resources.

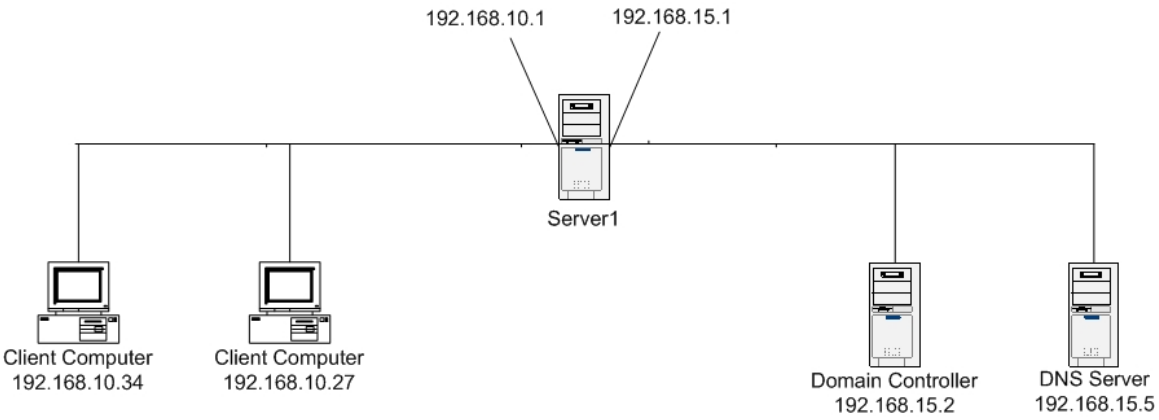
C: The clients must still use the local DNS server for name resolution on the local network. If the clients would be configured to use the DNS Server at the ISP for name resolution they would, theoretically, be able to access the internet web site but they wouldn't be able to access local resources.
It would require a lot administration to configure each client manually.

D: The DNS server must configured to forward requests to external DNS server, but it must still provide the local name resolution itself.

Q. 25

You are a network administrator for your company. Until recently, the network consisted of one subnet. However, because of recent growth, all of the company's servers, the domain controller, and the DNS server are now on a second subnet.

A server named Server1 separates the two subnets. Server1 has two network interfaces. Because of the addition of the new subnet you configure all servers and client computers with appropriate new IP addresses, class C subnet masks, and default gateway addresses. The relevant portion of the network is shown in the exhibit.



You test the configuration from one of the client computers. You can ping other client computers and the nearside interface of Server1. However, you cannot ping any of the other servers by IP addresses or host name.

You need to ensure that the client computers can connect to all of the servers. What should you do?

A. Change the subnet mask on all computers to 255.255.255.128.
B. Enable IP routing on Server1.
C. Configure a DNS server address on each client computer and on each server.
D. Configure the IP addresses to be the same on both interfaces on Server1.

Answer: B
Explanation: In order for the computers on the different subnets to be able to communicate, communication must be routed between the subnets. You can use a Windows 2000 server as a software router simply by enabling routing on it.

This is not a name resolution problem since pinging the IP addresses doesn't work.

Incorrect Answers:
A: All computers have already been configured with appropriate Class C subnet mask (255.255.255.0). There is no need to change the subnet mask.
C: This is not a name resolution problem since pinging with IP addresses doesn't work. No data would be passed between the subnets until routing is enabled on the server.
D: All network devices, including LAN interface, must use unique IP addresses. We cannot use the same IP address on the different interfaces.

Q. 26
You are a network administrator for your company. The network consists of a single Windows 2000 Domain. The domain contains Windows 2000 Server computers, Windows 2000 Professional computers, and Windows NT workstation 4.0 computers. You administer two Windows 2000 DNS servers, two Windows 2000 WINS servers, and two Windows 2000 DHCP servers.

All of the servers have static IP addresses and all of the client computers are DHCP clients. All servers and client computers are configured as WINS clients.

You want all client computers in the domain to be dynamically registered in DNS. What should you do?

A. For all computers in the domain, manually configure DNS parameters and run the **ipconfig/registerdns** command.
B. Configure an Active Directory integrated zone for the domain.
C. Configure the DHCP servers to register DHCP clients in DNS.
D. Configure the DNS zone for the domain to use WINS forward lookup, and ensure that the **Do not replicate this record** check box is cleared.

Answer: C
Explanation: We must enable dynamic registrations of all client computers in the domain. This can be done by configuring the DHCP server to automatically update client information in DNS both for Windows 2000 clients and for downlevel clients.

Steps:

1. Open the DHCP console.
2. Right-click on the DHCP server and choose **Properties**.
3. Select the DNS tab.
4. Select **Automatically update DHCP client information in DNS.**
   This allows the DHCP server to register Windows 2000 computers in the DNS zone.
5. Select **Enable updates for DNS clients that do not support dynamic updates**.
   This allows the DHCP server to register downlevel clients like Windows NT 4.0 in the DNS zone.
6. Click OK.

Incorrect Answers:

A: The ipconfig/registerdns command is used to manually force a refresh of the client name registration in DNS. This is a manual update not a dynamic update as was required.

B: An Active Directory Integrated zone is not required for dynamically registration of clients in DNS.

D: By configuring the DNS zone to use WINS forward lookup the DNS service would be able to use WINS servers to look up names not found in the DNS domain namespace by checking the NetBIOS namespace managed by WINS.
By clearing the **Do not replicate this record** the would prevent the records retrieved from WINS from being replicated other servers during zone transfers.
Neither of these two settings would enable clients to register dynamically in DNS.

Q. 27

You are a network administrator for your company. You are installing Windows 2000 Advanced Server on a new computer.

The server contains two PCI network adapters and a PCI video adapter. The server's motherboard has a built-in dual-channel SCSI adapter that hosts several devices, as shown in the following table:

SCSI adapter function ID	SCSI adapter device ID	Attached SCSI device	SCSI device ID
0	14	Hard disk	0
0	14	Hard disk	1
0	14	Hard disk	2
0	14	Hard disk	3
1	14	Removable disk cartridge drive	0
1	14	Tape backup device	1
1	14	CD-ROM drive	2

The installation process begins normally. However, prior to copying files, Windows 2000 Setup informs you that it cannot detect any mass storage devices on your computer. The installation will not resume.

You need to correct this problem and complete the installation. What should you do?

A. Reconfigure the second SCSI adapter to have a SCSI device ID of 7.
B. Reconfigure the removable disk cartridge drive to have a SCSI device ID of 4.
C. Reserve an IRQ for each SCSI adapter in the system BIOS.
D. Restart setup and install the driver for the SCSI adapter during the initial file copy.
E. Configure the system BIOS boot device option to boot from the SCSI hard drive.

Answer: D
Explanation: Apparently Windows 2000 doesn't contain an appropriate device driver for the SCSI adapter, instead a device driver must be provided during the installation process. The SCSI device driver must be installed during the text phase of the installation process. The F6 button should be clicked when the system prompts you to click "F6" to install SCSI or RAID devices.

Incorrect Answers:
A: This is not the most likely problem. The SCSI adapter device could very well be the same on the two adapters.
B: The removable Tape backup device is physically installed on SCSI adapter 1 while the hard disks are installed on SCSI adapter 0. There should be no conflict between the devices. The removable disk drive doesn't need to be reconfigured.
C: IRQs must only be reserved for legacy devices. A dual-channel SCSI adapter is most likely not a legacy device.
E: The SCSI hard drive is not accessible. Windows 2000 Setup cannot find any mass storage devices. Changing the BIOS boot device option will not help.

Q. 28
You are the administrator of a Windows 2000 server computer that is used for software development and testing. The server contains two hard disks, which are configured as drive C and drive D. Both are formatted as NTFS.

The server is configured with two installations of Windows 2000 Server. The server's Boot.ini file is as follows:

[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(0)partition(1) \WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1) \WINDOWS="Microsoft Windows 2000 Server I" /fastdetect
multi(0)disk(0)rdisk(1)partition(1) \WINDOWS="Microsoft Windows 2000 Server II" /fastdetect

C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Recovery Console"/cmdcons

You want the server to start the Windows 2000 Server installation that is located on drive D, unless an administrator selects the other installation during startup. Which Boot.ini file should you use?

A.
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(1)partition(1) \WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1) \WINDOWS="Microsoft Windows 2000 Server I" /fastdetect
multi(0)disk(0)rdisk(1)partition(1) \WINDOWS="Microsoft Windows 2000 Server II" /fastdetect
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Recovery Console"/cmdcons

B.
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(0)partition(2) \WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1) \WINDOWS="Microsoft Windows 2000 Server I" /fastdetect
multi(0)disk(0)rdisk(1)partition(1) \WINDOWS="Microsoft Windows 2000 Server II" /fastdetect
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Recovery Console"/cmdcons

C.
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(0)partition(1) \WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1) \WINDOWS="Microsoft Windows 2000 Server I" /fastdetect
multi(0)disk(0)rdisk(1)partition(1) \WINDOWS="Microsoft Windows 2000 Server II" /fastdetect
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Recovery Console"/cmdcons

D.
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(1)partition(0) \WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1) \WINDOWS="Microsoft Windows 2000 Server I" /fastdetect
multi(0)disk(0)rdisk(1)partition(0) \WINDOWS="Microsoft Windows 2000 Server II" /fastdetect
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Recovery Console"/cmdcons

Answer: A

Explanation: We want to change the default boot partition. The line beginning with multi=0 defines the default boot partition. We should use the first partition on the second disk. The first partition is denoted partition(1) since partitions are numbered starting from 1. The second disk is denoted rdisk(1) since disks are numbered starting from 0. We should use the default line of:
default=multi(0)disk(0)rdisk(1)partition(1) \WINDOWS

Incorrect Answers:
B: We should use the partition(1) parameter since the scenario doesn't mention that the D hard drive is partitioned. We must use the first and only partition on drive D.
C: The rdisk parameter on the default= line should be rdisk(1) not rdisk(0), since D is the second hard disk..
D: The partition parameter on the default= line should be partition(1) not partition(0). There is no partition 0.

Q. 29
You are a network administrator for your company. The network contains 50 Windows 2000 Server computers, which are in the Servers Organizational Unit (OU) in Active Directory. The network also contains 1,500 Windows 2000 Professional computers, which are in the computers container in Active Directory.

You need to deploy the most recent Windows 2000 service pack. The service pack must update only the servers.

You download the service pack and extract the file into a newly created shared folder named SPFiles. You need to install the service pack on all of the servers, and you want the installation to occur on all of the servers, and you want the installation to occur with no user interaction.

What should you do?

A. Create a Group Policy Object and link it to the Servers OU. Under the computer configuration, configure the GPO to assign the Update.msi file from the SPFiles folder. Restart each server.
B. Create a Group Policy Object and link it to the Servers OU. Under the computer configuration startup script, configure the GPO to assign the Update.msi file from the SPFiles folder. Restart each server.
C. Create a Group Policy Object and link it to the Domain level. Under the user configuration logon script, configure the GPO to assign the Update.msi file from the SPFiles folder. Log on to each server as Administrator.
D. Create a script that runs the Update.exe file from the SPFiles folder. Create a Group Policy Object and link it to the Servers OU. Modify the computer configuration of the GPO to run the script on startup. Restart each server.

Answer: A
Explanation: An Update.msi package should be deployed throughout the domain by using a computer-level Group Policy deployment. We create a new GPO, link the GPO to Servers OU, and configure the GPO to assign the update.msi file. We then restart the server. The update.msi file will be automatically installed.

Reference:
Best Practices for Using Windows 2000 Update.msi Package for Service Pack 1 Installation (Q278503)
White Paper, Windows 2000 Service Pack 1 Installation and Deployment Guide
White Paper, Windows 2000 Service Pack 2 Installation and Deployment Guide

Incorrect Answers:
B: There is no need to use a startup script.
C: A GPO linked to domain level would be applied to all computers in the domain. We are only interested in updating the servers.
D: This proposed solution would run the installation script every time a server reboots. Furthermore .msi files should be used for Active Directory deployment of Service packs. Update.exe is only used on the local computer.

Q. 30
You are the administrator of a Windows 2000 Server computer in your company's accounting department. The server runs Terminal Services in application mode. All users in the accounting department run their business applications in Terminal Service sessions.

A manager in the accounting department runs an application on the server. The application requires three hours to process financial and accounting data. This application must be run every Friday morning so that the data will be available to the director of accounting application to run with the least amount of performance impact on the other business applications.

What should you do?

A. Configure all other business applications to have High priority.
B. Configure all other business applications to have RealTime priority.
C. Configure the accounting application to have AboveNormal priority.
D. Configure the accounting application to have BelowNormal priority.

Answer: D
Explanation:

The application should be run at a low priority level in order to make least performance impact on the other applications. Either the low or the belownormal priorities could be considered.

Note: There are 5 priority levels in Windows 2000:
Realtime: the highest level which are used by some system processes, but almost never should be used for user processes.
High: Highest recommended priority level for user processes
Above Normal
Normal The default priority setting.
Belownormal
Low The lowest priority setting.

Incorrect Answers:
A: Running at a high priority would increase the load of the server.
B: Running the application in Realtime would be the worst possible choice. The performance of the server would suffer.
C: Running at a high priority would increase the load of the server.

Q. 31
You are a network administrator for your company. All servers run Windows 2000 Server. Users report that a file server named ServerA has very slow response time. It takes several seconds to open small files that are located on the server's hard disk, and it can take several minutes to open large files. Users report that no problems occur when they access files that are stored on other servers.

You monitor ServerA by using System Monitor. You discover that the values for Disk Queue Length and Split I/O are consistently high, even when users attempt to read small files. You also discover that the server has more than 40 GB of free space available.

You need to optimize disk read performance for ServerA. What should you do?

A. Use Disk Defragmenter to optimize the file structure on ServerA.
B. Use Disk Cleanup to remove unused files and folders from ServerA.
C. Disable write caching on the hard disk to optimize file access.
D. Configure the performance options on ServerA to optimize performance for background services.

Answer: A
Explanation: A fragmented hard disk would slow down the disk performance considerably. Microsoft recommends a defragmentation a month.

Incorrect answers:

B: The server has 40GB of free space. On a file this would slow down the disk performance.
C: Disabling write caching would decrease, not increase, disk performance.
D: Optimizing performance for background services could improve performance of a domain controller or a SQL Server computer. It would not, however improve the performance of a file server.

Q. 32
You are a network administrator for your company. Company executives plan to deploy 25 new Windows 2000 member servers and 25 new Windows 2000 Domain controllers. All Active Directory server accounts are in the default locations.

You need to install 290 hot fixes as part of the operating system installation on the new computers. The hot fixes must not be installed on any current Windows 2000 Server computers.

You create a distribution folder for the host fixes. What should you do next?

A. Use Setup Manager to create an answer file that will run a script to install the hot fixes from the distribution folder during setup.
B. Use Setup Manager to create an answer file. Add lines in the Cmdlines.txt file to install the hot fixes from the distribution folder during setup.
C. Create a script that will install all of the hot fixes automatically. Configure a Group Policy Object and link it to the domain level to run the script on startup.
D. Create a Group Policy Object and link it to the Domain Controllers OU and to the Computers container. Configure the GPO to assign the hot fixes as assigned applications.

Answer: B
Explanation: Hot Fixes are minor patches, usually limited to a few files covering a specific aspect of the product, which repair, replace, or enhance a function. Hot fixes are packaged as auto-extracting files that include a file called hotfix.exe that runs the install.
The Cmdlines.txt file contains the commands that GUI mode runs when installing optional components, such as hot fixes that must be installed immediately after the installation of Windows 2000.

Incorrect answers:
A: The answer file cannot run installation scripts. Instead cmdlines.txt must be used.
C: After creating a script that installs the hot fixes, configuring a GPO to run the script at startup, and linking the GPO at domain level would install the hot fixes on the existing Windows computers (except the Domain Controllers). But the hot fixes should not be installed on any current server.
D: The hot fixes must not be installed on any current server. Assigned the hot fixes with a GPO linked to the Domain Controller OU would, if it were successful, install the hot fixes on all domain controllers.

Q. 33
You are the network administrator for your company's branch office. You receive a memo from the main office indicating that a new custom software application will be deployed to the Windows 2000 Professional computers in your office that evening.

The following morning, the users in your office report that their computers will not start. Each computer stops a responding at the Windows 2000 Professional logon screen.

You contact the main office and the application's developers inform you that the new application includes a service named Data Listener. They discovered a problem with the service that is preventing the client computers in your office from starting.

The programmers at the main office will attempt to correct the problem. Until the problem is corrected, you need to allow your users to start their client computers normally and to access network resources. You need to accomplish this task as quickly as possible.

What should you do on each client computer?

A. Restart the computer by using safe mode.
B. Restart the computer by using a startup floppy disk, and run the **fixmbr** command.
C. Restart the computer by using the Recovery Console. Run the **disable "Data Listener"** command.
D. Restart the computer by using the Windows 2000 Professional CD-ROM, and select the option to repair the installation.

Answer: C
Explanation: The recovery console can be used to disable a network service that prevents the computer from starting.

Note: The Recovery Console is a command-line interface that can be used to access a hard disk of a Windows 2000 computer system. It can be accessed from the Windows 2000 Professional installation CD-ROM and can be used to repair an installation of Windows 2000 Professional by repairing the registry or by disabling a device driver or service. To repair an installation of Windows 2000 Professional by disabling a device driver, boot the computer from the Windows 2000 Professional installation CD-ROM. On the Welcome to Setup screen, click R to open the Repair Options screen, and click C to activate the Recovery Console. If we are unsure of the name of the service or driver that is causing the problem we can type 'listsvc' to obtain a list of the device drivers and services that currently installed on the computer. Then use the **disable "Data Listener"** command to the disable the faulty service.

Incorrect answers:
A: The computer would probably not start in safe mode due to the faulty service.
B: You cannot start the computer with a startup floppy disk.

In recovery console the **fixmbr** command would replace the master boot record.

D: Repairing the installation is unnecessary and would require more effort. Only the service must be disabled.

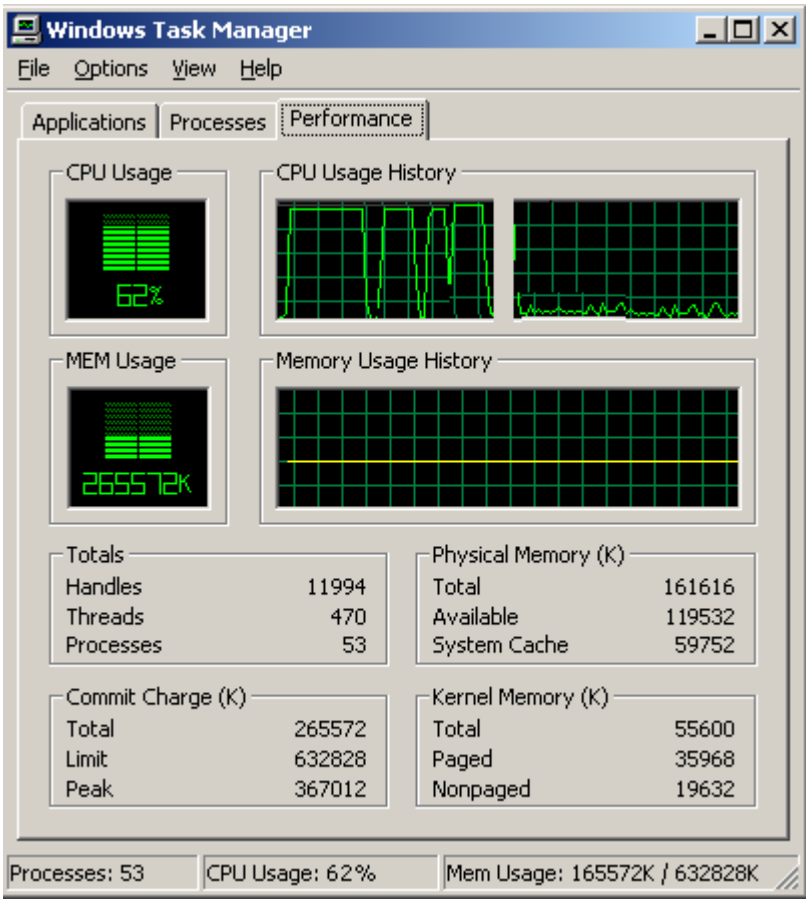
Q. 34

You are a network administrator for your company. All servers run Windows 2000 Server.

Users in the finance department report significantly slow performance when they access a database application that is hosted on a multiprocessor server named ServerA. The application was designed for symmetric multiprocessing (SMP) and for use with Windows NT server 4.0 computers. The application runs constantly as a background application.

Users do not report problems when they access the same database application running on a server named ServerB. Both servers have identical hardware.

You start task manager on serverA. You view the information that is shown in the exhibit.



You need to optimize performance for users in the finance department when they access the database application. What should you do?

A. Configure the application to run in a separate memory space.
B. Configure the application's process to run with high priority and with affinity for the second processor only.
C. Increase the amount of physical memory and increase the size of the paging file on serverA.
D. Set processor affinity for the application to allow the application to use all available processors.

Answer: D
Explanation: By examining the exhibit we see that 1st processor is heavily used (on the left), but the 2nd processor is far from its capacity (on the right). The application is apparently only using the 1st processor. We must enable it to use all available processors.

Incorrect answers:
A: Windows 2000 application runs in separate memory spaces by default.
Only legacy 16-bit application would sometimes need to be configured to run in a separate memory space.
B: The application support symmetric multiprocessing and would run faster on all available processor.
C: The memory is not the problem. According the exhibit there are lot of memory available.

Q. 35
You are a network administrator for your company. A user named Marc reports a problem with his Windows 2000 Professional computer.

You examine the computer and discover that it is displaying a STOP message. The documentation for Marc's computer indicates that the computer contains a single hard disk, which is configured as a single NTFS logical volume.

Marc reports that the computer was working normally until he connected a new USB digital camera to the computer. The computer installed the camera's software drivers, and then restarted. After the computer restarted, it displayed the STOP message and Marc was not able to log on to the computer.

You need to return Marc's computer to normal operation as quickly as possible. What should you do?

A. Restart the computer by using safe mode.
B. Restart the computer by using the last known good configuration

C. Restart the computer by using the Windows 2000 Professional CD-ROM, and select the option to repair the installation.
D. Restart the computer by using the Windows 2000 Professional CD-ROM, and select the option for Recovery Console.

Answer: B
Explanation: We have installed a bad driver. We have not had a successful logon after the bad driver was installed so we can safely use the last known good configuration.
The last known good configuration requires the least administrative effort and is therefore the preferred method. It will return the state of the computer as it were when the last successful log on took place.

Incorrect answers:
A: Safe mode could possibly be used. It would require more effort though.
C: It is unnecessary to repair the installation. This would involve a lot of work and some configuration might be lost.
D: The recovery could be used to disable the device driver. It would, however not be quickest method to recover.

Q. 36
You are a network administrator for your company. The network consists of a single Windows 2000 Domain. All servers run Windows 2000 Server. All client computers run Windows 2000 Professional.

A server in the sales department has a tape backup device installed. The device functions normally by using the driver from the Windows 2000 Server CD-ROM. You install an update driver for the device that is supplied by the manufacturer. When you restart the server, you receive the following error message: "STOP: IRQL_NOT_LESS_OR_EQUAL."

You restart the server, and you receive the same error message. You need to correct the problem and return the server to normal operation. What should you do?

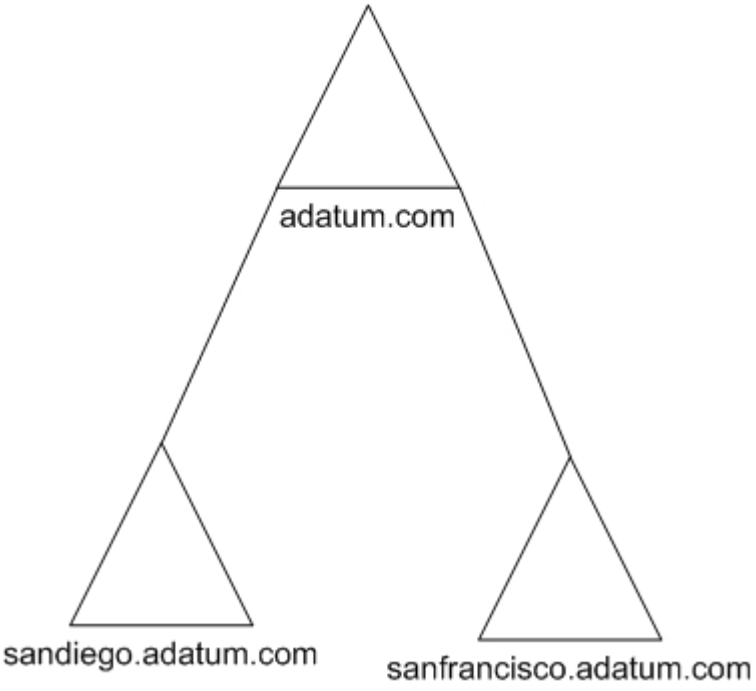
A. Restart the server in safe mode. Create a local computer policy to enable Windows File Protection.
B. Restart the server in safe mode. Log on as an administrator. In the **Driver Signing Options** dialog box, set File Signature Verification to **Ignore**.
C. Restart the server by using the last known good configuration.
D. Restart the server by using the Recovery console. Enable the new device driver by using the **Service_system_start** parameter.

Answer: C

Explanation: We have installed a bad driver. The last known good configuration can be used since we have not have had a successful logon after the bad driver was installed.
The last known good configuration requires the least administrative effort and is therefore the preferred method. It will return the state of the computer as it were when the last successful log on took place.

Incorrect answers:
A: Windows File protection checks the integrity of the system files. In this scenario we have a device driver problem. Windows File protection is of no use in fixing this problem.
B: We must remove the faulty driver. It is too later to configure Driver Signing now. The harm has already been done.
D: The device driver should be disabled or removed, not enabled.

Q. 37
You are a domain administrator for A. Datum Corporation. The company's network consists of three domains, as shown in the exhibit.



You are responsible for the sandiego.adatum.com domain. The sandiego.adatum.com domain contains users accounts for 50 of the employees in the finance department. Recently, a shared folder named FinanceA was created in the sandiego.adatum.com domain. FinanceA can be accessed by only those 50 employees. FinanceA contains forms that are used by the 50 employees.

You are instructed to create a group on your domain controllers that will allow finance users whose user accounts are in global from the other domains to access FiannceA. You must accomplish this goal while minimizing replication overhead.

What should you do?

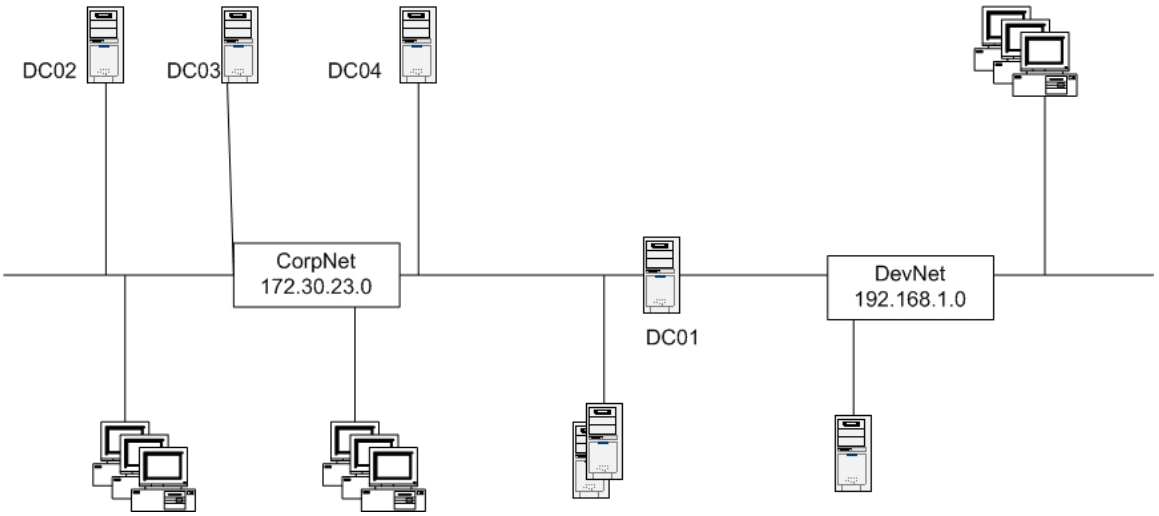
A. Create a global group. Add the appropriate groups from the other domains to the global group. Assign the global group permissions for FinanceA.
B. Create a domain local group. Add the appropriate groups from the other domains to the domain local group. Assign the domain local group permissions to the FinanceA.
C. Create a universal group. Add the appropriate groups from the other domains to the universal group. Assign the universal group permissions for FinanceA.
D. Create a distribution group. Add the appropriate groups from the other domains to the distribution group. Assign the distribution group permissions for FinanceA.

Answer: B
Explanation: The preferred Microsoft solution is:

1. Assign appropriate permissions to a domain local group.
   In this scenario the domain local group is assigned permissions to the FinanceA share.
2. Add the appropriate groups from the other domain (and the current domain) to the domain local group.

Incorrect answers:
A: A global group can only contain USER accounts, computer accounts, and global groups from the same domain. A global group cannot contain global groups from other domains.
C: Creating a universal group, assigning the appropriate permission the universal, and adding the appropriate global groups from the other domains would work. This would not be the best solution though since changes in the universal group would have to be replicated between the domains. A domain local group is local in scope and would not have to be replicated to the other domains.
D: A distribution group is only used by applications, not by Windows 2000. A distribution group cannot be used to configure permissions.

Q. 38
You are a network administrator for your company. The network consists of a single Windows 2000 Domain. The domain contains four Windows 2000 Domain controllers. The relevant portion of your network is configured as shown in the exhibit.



The domain controller named DC1 is a multihomed computer that provides DNS and DHCP services for the company intranet and only DHCP services for a secure network used by the software development department. DC01 does not route between the two networks. The computers in the software development department are not members of the domain.

DC01 hosts an Active Directory integrated DNS zone. DC01 is configured as shown in the following table:

Network adapter	IP address	Subnet mask	Default gateway	DNS server address
NIC1	172.30.23.1	255.255.255.0	None configured	127.0.0.1
NIC2	192.168.1.1	255.255.255.0	None configured	127.0.0.1

You discover that Active Directory replication intermittently fails between DC01 and the other domain controllers. When this occurs, you receive the following error message: "RPC server is unavailable." There is no consistent pattern to the replication failures. The other domain controllers do not experience this problem when replicating to each other.

You need to ensure that replication occurs normally between all domain controllers. What should you do?

A. In the TCP/IP properties for NIC1 on DC01, disable dynamic DNS registration. Remove all A (host) records from the DNS zone for DC01 for the address 172.30.23.1. Remove the address 172.30.23.1 from the **Interfaces** tab in the properties for DC01 in the DNS console.

B. In the TCP/IP properties for NIC2 on DC01, disable dynamic DNS registration. Remove all A (host) records from the DNS zone for DC01 for the address 192.168.1.1. Remove the address 192.168.1.1 from the **Interfaces** tab in the properties for DC01 in the DNS console.

C. In the TCP/IP properties for NIC1 on DC01, disable dynamic DNS registration. Remove all A (host) records from the DNS zone for DC01 for the address 192.168.1.1. Disable round robin functionality on DC01. Disable recursive queries on DC01.

D. In the TCP/IP properties for NIC2 on DC01, disable dynamic DNS registration. Remove all A (host) records from the DNS zone for DC01 for the address 172.30.23.1. Disable round robin functionality on DC01. Disable recursive queries on DC01.

Answer: B

Explanation: The DNS server should only be configured for NIC1, which is connected to the domain. DC01 should not provide DNS services for the development subnet on NIC2. We must remove all host records for DC01 for the address 192.168.1.1. Then we have to remove the address 192.168.1.1 from the interfaces. This will disable DNS on NIC2, or in other words make DC01 only listen for DNS on NIC1.

Note: The error **RPC Server is Unavailable** can occur when:

- The RPC service may not be started.
- You are unable to resolve a DNS or NetBIOS name.
  This is the problem in this scenario. We are sometimes unable to resolve a DNS name. This occurs because there are incorrect host records where DC01 has the IP address 192.168.1.1, in the DNS zone. Computers who try to connect to DC01 with the IP address 192.168.1.1 will not be able to connect to DC01.
- An RPC channel cannot be established.

Reference: Troubleshooting "RPC Server is Unavailable" in Windows (Q224370)

Incorrect answers:

A: Removing NIC1 as a DNS interface would disable DNS on NIC1, the domain interface. We must disable DNS on NIC2 instead.

C: NIC2 must be removed from the interfaces not NIC1.

D: We most remove the address 192.168.1.1. from the Interfaces. Disabling round robin would not disable DNS on NIC2.

Q. 39

You are the desktop administrator for your company. The company is migrating from a Windows NT 4.0 domain in to a new Windows 2000 Domain. As part of the migration, you are removing Windows NT workstation 4.0 computer accounts from the Windows NT domain and adding them to a Windows 2000 Active Directory domain.

You add 10 Windows NT workstation computer accounts to the Active Directory domain. When you attempt to add another Windows NT workstation computer account to the Active Directory domain, you

receive the following error message: "The machine account for this computer either does not exist or is unavailable."

You need to be able to add Windows NT workstation computer accounts to the Windows 2000 Active Directory domain. What should you do?

A. Configure a DNS server for the Windows NT workstation computers that have not been added to the Active Directory domain.
B. Delete from the Windows NT domain the computer accounts for the Windows NT workstation computers that have not been added to the Active Directory domain.
C. Ask the domain administrator to assign you the **Allow-Create Computer objects** permission for the Computers container.
D. Ask the domain administrator to assign you the **Allow-Create Computer objects** permission for the Domain Controllers container.

Answer: C
Explanation: This error message occurs after you have joined 10 computers to the domain from a Windows NT 4.0 computer. In order to work around this problem you could either pre-create computer accounts in the Active Directory, or (like in this answer) assign **Create Computer objects** permissions on the Computers container for the user.

Reference: Domain Users Cannot Join Workstation or Server to a Domain (Q251335)

Incorrect answers:
A: This is not a name resolution problem.
B: Deleting the computer accounts in the old Windows NT domain will not help.
D: The permission must be assigned to the Computer Container, not the Domain Controllers container.

Q. 40
You are the administrator of an organizational Unit (OU) named New York. The New York OU contains OUs named Operations, Accounting, and Executive. You create a software deployment Group Policy Object that assigns an application named CorpFinance. You link the GPO to the New York OU.

Users in the Operations OU report that the CorpFinance application shortcut does not appear on their Start menus. Users in the Accounting and Executive OUs report that the shortcut appears on their Start menus.

You need to ensure that the CorpFinance application shortcut appears on the Start menu for every user in the New York OU. What should you do?

A. Modify the GPO so that CorpFinance is published instead of assigned.
B. Modify the permissions on the CorpFinance installation package so that members of the Operations OU have the **Change** permission.
C. Configure the Operations OU to not block policy inheritance.
D. Configure the GPO to use the basic installation user interface.

Answer: C
Explanation: The GPO is not applied to the Operations OU. Apparently the Operations OU blocks policy inheritance.

Incorrect answers:
A: The application has correctly been chosen to be assigned, not published. Assigned applications appear in the Start menu, while published applications must be manually installed.
B: The users should only have Read permission, not Change permissions, on the installation package. Only administrators should have change permission on the distribution folder.
If this were a file permission problem the users in the Operations OU would get an error message indicating this problem when they started their computers.
D: The installation user interface worked for users in the Accounting and the Executive OUs so there is nothing wrong with the installation user interface or the installation package.

Q. 41
You are a network administrator for your company. You need to create a Group Policy Object that requires user accounts to have a minimum password length of seven characters. All of the Active Directory user accounts are in the MN Organizational Unit (OU).

Under the computer configuration, you create a GPO named PasswordGPO that requires a minimum of seven characters, and you link this GPO to the MN OU. After you link the GPO, you find out that users can create passwords that are only one character in length.

You need to ensure that all users in the MN OU are required to have a minimum password length of seven characters. What should you do?

A. Remove the GPO link on the MN OU for PasswordGPO. At the domain level, add a link to the PasswordGPO, and ensure that the GPO has the highest priority.
B. Create a new GPO and link it to the MN OU. Configure the password requirement for this GPO to be minimum of seven characters, and make the GPO the highest priority.
C. Run the **Secedit/refreshpolicy machine_policy/enforce** command on the domain controller on which you created the GPO.
D. Run the **Secedit/refreshpolicy user_policy/enforce** command on the domain controller on which you created the GPO.

Answer: A
Explanation: Password policies can only be applied at domain level. They cannot be applied to an OU. We must link the PasswordGPO at the Domain level.

Incorrect answers:
B: Password policies can only be applied at domain level. They cannot be applied to an OU.
C: Password policies can only be applied at domain level. The GPO must be linked at the domain level.
D: Password policies can only be applied at domain level. The GPO must be linked at the domain level.

Q. 42
You are a network administrator for your company. All user accounts and groups are in the New York organizational unit (OU). The user accounts of the help desk personnel are members of the Helpdesk group.

You need to allow the Helpdesk group to manage group memberships, including creating and managing new groups. However, you need to ensure that help desk personnel cannot create or modify user objects.

What should you do?

A. Under the New York OU, create two new OUs and name them NY Users and NY groups. Move all user accounts to the NY Users OU, and move all groups to the NY groups OU. Modify the Active Directory permissions for the New York OU by assigning the Helpdesk group the **Allow-Full Control** permission.
B. Under the New York OU, create two new OUs and name them NY Users and NY Groups. Move all user accounts to the NY Users OU, and move all groups to the NY groups OU. Modify the Active Directory permissions for the NY Groups OU by assigning the Helpdesk group the **Allow-Full Control** permission.
C. Run the Delegation of Control wizard on the New York OU. Delegate the **Modify the membership of a group** task to the Helpdesk group.
D. Run the Delegation of Control wizard on the New York OU. Delegate the **Create, delete, and manage groups** task to the Helpdesk group.

Answer: D
Explanation: The **Create, delete, and mange group** right would allow the Helpdesk group to manage groups in the OU. They would also be able to create new groups.

Incorrect answers:

A: Giving the Helpdesk group **Full Control** permission to the New York would allow them to create and modify user objects in the New York OU and in the child OUs.
B: Assigning **Full Control** permission on an OU to the Helpdesk group would allow them to create and modify user objects in this OU.
C: The Helpdesk group must be able to create new groups. The **Modify the membership of the group** right is not enough.

Q. 43
You are an administrator of your company's single Windows 2000 Domain. The domain contains 10 departmental organizational unit (OUs). Each OU is controlled by a separate administrative group.

During a routine security audit, you discover that the local Administrators groups on member servers contain users who are not administrators. You want to ensure that the local Administrators group on every server contains only valid administrator accounts from the appropriate department.

What should you do?

A. Configure Group Policy for each OU to specify the appropriate membership for the local Administrators group on the servers in that OU.
B. Configure Group Policy for the domain to specify the appropriate membership for the local Administrators group on the servers in that OU.
C. Configure Group Policy for the default Domain Controller OU to specify the appropriate membership for the local Administrators group on the servers in that OU.
D. In each OU, create a new child OU that contains all of the appropriate Administrator user accounts for that OU. Configure Group Policy for each new child OU to specify the appropriate membership for the local Administrators group on the servers in that OU.

Answer: D
Explanation: We must make the configuration at OU level, since we have to specify the appropriate local administrators for each OU. We do it by:

1. Create a new child OU for each departmental OU.
2. Add all the user accounts that should be member of the local Administrator group of the department to the new child OU.
3. Create a GPO for each new child OU that restricts the membership of the Local Administrators account to the members of the child OU.

Note: Domain controllers don't have any local administrators group. Only member servers or stand-alone servers have local administrator groups.

Incorrect answers:

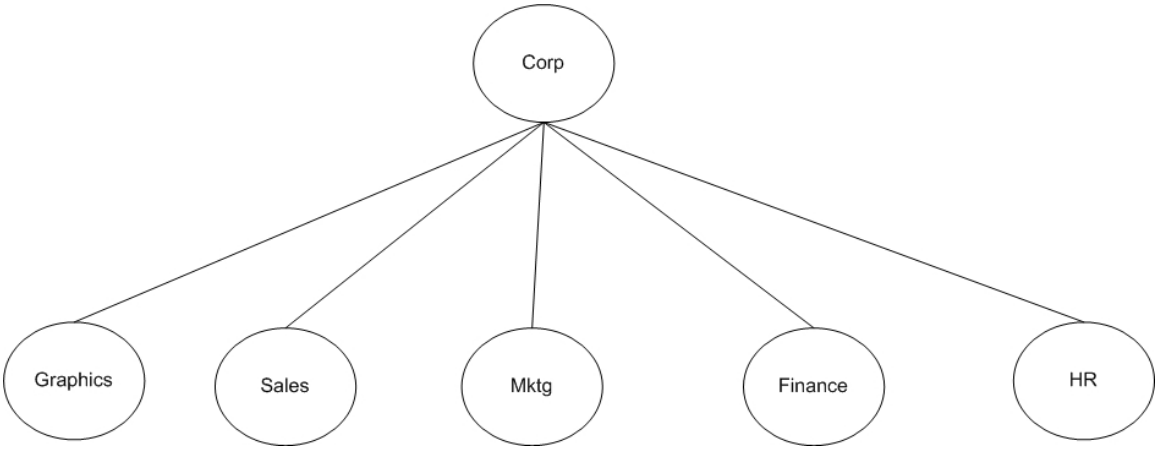
A: We must collect the users that are allowed to be local Administrators in some way. We could put them in a group or in an OU and then let the GPO use this group or OU to restrict the membership of the local Administrators account.

B: We cannot create a GPO at domain level that restricts membership to the local Administrators group for administrators of the corresponding OU.

C: We are interested in the member servers not the domain controllers since the domain controllers don't have a local administrator group. We cannot use the default Domain Controller OU.

Q. 44

You are a network administrator for your company. The network consists of a single Windows 2000 Domain. The domain has an Organizational unit (OU) structure, as shown in the exhibit.



All user accounts are created in the Corp OU. All user accounts are members of a CorpUsers group that is located in the Corp OU. All user accounts are also members of department-specific groups that are located in the departmental OUs.

Each department has its own administrative staff, which is responsible for creating computer accounts, troubleshooting user and computer problems, and performing general system maintenance. Departmental administrators are members of groups named <*department*>Admins located in the departmental OUs. Departmental administrators have been delegated full control of their OUs. All Computer accounts are located in their appropriate departmental OUs.

Group Policy Objects are configured as shown in the following table:

GPO name	Linked to	Settings/restrictions	Options
Users	Corp OU	Disable Control Panel. Remove Run command from Start menu. Disable and	No override

		remove links to Windows Update. **Remove "Map Network Drive" and "Disconnect Network Drive" in Windows Explorer**	
Departmental Admins	**Corp OU**	**No settings configured**	

The departmental administrators report that they cannot access Control Panel to the Run command on their own computers or when they attempt to correct problems on users' computers.

The departmental administrators require access to the restricted tools. What should you do?

A. Disable the **No Override** option for the Users GPO.
B. Enable the **No Override** option for the Department Admins GPO.
C. Select **Block Policy inheritance** in the Group Policy properties for each child OU.
D. Change the Group Policy processing order to ensure that the Department Admins GPO is processed last.
E. Assign the **Deny-Apply Group Policy** permissions to the various <*department*>Admins groups for the Users GPO.

Answer: E
Explanation: The departmental administrators are also users. The User GPO will be applied to them as well. This is the reason for the problem.
By denying the **Apply Group Policy** permissions on the Users GPO for the Departmental Administrators the Users GPO would not be applied to them.

Incorrect answers:
A: Disabling the **No Override** option for the Users GPO would be a bad idea. Then the Departmental Administrators could override these settings for the local users.
B: The **No Override** option applied Departmental Admins GPO would have no effect since no settings are configured for this GPO.
C: The **No Override** option at the CORP OU will override the **Block Policy inheritance** at the departmental OUs.
D: Changing the order in which the GPOs are applied would not change matters. The Users GPO would still be applied the Departmental Administrators.

Q. 45
You are a network administrator for your company. The help desk manager reports that the help desk is receiving a large number of requests from sales representatives who need to have their passwords reset. The help desk manager asks you to delegate this task to someone other than help desk personnel.

The user accounts of all sales representatives are in the sales Users organizational unit. The user accounts of all sales managers are in the Sales Manager OU and are members of the Sales Managers group. You decide to allow the Sales managers to reset the passwords for their sales representatives when necessary. You need to configure Active Directory without compromising overall network security.

What should you do to allow the members of the Sales Managers group to reset passwords for the sales representatives?

A. Run the Delegation of Control wizard at the domain level and delegate the **Create, Delete, and manage user accounts** task to the Sales Managers group.
B. Run the Delegation of Control wizard on the Sales Users OU and delegate the **Create, Delete, and manage user accounts** task to the Sales Managers group.
C. Run the Delegation of Control wizard on the Sales Users OU and delegate the **Reset passwords on user accounts** task to the Sales Managers group.
D. Run the Delegation of Control wizard at the domain level and delegate the **Reset passwords on user accounts** task to the Sales Managers group.

Answer: C
Explanation: The managers must be given the **Reset passwords on user accounts** right on the Sales OU. This will allows the managers to reset passwords only for the sales representatives.

Incorrect answers:
A: The managers should not be allowed to create and delete user accounts.
B: The managers should not be allowed to create and delete user accounts.
D: The managers don't need to be able to reset passwords throughout the domain. They only need to reset passwords of the users accounts in the Sales OU.

Q. 46
You are a domain administrator for your company. You are installing a Windows 2000 Server computer named ServerA and 25 Windows 2000 Professional computers in a new branch office.

You want to enable the client computers in the branch office to access the Internet as needed. You have a dial-up account with a local Internet service provider (ISP).

You want to reduce connection charges from your ISP. Therefore, you want the connection to be active only when internet resources are requested.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

A. Attach a modem to ServerA and create a dial-up connection to the ISP.
B. Attach a modem to one of the Windows 2000 Professional computers and create a dial-up connection to the ISP.
C. Configure the modem to use software handshaking.
D. Configure the modem to use hardware handshaking.
E. Configure the dial-up connection to enable on-demand dialing.
F. Configure the dial-up connection to enable Internet Connection Sharing.
G. Configure the client computers in the branch office to enable Internet Connection Sharing.

Answer: A, E, F
Explanation:
It is easy to configure ICS:

1. Attach a modem to the computer which will be used as the ICS computer.
   Use a Windows 2000 server to support more than 10 simultaneous users.
2. Create a dial-up connection to ISP.
3. Enable on-demand dialing if you only want to stay online when there is activity on the connection.
4. Enable Internet Connection Sharing on the dial-up connection.
   This is just a checkbox that must be selected.
5. Make sure that the (ICS) clients on the local network are enabled for DHCP.
   This is the default in all Windows version since Windows 95.

Incorrect answers:
B: Only a maximum of 10 computers can simultaneously be connected to a specific shared source on a Windows 2000 Professional computer. There are 25 client computers and one server on the network so this could restrict the number of users that access the internet.
C: As long as the modem is able to communicate with the ISP the ICS would function with or without software handshaking.
D: As long as the modem is able to communicate with the ISP the ICS would function with or without hardware handshaking.
G: Internet sharing should be enabled on the ICS server computer not at the client computers. The client computers just have to be enabled as DHCP clients.

Q. 47
You are a domain administrator for your company. The network consists of a single Active Directory domain and contains a Windows 2000 Server computer named ServerA.

ServerA has Routing and Remote Access installed. Employees use ServerA to connect to the corporate network by using a dial-up connection. The remote access policy for ServerA change frequently.

The company is hiring 200 new employees who will work remotely. You need to add four Windows 2000 Server computers with Routing and Remote access installed so that the new employees can dial in to the network.

You want to configure all of these Routing and Remote Access servers to use the same remote access policies. You want to configure and maintain the remote access policies with the least amount of administrative effort.

What should you do?

A. Add the new Routing and Remote access servers to the domain. Place the remote access policies on ServerA.
B. Promote ServerA to a domain controller in the domain. Add the new Routing and Remote Access Servers as members of the domain.
C. Install the Internet Authentication Service (IAS) on ServerA. Configure the new Routing and Remote Access servers to use serverA for authentication requests.
D. Create a new domain controller named ServerB. Install the Internet Authentication Server (IAS) on ServerB. Configure the new Routing and Remote access servers to use serverB for authentication requests.

Answer: C
Explanation: IAS provides connection authentication, authorization, and accounting for dial-up and virtual private network (VPN) remote access and for router-to-router connections.
We want to configure IAS with the least administrative effort. Setting up IAS in this scenario is not hard:

1. Install the Internet Authentication service on ServerA.
2. Configure the other four RRAS computers to use RADIUS authentication and specify that ServerA should be used for authentication.

Incorrect answers:
A: To centralize the administration of several RRAS servers an IAS server is needed.
B: To centralize the administration of several RRAS servers an IAS server is needed.
D: Installing a new domain controller with IAS would provide redundancy for the Active Directory and would offload some work from the Domain Controller. However it would require more administrative

effort than simply installing IAS on the existing domain controller ServerA. In this scenario the requirement is to accomplish the goal with the least amount of administrative effort.

Q. 48
You are a domain administrator for your company. You are installing a network in a new branch office. The network contains two Windows 2000 Server computers and 10 Windows 2000 Professional computers. A Windows 2000 Server computer named ServerA provides DHCP service for the network.

You are installing a new Windows 2000 Server computer named ServerC. You have a dial-up account with a local Internet service provider (ISP). You connect a 56-Kbps modem to ServerC. You want to use serverC to provide shared access to the internet.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

A. Install the WinSock proxy client on ServerC.
B. Install the WinSock proxy client on all of the client computers.
C. Install the DNS service on ServerC.
D. Install internet connection sharing on ServerC.
E. Uninstall the DHCP service on serverA.
F. Create a dial-up connection on ServerC and configure the connection with the ISP account information.

Answer: D, E, F
Explanation:
We configure the network for ICS with the following steps:

1. Uninstall the DHCP service on serverA. (E)
ICS includes a DHCP allocator which functions as a mini-DHCP server. ICS cannot function on a network which has a DHCP server running.

2. Create a dial-up connection on ServerC. Configure the connection with the ISP account information.

3. Enable ICS on ServerC.
This step is accomplished by a simple click in a checkbox.

Incorrect answers:
A: Wins Proxy client is not required for setting up ICS.
B: Wins Proxy client is not required for setting up ICS.
C: ICS doesn't require DNS. In fact ICS would not function on a network where a DNS server is running.

Q. 49
You are a domain administrator for your company. The network consists of a single Active Directory domain. The network contains 15 Windows 2000 Server computers and 150 Windows 2000 Professional computers. A server named ServerA has Routing and Remote Access Installed and is configured for incoming dial-up connections.

You install Windows 2000 Professional on a home computer named Home1. You create a new PPP dial-up connection to connect to ServerA. You configure the connection to use both of the external modems on Home1 and to use Multilink. You start the dial-up connection administrator connect to ServerA. You notice that only one of the modems is connected to serverA.

What should you do?

A. Configure the dial-up connection on Home1 to use SLIP.
B. Configure ServerA to accept Multilink dial-up connections.
C. Replace the modems on ServerA with new modems that support SLIP
D. Replace the modems on Home1 with new modems that support Multilink.

Answer: B
Explanation: Multilink must be enabled both at the dial-up client and at the RRAS server.

Incorrect answers:
A: SLIP is an old legacy protocol mostly used to connect to UNIX remote access servers. Windows 2000 Server doesn't allow SLIP for in-coming connections.
C: SLIP is a communication protocol. Modems transmit electronic signals and they don't have to be compatible in any way with high-level communication protocols like SLIP.
D: Multilink is supported in the operating system. The modems functions as usual and doesn't have to meet any special requirements to be used in multilink connections.

Q. 50
You are the administrator of a Windows 2000 Server computer that runs terminal Services. A user named Marc uses Terminal services to connect to the server in order to run a custom Windows-based application that is installed on the server.

The application takes two hours to generate a sales report. Marc reports that he can connect to the server and log on, run the application, and start the report. However, his Terminal Services client disconnects from the server before the report is complete. When Marc attempts to reconnect to the server, he discovers that the application is no longer running.

You need to ensure that Marc's computer can remain connected to the server long enough for the application to complete the sales report. You do not want to affect how other users use the server.

What should you do?

A. In Terminal services Manager, shadow Marc's session after Marc has been connected to the server for 20 minutes, and troubleshooting the problem.
B. In Active Directory Users and Computers, modify Marc's user account by specifying a maximum Terminal Services disconnect time of three hours.
C. In Active Directory Users and Computers, modify Marc's user account by specifying a maximum Terminal Services idle time of three hours.
D. In Terminal Services Configuration, modify the RDP-TCP connections by setting the maximum idle time to three hours.

Answer: C
Explanation: Many Terminal server settings can be set on the Sessions tab of the Account Properties Dialog box in Active Directory Users and Computers. The Idle session limit can be set to three hours. This would allow Marc's session to finish the report before the Terminal Services connection disconnects.
The Idle session limit setting specifies the maximum time a session can remain idle.

Incorrect answers:
A: Shadowing allows you to remotely control an active session of another user. You can either view or actively control the session. If you choose to actively control a user's session, you will be able to input keyboard and mouse actions to the session. This would not keep the computer connected to the terminal server though.
B: The Maximum Disconnection Time option specifies the maximum time a session can remain disconnected. But we want Marc's computer to be connected to the computer so that the report can be produced.
D: The RDP-connections cannot be used to configure the duration of a connection for a specific user.
Note: The Remote Desktop Protocol (RDP) is designed to provide remote display and input capabilities over network connections for Windows-based applications running on a server.
Reference: Explanation of RDP-TCP Permissions in Windows 2000 (Q243554)

Q. 51
You are a network administrator for Contoso Pharmaceuticals. The network contains three Windows 2000 Server computers, which run the DNS server service, and two UNIX BIND-based DNS servers. The Windows 2000 DNS servers are domain controllers for a single domain named ad.contoso.com. The DNS zone type for ad.contoso.com is Active Directory integrated. The zone is configured with default refresh and expire intervals and default zone transfer properties.

Windows 2000 Server computers in the domain are configured to dynamically register with the Windows 2000 DNS servers. However, all Windows 2000 Professional and UNIX computers are configured to use the BIND-based DNS servers for name resolution.

You create secondary zones for ad.contoso.com in each of the BIND-based DNS servers, and you configure the ad.contoso.com domain controllers as the master DNS servers. When you inspect the secondary zone on the BIND-based DNS servers the next day, there are no records in the zone.

You need to ensure that the secondary zones on the BIND-based DNS servers include up-to-date DNS records. What should you do?

A. On one of the domain controllers, select the **Allow zone transfers** check box in the properties for the zone.
B. On one of the domain controllers, increase the expire interval for the ad.contoso.com zone to two days.
C. On one of the domain controllers, change the zone type for ad.contoso.com to standard primary. On the remainder of the domain controllers, change the zone type to standard secondary.
D. On each of the domain controllers, assign the Pre-Windows 2000 Compatible Access group the **Allow-Read** permission for the ad.contoso.com zone.

Answer: C
Explanation: BIND DNS servers do not support Active Directory integrated zones. They are limited to primary and secondary zones. We must change zone types from the Active Directory integrated zones to standard secondary on all Windows 2000 DNS server except one, and to standard primary on one of the Windows 2000 DNS servers.

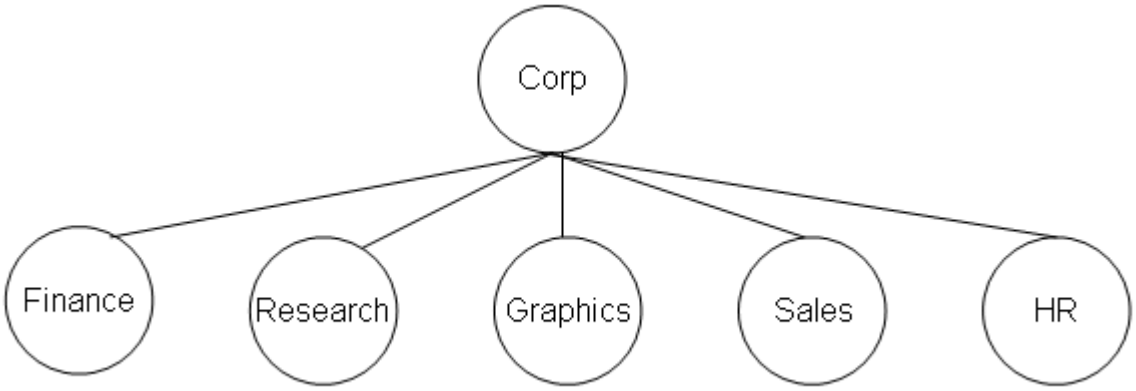
Incorrect answers:
A: The default zone transfer setting is to allow zone transfers to any DNS server.
BIND DNS servers cannot be integrated with Windows 2000 DNS servers that use Active Directory integrated zones.
B: The expire interval is used by other DNS servers configured to load and host the zone to determine when zone data expires if not renewed. But the DNS are not able to receive DNS zones from the Active Directory DNS zones on the Windows 2000 DNS servers.
D: The Pre-Windows 2000 Compatible Access is mainly used to integrate Windows NT 4.0 RAS with Windows 2000 RRAS. The UNIX BIND DNS servers would not gain access to the Active Directory DNS zones as members of this group.
Reference: HOW TO: Add Users to the Pre-Windows 2000 Compatible Access Group (Q303973)

Q. 52

You are a network administrator for your company. The network consists of a single Windows 2000 Domain. All client computers run Windows 2000 Professional and are members of the domain.

Client computers in the research department and the graphics department are new and have clean installs of Windows 2000 Professional. Client computers in the other departments have been upgraded from Windows NT workstation 4.0 to Windows 2000 Professional.

The domain contains an organizational unit (OU) hierarchy, as shown in the exhibit.



You want to ensure that all upgraded computers have the same security configuration as the computers that have the clean installs. You also want to ensure that all client computers have strong password policies applied, and that an administrator is required to unlock locked user accounts for the research department and the human resources (HR) department.

You create a Group Policy Object named DefaultSec, which applies security setting that are required for all users and computers. You create a second GPO named HiSec, which has the security setting that are required by the HR and the Research departments. Both GPOs use custom security templates.

You import the Basicwk.inf security template in to the Default Domain GPO
How should you link the GPOs to the OUs?

To answer click the select and place button, and then drag the appropriate Group Policy Object to the appropriate department OU. Note that GPOs can be used more than once.

SELECT AND PLACE

Answer:

Comments:

The Default Domain Policy GPO is applied to the domain by definition and will not have to be applied to any OU.
The DefaultSec GPO should be applied to all users and computers so we apply it highest possible OU, we link it to the Corp OU.
The HiSec GPO should only be applied to the Research and HR departments so we link to the Research OU and to the HR OU.

Q. 53
You are the administrator for your company's intranet web site. The web site is hosted on a Windows 2000 Server computer.

You need to install a new web server component that will be used with a new web site that is in development. The new component is an ISAPI-based application. You install the component in a virtual directory named COMMON and configure the Read, Script, and Execute permissions.

When the developers test their applications by using the new component, they receive an error message stating that the component could not be started.

You want to ensure that the new component functions properly on the web site. What should you do?

A. Configure the intranet web site to remove the default application.
B. Configure the COMMON virtual directory to run with low application protection.
C. Configure the COMMON virtual directory to run with high application protection.
D. Configure the **Execute** permission on the intranet web site to enable Scripts only.
E. Configure the **Execute** permission on the intranet web site to enable Scripts and Executables.

Answer: E
Explanation: ISAPI applications are executables not scripts. The **Execute** permission on the intranet web site must be configured to enable Scripts and Executables, not Scripts only.

Steps:
1. Open the Internet Services Manager
2. Right-click on the Virtual Directory and select Properties
3. Change the Execute Permissions option to **Scripts and Executables**.

Note: ISAPI (Internet Server Application Programming Interface) is an API for writing extensions to web servers. It was originally developed by Process Software, and adopted by Microsoft as its standard server API. It complements or replaces the Common Gateway Interface (CGI), the standard interprocess protocol for writing extensions to web servers.
Incorrect answers:

A: If you remove the default you must specify a new application.
The **Execute** permission must be changed to **Scripts and Executables**.
B: When a virtual directory is running in the IIS Process (Low Application Protection) IIS runs as SYSTEM and then impersonates the Anonymous User. This wouldn't allowed the ISAPI application to be run.
C: High application protection prevents in Impersonation. It wouldn't allow the ISAPI based to run.
D: The **Execute** permission on the intranet web site must be configure to enable Scripts and Executables, not Scripts only. ISAPI applications are executables not scripts.

Q. 54
You are a network administrator for your company. To meet the requirement of the company's new password policy, you must configure a minimum length of eight characters for new network passwords.

On a domain controller named DC01, you modify the Default Domain Group Policy Object (GPO). You test the new configuration on your Windows 2000 Professional computer. You can still create two-character password.

You need to ensure that the password policy changes are immediately enforced for all users in the domain. What should you do?

A. On DC01, run the **Secedit/refreshpolicy machine_policy/enforce** command.
B. On DC01, run the **Secedit/refreshpolicy user_policy/enforce** command.
C. Create a new GPO and configure the password policy. Link the new GPO to the organizational unit (OU) that contains all user accounts.
D. Create a new GPO and configure the password policy. Link the new GPO to the organizational unit (OU) that contains all computer accounts.

Answer: B
Explanation: The **secedit /refreshpolicy user_policy /enforce** command immediately applies the GPO for all the appropriate users. Here it applies to all users in the domain, since the GPO is the Default Domain Group Policy object.

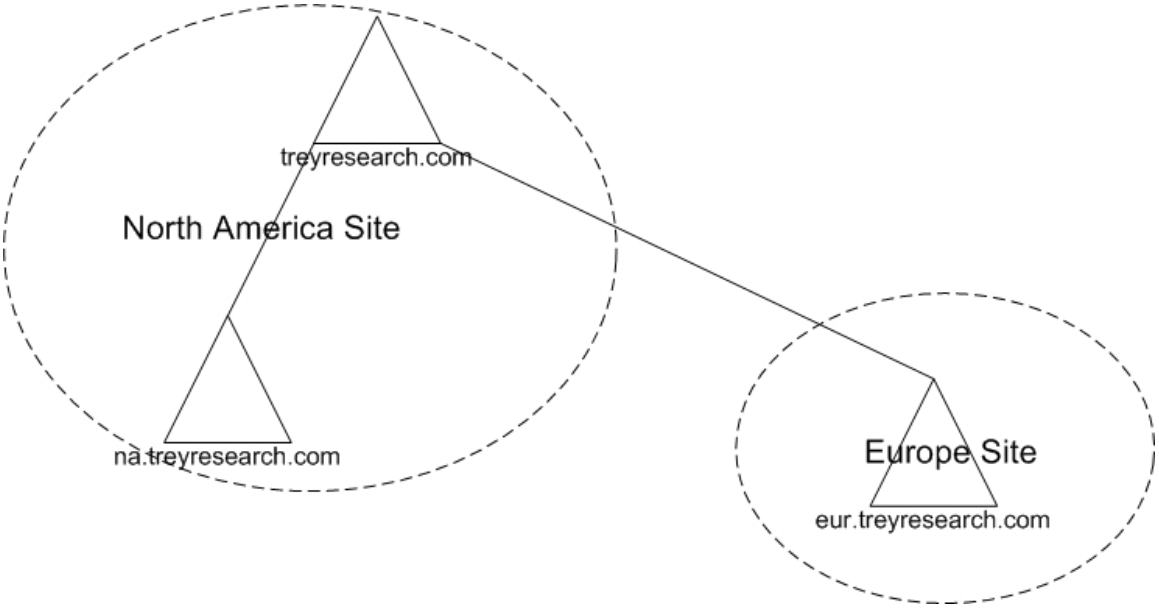
Note: Windows 2000 Domain Controllers refresh to other Windows 2000 Domain Controllers at 5 minute intervals. Non-DC Windows 2000 computers are refreshed every 90 minutes.

Reference: Using SECEDIT to Force a Group Policy Refresh Immediately (Q227302)

Incorrect answers:
A: The requirement is to apply the password policy for all users, not all computers.
C: Password polices must be applied at the Domain level, not at OU level.

D: Password polices must be applied at the Domain level, not at OU level.

Q. 55
You are an enterprise administrator for Trey Research, a company that is based in Los Angeles. The network consists of three Windows 2000 domains in two sites, as shown in the exhibit.



Trey Research anticipates company growth of up to 200 percent during the next 12 months, and plans to add as many as three new sites and four new child domains to the network during that time.

Company IT policy dictates that user account and password security policy settings must be applied consistently to all users throughout the company. You configure the Group Policy Object to the treyresearch.com domain as shown in the following table:

GPO name	Linked to	Settings/restrictions	Options
Enterprise Security	Entire domain	Accounts locked out after three bad logon attempts. Administrator must unlock locked user accounts. Minimum password length is eight characters. Passwords must meet complexity requirements. Minimum password age is 27 days. Maximum password age is 30 days. Remember last 12 passwords.	(None selected)

You later discover that the settings that defined in the Enterprise security GPO are being applied to users located in only the treyresearch.com domain. You need to ensure that these settings are applied to all users in the company.

What should you do?

A. Delete the Default Domain GPO in the child domains.
B. Enable the **No Override** option for the Enterprise Security GPO.
C. Create a new site that contains all domains, and link the Enterprise Security GPO to the site.
D. Create and link new GPOs in the child domains with the same settings as in the root domain.

Answer: D
Explanation: Group Policy that is associated with one domain does not automatically propagate to other domains in the forest. A domain acts as security boundary. For a Group Policy from one domain to be associated with another domain, it must be explicitly linked.

Note: Account policy contains Password policy, Account policy, and Kerberos policy.

Reference: Configuring Account Policies in Active Directory (Q255550).
Domain Security Policy in Windows 2000 (Q221930)

Incorrect answers:
A: It is possible to delete the Default Domain GPO in the child domains. This would not, however solve the problem.
B: A domain acts as security boundary. For a Group Policy from one domain to be associated with another domain, it must be explicitly linked.
C: Domain account policies cannot be applied to sites. The GPO must explicitly be linked to all domains.

Q. 56
You are the administrator of a Windows 2000 Server computer named ServerA. You install Terminal Services on serverA in remote administration mode. You use Terminal Services to administer ServerA for four months.

After four months, you reinstall Terminal Services in application server mode. You install and configure eight user applications on ServerA, and the users in your company being connecting to serverA by using Terminal services client software.

Three months later, users report that they cannot connect to ServerA. You discover that you cannot connect to ServerA by using an administrator user account. You verify that serverA is running properly and is connected to the network.

You need to ensure that users and administrators can connect to ServerA. What should you do?

A. Modify the default Terminal Services user properties so that all domain user accounts have permission to connect to Terminal Services.
B. In Terminal Services Configuration, delete and re-create the default RDP-RCP connection
C. Install and configure a Terminal Services Licensing server on your network. Configure ServerA to use the new licensing server.
D. Ask a domain administrator to relocate ServerA's computer account into an Organizational Unit (OU) named AuthorizedTerminalServer.

Answer: C
Explanation: Terminal Services administration mode doesn't require any licensing. Terminal Services application server mode requires licensing. You are allowed to run Terminal Services in application server mode for 90 days without using any license. If you have not enabled the license service when this period ends, your Windows 2000 Terminal Services will fail to operate. This is what happened in the scenario. After a Terminal Services Licensing server has been set up and you have obtained a new license the Terminal Server would start to run again.

Incorrect answers:
A: This is a licensing problem, not a permissions problem. The server has been running for 3 months without any permission problems.
B: This is a licensing problem, not a Remote Desktop Protocol (RDP) protocol problem. The server has been running for 3 months without any problems.
D: To make the Terminal Server run you must set up a license for it. The 90 day trial period is over.

Q. 57
You are the administrator of four Windows 2000 Server computers in the sales department. Each server has a single Pentium III-600 processor, 192 MB of RAM, and a single 30-GB hard disk. All computers have 100-Mbps network adapter cards.

Users in the sales department report that when they attempt to access files or submit print jobs to a server named ServerA, performance becomes very slow. You use system Monitor to monitor ServerA and discover the information that is shown in the following table:

Object	Counter	Average	Minimum	Maximum
Processor	% Processor Time	25%	4%	100%
System	Processor Queue Length	0.038	0.000	2
Memory	Pages/sec	5.657	0.000	95.703
Memory	Available Mbytes	65.981	64.000	67.000
Physical Disk	Avg. Disk sec/Transfer	2.231	0.000	4.003

Physical Disk	**Disk Queue Length**	**0.793**	**0.000**	**1.861**
Server	**Bytes Total/sec**	**12.787**	**0.000**	**252.560**
Network Interface	**Bytes Total/sec**	**241.552**	**0.000**	**9640.316**

You need to improve the performance of ServerA for the users in the sales department. What should you do?

A. Upgrade or replace the RAM in the server.
B. Upgrade or replace the hard disk in the server.
C. Upgrade or replace the processor in the server.
D. Upgrade or replace the network adapter card in the server.

Answer: B
Explanation: The single counter that is indicating a performance problem is the **Avg. Disk sec/Transfer** counter. The value of this counter indicates that average disk transfer time is 2.231 seconds. A value below 0.3 would indicate normal behavior. There might be some physical problem with the hard disk and it should be replaced.
Reference: Technet Windows 2000 Server Resource kit: Performance Monitoring

Incorrect answers:
A: An average Pages/Sec with 20 or above (here 5.657) would indicate that the system would require more memory.
C: The processor is not overloaded. The processor would be overloaded if the average % Processor Time counter is over 85% (here 20%) or when the Processor Queue Length consistently has a value of 4 or above.
D: There is no indication of any problems with the Network Interface card.
The **Server:Bytes Total/sec** counter shows the number of bytes the server has sent to and received from the network. An average value of 12.787 is normal.
The **Network Interface:Bytes Total/sec** how busy the network interface card is. An average value 241 is normal.

Q. 58
You are a network administrator for your company. The network consists of a single network subnet. The network contains a Windows 2000 Server computer named serverA, which runs the DNS server service. All client computers run Windows 2000 Professional, and they are configured with static IP addresses. The client computers are configured to use ServerA for DNS name resolution.

Another administrator, named Peter, installs Windows 2000 Server on a new computer named ServerB. He installs the DNS server service and the DHCP server service on ServerB. Peter configures the DHCP

server to issue dynamic IP addresses to client computers. He also configured the DHCP server to configure client computers to use ServerB for DNS name resolution.

You reconfigure all client computers to use DHCP to obtain IP addressing information, and you uninstall the DNS server service from ServerA.

All users now report that they cannot access any network resources by name. You need to ensure that users can access network resources by name.

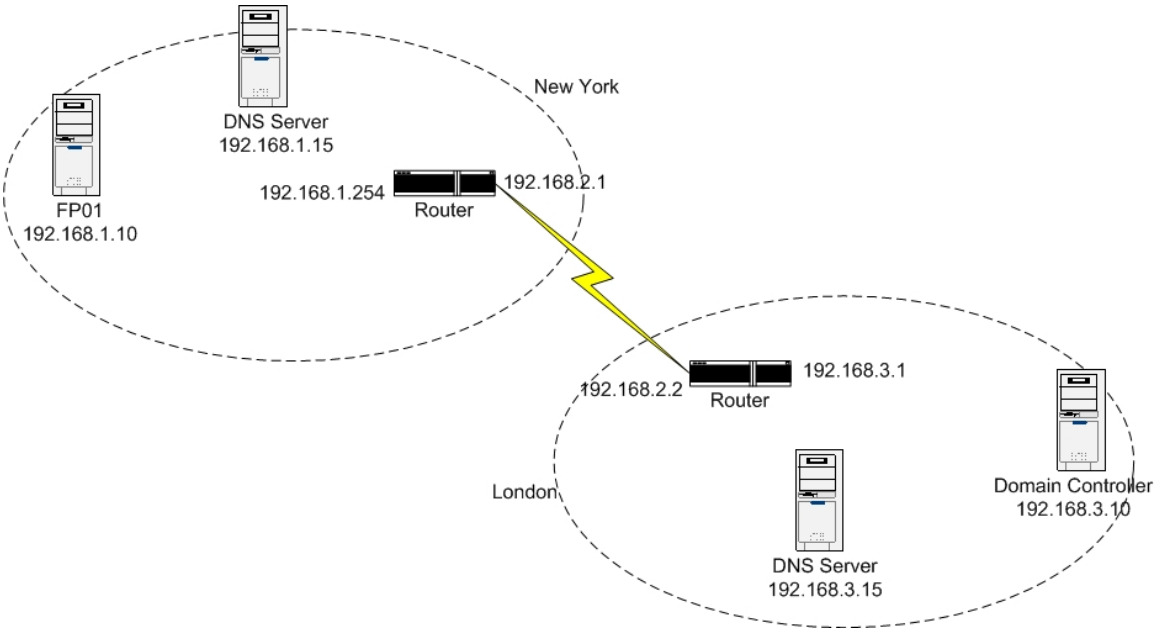
What should you do?

A. Configure the DNS server on ServerB to include a static A (host) record that contains the name and IP address of ServerA.
B. Run the **ipconfig/registerdns** command on each client computer.
C. Delete the Hosts file on each client computer.
D. Reconfigure each client computer to remove ServerA's IP address from the list of DNS servers and to obtain a list of DNS servers automatically.

Answer: D
Explanation: On the clients we have changed the TCP/IP configuration so that the IP address and network mask are to be received dynamically instead of a static configuration as earlier. We must also change TCP/IP configuration on the clients to **Obtain DNS server address automatically**. The clients are still configured to use the old DNS server at ServerA.

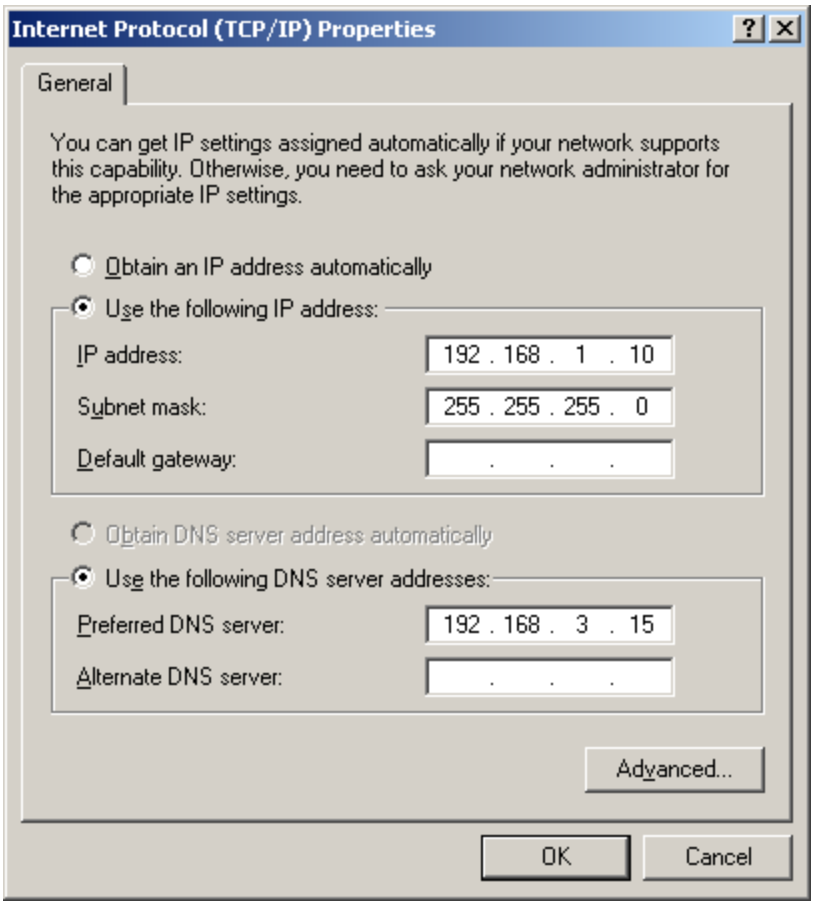
Incorrect answers:
A: There would be no point in adding a host record for the ServerA at the DNS serverB. The DNS service has been uninstalled on ServerA.
B: The clients are still configured to use, the now nonexistent, DNS ServerA. The clients would try register at ServerA when they run the **ipconfig/registerdns** command.
C: Deleting the hosts file, which doesn't seem to be used, would not change the basic problem: the clients must be configured to use ServerB as DNS server.

Q. 59
You are a network administrator for your company. The network is configured as shown in the Network exhibit.



You view the system log of FP01 and notice a large number of identical warning messages that state the following: "The redirector was unable to initialize security context or query context attributes."

The IP properties for FP01 are shown in the IP Properties exhibit.



You need to prevent these warning message form occurring. What should you do?

A. Configure the default gateway for FP01 to 192.168.1.254
B. Configure the default gateway for FP01 to 192.168.2.1
C. Configure the primary DNS server for FP01 to 192.168.1.15
D. Configure the primary DNS server for FP01 to 192.168.3.15

Answer: A
Explanation: The error message indicates a security problem. FP01 cannot connect to a Domain Controller. FP01 is not able to communicate with the domain controller (or the remote DNS server), which is located in the remote network in London.
In order for computers to access resources outside their local segment the Default Gateway setting must be configured. The Default Gateway IP address should be set the IP address of the local interface of the Router; in this scenario it should be set to 192.168.1.254.

Incorrect answers:

B: The IP address 192.168.2.1 corresponds to the external interface on the Router. The IP address of the local interface on the Router, 192.168.1.254, must be used.
C: Changing the preferred DNS server to 192.168.1.15 would not be a bad idea. It is better to use the local DNS server instead of the remote DNS server, but the default gateway should still be configured.
D: The preferred, or primary, DNS server is already configured to be 192.168.3.15.

Q. 60
You are a domain administrator for your company. The network consists of a single Active Directory domain. The network contains 10 Windows 2000 Server computers and 200 Windows 2000 Professional computers. A server named ServerA has routing and remote access installed and is configured for incoming dial-up connections.

Five employees will be traveling overseas. They need to be able to dial in to ServerA while they are traveling. The employees will be using Windows 2000 Professional portable computers to dial in to the network.

You need to ensure that the dial-in connections on the portable computers are as secure as possible. Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

A. Configure ServerA to require EAP-CHAP authentication.
B. Configure ServerA to require MS-CHAP v2 authentication.
C. Configure ServerA to require L2TP connections for all dial-in users.
D. Configure ServerA to require Microsoft Point-to-Point Encryption (MPPE) for all dial-in users.
E. Install a server encryption certificate on ServerA and enable IPSec.
F. Install an encryption certificate on all client computers and enable IPSec

Answer: C, E, F
Explanation: We enable IPSec and create certificates at both the server and the clients. Then we configure the Server for L2TP. L2TP is required for IPSec.

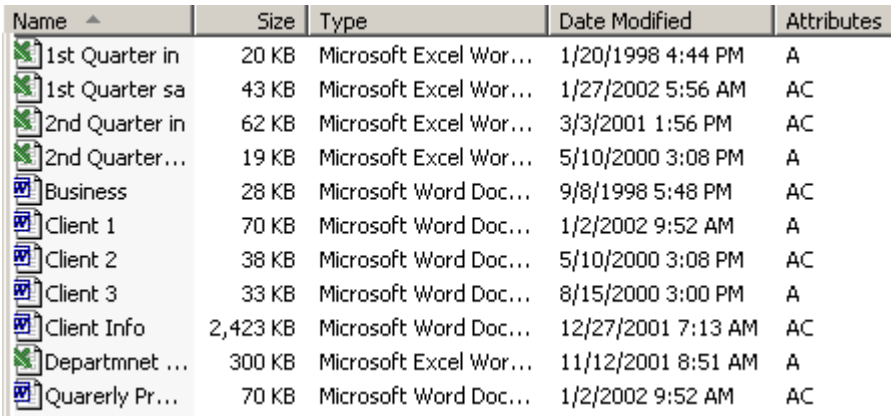
Incorrect answers:
A: There is a protocol EAP-CHAP, but Windows 2000 doesn't support it. Windows 2000 supports EAP-TLS.
B, D: MS-CHAPV2 with MPPE encryption is also secure. It is the next best solution.

Q. 61
You are the administrator for one of your company's branch office. All of the company's file servers have indexing enabled, with the default values.

A user named Maria is responsible for document archiving and retrieval Maria must log the files as she archives them.

A new partition has been created on one of the file servers for archiving and retrieval. A portion of the drive space on this partition is used for other purposes. A shared folder has been created on the partition. Users place files to be archived in this shared folder.

Maria logs the appropriate files and moves them to a compressed folder on the partition. The folder is named Archive. A portion of the contents of the archive folder is shown in the exhibit.



Name	Size	Type	Date Modified	Attributes
1st Quarter in	20 KB	Microsoft Excel Wor...	1/20/1998 4:44 PM	A
1st Quarter sa	43 KB	Microsoft Excel Wor...	1/27/2002 5:56 AM	AC
2nd Quarter in	62 KB	Microsoft Excel Wor...	3/3/2001 1:56 PM	AC
2nd Quarter...	19 KB	Microsoft Excel Wor...	5/10/2000 3:08 PM	A
Business	28 KB	Microsoft Word Doc...	9/8/1998 5:48 PM	AC
Client 1	70 KB	Microsoft Word Doc...	1/2/2002 9:52 AM	A
Client 2	38 KB	Microsoft Word Doc...	5/10/2000 3:08 PM	AC
Client 3	33 KB	Microsoft Word Doc...	8/15/2000 3:00 PM	A
Client Info	2,423 KB	Microsoft Word Doc...	12/27/2001 7:13 AM	AC
Departmnet ...	300 KB	Microsoft Excel Wor...	11/12/2001 8:51 AM	A
Quarerly Pr...	70 KB	Microsoft Word Doc...	1/2/2002 9:52 AM	AC

Maria has Read and Modify permissions for the Archive folder. The files are backed up on tape and the tape is stored off site. Maria reports that she is running out of space on the partition. You will not be able to purchase hardware during the next three months.

You need to free up space on the partition. What should you do?

A. Enable offline caching of files on the partition.
B. Disable indexing of the partition.
C. Configure a scheduled task to defragment the partition on a weekly basis.
D. Configure a scheduled task to compress the files on the partition on a nightly basis.

Answer: D
Explanation: By looking at the exhibit we see that not all files are compressed. Not all files have the C, compressed, attribute. By compressing all the files on a nightly basis a lot of space would be freed up.

Incorrect answers:
A: Enabling offline caching will not free up disk space.

B: Indexing requires data structures to keep the indexes. This takes disk space. By disabling indexing disk space would be freed up. However, much more space would be freed up if all the files on the partition were compressed.
C: Defragmenting will not free up disk space.

Q. 62
You are a network administrator for your company. The network consists of a single Windows 2000 Domain. All client computers run Windows 2000 Professional and are members of the domain.

Peter is a user in the graphics department. He connects a print device to his computer. He wants other users in the graphics department to be able to find the printer in the directory and to use it to print documents from the network.

Peter reports that neither he nor any other users can find the printer in the directory and that no remote users can submit print jobs. Peter can print documents locally.

You need to ensure that Peter and other users in the graphics department can find the printer in the directory and can print documents from the network. What should you do?

A. In the printer properties, share the printer on Peter's computer.
B. In the printer properties, assign the Everyone group the **Allow-Print** permission.
C. In Active Directory users and Computers, add the printer as a child object to Peter's computer object.
D. In Active Directory users and Computers, select the **Trust computer for delegation** check box in Peter's computer properties.
E. In Active Directory Users and Computers, assign users in the graphics department the **Allow-Read Public Information** permission for Peter's computer object.

Answer: A
Explanation: Simply sharing a printer on a Windows 2000 Professional computer that is part of the Domain will publish the printer in the Active Directory automatically.

Note: Printers on non–Windows 2000 print servers must be published manually in Active Directory.

Incorrect answers:
B: The Everyone group gets **Allow-Print** permission by default when the printer is shared.
C: Peter must share the printer first. The printer you want to publish must be shared.
D: Peter must share the printer first. Peter's computer doesn't need the **Trust computer for delegation** rights in order to share and publish the printer in the Active Directory.

E: Peter must share the printer. Users don't have to assigned **Read Public Information** permission on Peter's computer in order to use a shared printer.

Q. 63
You are the desktop administrator for your company. You need to configure one of the computers in a dual-boot configuration for Windows 98 and Windows 2000 Professional.

The computer has a single hard disk that is partitioned into two primary partitions. The first partition is the system partition for both operating systems, and it is 3 GB in size. The second partition is for data, and its also 3 GB is size.

You need to configure the computer so that both operating systems will function properly and will be able to access all of the space on both partitions. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Format the system partition as FAT.
B. Format the system partition as FAT32.
C. Format the system partition as NTFS.
D. Format the data partition as FAT.
E. Format the data partition as FAT32.
F. Format the data partition as NTFS.

Answer: B, E
Explanation: FAT32 can be used both by Windows 98 and by Windows 2000.

Incorrect answers:
A: FAT32 is preferred to FAT.
C: Windows 98 cannot access or be installed on NTFS partitions.
D: FAT32 is preferred to FAT.
F: Windows 98 cannot access NTFS partitions.

Q. 64
You are the administrator of a Windows 2000 file server named ServerA. ServerA is a member of a Windows 2000 Domain. A folder on ServerA named I:\Data\ServerAdmins is shared as ServAdmin. NTFS and share permissions are configured as shown in the following table:

Folder	Share name	Share permission	NTFS permission for folders and files

I:\Data\ServerAdmins	**ServAdmin**	**Everyone-Full Control**	**Local administrators-Full Control**

Users in the built-in Domain Admins group have persistent mapped drives to ServAdmin.

You do not want users to see the shared folder when they type \\ServerA from the Run command or when they browse the network. You want domain administrators to be able to access the resources that are in the folder.

What should you do?

A. Stop and disable the Computer Browser service on ServerA by using Computer Management
B. Modify the share permissions to assign only the Local Administrators group the **Allow-Full Control** permission.
C. Publish ServAdmin in Active Directory. Assign permissions for the published shared folder to only the Domain Admins group.
D. Re-create ServAdmin as ServAdmin$. Instruct the users in the Domain Admins group to delete and then re-create their persistent mapped drive connections to ServAdmins$.

Answer: D
Explanation: By adding a $-sign to the end of a share name the share will be hidden. No one will see a hidden share or be able to browse to this hidden share.

Incorrect answers:
A: Disabling the computer browser on ServerA would only disable browsing from the server. It would not prevent browsing (or the Run\\ command) from the clients. The ServAdmin share would still be visible for users.
B: Changing NTFS permissions in any way whatsoever would not make the share hidden.
C: Changing Share permissions in any way whatsoever would not make the share hidden.

Q. 65
You are the administrator of your company's Windows 2000 file servers. There are 200 users in the company.

A file server named ServerA functions as a file and print server. ServerA has a single partition that stored home folders and other shared user data.

You configure quotas for all users' home folders. After you configure quotas on ServerA, users report that they are being prevented from creating new files in their home folders even though their home folders do not exceed the quota limit.

You need to enforce quota limits based only on home folder usage. You need to accomplish this task with the least amount of administrative effort.

What should you do?

A. Place all of the home folders on a single, separate partition and configure quotas on the new partition.
B. Create a unique partition for each user's individual home folder and configure quotas on each partition.
C. Assign the users the **Allow-Take Ownership** permission for their home folders and then instruct the users to take ownership of their home folders.
D. Create a quota entry for each individual user.
E. Share each home folder separately.

Answer: A
Explanation: Quotas are calculated per user and partition basis. By creating a separate partition for the home folders only the files in the home folder would count towards their quota.

Incorrect answers:
B: It is not necessary to create a partition for each single user. Quotas are calculated per user and partition basis.
C: Taking ownership of their home folders would increase their quota in any way. It wouldn't enable them to save more files.
D: Creating separate quota entries is only useful if you want different users to have different quota limits.
E: Quotas are calculated per user and partition basis. Shares don't increase or decrease the quota for any user.

Q. 66
You are the administrator of a Windows 2000 file server named ServerA. ServerA is a member server in a Windows 2000 Domain. You create a fold named H:\EmployeeHandbook on a volume that is formatted as NTFS. You share the folder as EmployeeHandbook$.

You want users of Windows 2000 Professional computers to be able to search the network for the share by name. You want the users to be able to find the share without needing to know the name of the server.

What should you do?

A. Run the net share **EmployeeHandbook$** command on a domain controller.
B. Publish the share in Active Directory by using Active Directory Users and Computers.

C. Run the **dcpromo** command on ServerA.
D. Create a virtual directory for the folder with an alias of EmployeeHandbook.

Answer: B
Explanation: It is possible to publish a hidden share in the Active Directory. This share could then be accesses through Active Directory; you could search for it. It would still be hidden in Windows Explorer or in My Network places for example.

Reference: Publishing a Shared Folder in Windows 2000 Active Directory (Q234582)

Note: By adding a $-sign to the end of a share name the share will be hidden. No one will be able to see a hidden share or be able to browse to the hidden share.

Incorrect answers:
A: Running the command net share **EmployeeHandbook$** on the domain controller would make the domain controller try to share the folder **EmployeeHandbook** as a hidden share. This would must likely fail and would not be helpful even if it succeeded.
C: Make ServerA a domain controller would be a drastic step and it would still not help. The share would still be hidden.
D: Virtual Directories can be created in Internet Information Services (IIS), but not in Windows 2000.

Q. 67
You are the administrator of a Windows 2000 file server named ServerA. ServerA is a member of a Windows 2000 Domain. You create a folder named I:Data on ServerA. In I:\Data, you create a subfolder for each of your company's 200 departments.

You want the users in each department to have full access to only their department's folder. You want to configure and manage this access with the least amount of administrative effort.

What should you do?

A. I:\Data
Configure share permissions to assign the Everyone group the **Allow-Full Control** permission.
Configure NTFS permissions for each department's folder to assign the **Allow-Full control** permission to the group that contains that department's users.

B. I:\Data
Configure share permissions to assign the Everyone group the **Allow-Read** permission only.
Configure NTFS permissions for each department's folder to assign the **Allow-Full control** permission to the group that contains that department's users.

C. Share each department's folder.
Configure share permissions to assign the **Allow-Full Control** permission to the group that contains that department's users.
Configure NTFS permissions for each department's folder to assign the **Allow-Full control** permission to the group that contains that department's users.

D. Share each department's folder.
Configure share permissions to assign the **Allow-Full Control** permission to the group that contains that department's users.
Configure NTFS permissions for each department's folder to assign the Everyone group the **Allow-Full control** permission.

Answer: A
Explanation: We create one single share and give Everyone Full Share permissions. Then we assign Full NTFS Permissions on each Departmental folder only to the corresponding people from that apartment.
This would require the users to browse and open one map, compared to sharing their departmental folder, but it is the least administrative effort which was a requirement in this scenario.

Note: The calculation of effective permission on a share can be done by:

1. Calculate the NTFS permissions. They are accumulative except for DENY that overrides all permissions.
2. Calculate the Share permission. They are accumulative.
3. Combine the calculated NTFS and Share permissions. The result is the most restrictive permission.

Incorrect answers:
B: With only the share permission of read no user would be able to change anything. They must have full share permission.
C: We only need one share, not a share for each department's folder.
D: We only need one share, not a share for each department's folder.

Q. 68
You are the administrator of a Windows 2000 file server named ServerA. ServerA is a member of a Windows 2000 Domain. A folder on ServerA named I:\data\LimitedPublic is shared as LimPub. NTFS and share permissions are configured as shown in the following table:

Folder	Share name	Share permission	NTFS permission for folders and files
I:\Data\LimitedPublic	LimPub	Everyone-	Everyone-Full Control

		Read	

You want all users who have a valid domain account to be able to create files in the folder and to be able to subsequently update the files that they create. You want to prevent users from accessing other users' files, but you want to allow the creator of a file to assign access for that file to other users.

Users report that they can access LimPub, but they cannot create files in the folder.
You need to configure permissions to allow appropriate access to the folder. What should you do?

A. Configure share permissions to assign the Everyone group the **Allow-Change** permission. Configure NTFS permissions for the folder to assign the Everyone group the **Allow-Write** permissions for the folder to assign the Creator Owner group the **Allow-Full Control** permission.
B. Configure share permissions to assign the Everyone group the **Allow-Change** permission. Configure NTFS permissions for the folder to assign the Everyone group the **Allow-Create/Write Data** permission and to assign the Creator Owner group the **Allow-Full Control** permission.
C. Configure share permissions to assign the Everyone group the **Allow-Full Control** permission. Configure NTFS folder permissions for the folder to assign the Everyone group the **Allow-Create Files/Write Data** permissions and to assign the Creator Owner group the **Allow-Full Control** permission.
D. Configure share permissions to assign the Everyone group the **Allow-Full Control** permission. Configure NTFS folder permissions for the folder to assign the Everyone group the **Deny-Read** permission and to assign the Creator Owner group the **Allow-Full Control** permission.

Answer: C
Explanation: In order to change file permissions on a created file the user must have full NTFS permission and full share permission to the file. We achieve this by giving everyone full share permission, and only the Creator Owner group full control. We must also allow users to create files and we accomplish this by assigning all users the NTFS Create/Write Data permission.

Note: The calculation of effective permission on a share can be done by:

1. Calculate the NTFS permissions. They are accumulative except for DENY that overrides all permissions.
2. Calculate the Share permission. They are accumulative.
3. Combine the calculated NTFS and Share permissions. The result is the most restrictive permission.

Incorrect answers:
A: The share permission must be set to full control to everyone.
B: The share permission must be set to full control to everyone.
D: The Everyone group is Denied Read permission to the folder. Since Deny overrides all permission no one would be able to read files in folder.

Q. 69
You are the administrator of your company's Internet Web Server. The web server is a Windows 2000 Server computer that hosts several Internet Web Sites, including the company's public internet Web site.

You want to allow employees to download company documents from the web server when the employees are away from the office. Employees will access the web server by using Microsoft Internet Explorer.

You want to ensure that security of each employee's network user name and password when the employees are accessing the documents. You also want to ensure that only employees can access the documents. What should you do?

A. Create an FTP site and configure it to use only anonymous user connections.
B. Create an FTP site and configure it to use only Basic authentication for user connections.
C. Create a document Web site and configure it to use only Basic authentication. Then enable directory browsing.
D. Create a document web site and configure it to use only integrated Windows authentication. Then enable directory browsing.

Answer: D
Explanation: We use a document Web site since the users will access it with Internet Explorer. We prefer Integrated Windows authentication since it is a secure authentication method that doesn't transmit usernames or passwords. Instead, it relies on a cryptographic exchange with the server.

Incorrect answers:
A: We cannot allow anonymous access. Anyone could get access.
B: The clients will use Internet Explorer. It would be more convenient for the users if use a Web Site instead of a FTP site.
C: The disadvantage is that Web browsers using Basic Authentication transmit passwords in an unencrypted form.

Q. 70
You are the network administrator for your company's branch office in Chicago. All client computers in the Chicago office run Windows 98. The network in the Chicago office is connected by a T1 line to the network in the main office in New York. Users on the network in the Chicago office access file servers that are located on the network in the New York Office.

The network in the New York office contains a WINS server. All company computers are configured to use the WINS server for name resolution. Managers in the company want to improve name resolution

performance. You are instructed to install and configure WINS on a Windows 2000 Server computer in the Chicago office.

You install WINS on a Windows 2000 Server computer named ServerA. You configure all client computers in the Chicago office to use ServerA for name resolution. All users immediately report that they cannot access servers in the New York office.

You need to ensure that client computers in the Chicago office use ServerA for name resolution. You need to ensure that users in the Chicago office can access servers in the New York office.

What should you do?

A. Create an Lmhosts file on ServerA that includes the name and IP address of the WINS servers in the New York office.
B. Collaborate with an administrator in the New York office to configure WINS replication between ServerA and the WINS server in the New York office.
C. Configure the client computers in the Chicago office to use the WINS server in the New York office as their primary WINS server and ServerA as their secondary WINS server.
D. Ask a domain administrator to add ServerA's computer account to an organizational unit (OU) named AuthorizedWINSServers.

Answer: B
Explanation: By setting up the WINS servers as replication partners they would both be able to resolve NetBIOS names in both Chicago and New York.

Incorrect answers:
A: Using an Lmhosts file for NetBIOS to IP address is awkward. You would have to put the Lmhosts file on all clients as well, not only on ServerA.
C: Using the WINS Server in New York as the primary WINS server would allow the clients to use resources in New York, but it would increase WAN network traffic, and performance would be decreased.
D: There would be no benefit of adding the WINS server to an OU in the Active Directory.

Q. 71
You are a network administrator for your company. The network contains a Windows 2000 Server computer named ServerA, which runs the DNS server service. All client computers on the network use ServerA for name resolution. ServerA is configured to forward name resolution requests to your Internet Service provider's (ISP) DNS server.

A user named Marc uses a Windows 2000 Professional computer on the network. His computer is configured to obtain IP addressing information by using DHCP. He reports that he cannot access a specific internet web site by using the site's URL. However, he can access other web sites. When he attempts to access the specific web site, he receives the following error message: "Server not found or DNS error." You can access the specific web site from your client computer and from other client computers on the network.

You need to ensure that Marc can access the specific web site by using its URL. What should you do on Marc's computer?

A. Stop and restart the DHCP client service.
B. Stop and restart the workstation service.
C. Run the **ipconfig/flushdns** command.
D. Run the **ipconfig/registerdns** command.

Answer: C
Explanation: One possible cause of this problem is an incorrect entry in the DNS client resolver cache. This entry is blocking access to the web site. The **ipconfig/flushdns** command removes all entries from the local DNS name cache.

Incorrect answers:
A: This is a DNS problem not a DHCP problem.
B: The workstation service enables browsing on the network, not on the Internet. Stopping and starting the workstation service would do no good.
D: The **ipconfig/registerdns** command registers, or refreshes, the clients DNS records in at the DNS server. These records are not the cause of this problem.

Q. 72
You are a network administrator for your company. The network consists of a single forest that contains two Windows 2000 Domains named wingtiptoys.com and tailspintoys.com. You administer a Windows 2000 Server computer named ServerA, which run the DNS server service. ServerA is located in a Branch office. The branch office contains computers in both domains.

ServerA contains an Active Directory integrated zone for only wingtiptoys.com. You want ServerA to also locally resolve names for computers in tailspintoys.com

What should you do?

A. Create a secondary zone for tailspintoys.com on ServerA.
B. Create an Active Directory integrated zone for tailspintoys.com on ServerA.

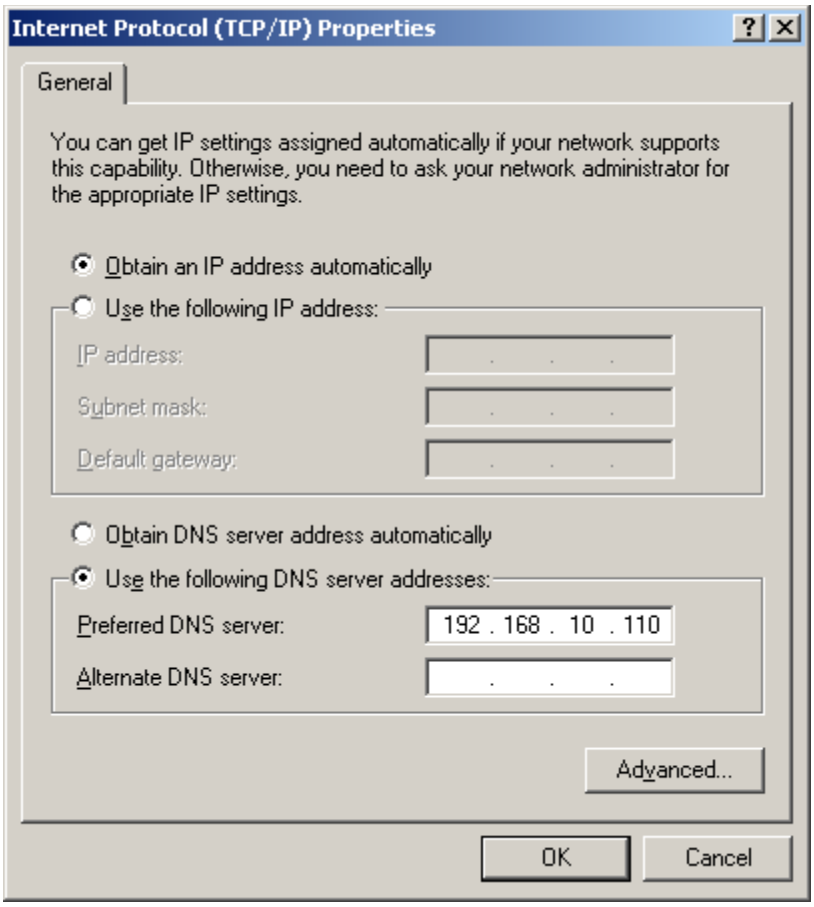
C. Create a primary zone for tailspintoys.com on ServerA.
D. Create a reverse lookup zone for tailspintoys.com on ServerA.

Answer: A
Explanation: In this scenario there already exist two domains. Both domains require DNS to function. We want use ServerA to resolve names for computers in tailspintoys.com. This will be accomplished by creating a secondary zone for the tailspintoys.com zone on ServerA.

Incorrect answers:
B: ServerA belongs to the tailspintoys.com domain. It cannot host an active directory integrated zone belonging to another domain.
C: There already exist a Active Directory integrated zone or a Primary zone for the tailspintoys.com. ServerA cannot be authorative for the tailspintoys.com zone.
D: We must install a forward lookup-zone, not a reverse lookup zone. ServerA cannot be authorative for the zone.

Q. 73
You are a network administrator for your company. The network consists of a single subnet. A DNS server, a DHCP server, and a Windows 2000 Domain controller are configured on the subnet. You do not have permissions on the DHCP server.

You add a new client computer to the network. Andrea is the user of this computer. When Andrea attempts to connect to the domain controller by using the domain controller's host name, she receives the following error message; "The network path was not found." The TCP/IP configuration settings are shown in the exhibit.



You need to configure the new client computer so that Andrea can connect to network resources by using host names. You need to configure the computer with the least amount of administrative effort.

What should you do?

A. In the client computer's Lmhosts file, add an entry for each server.
B. Configure the client computer to obtain the DNS server address automatically.
C. Install the Simple TCP/IP services on the client computer.
D. Configure static IP settings on the client computer.

Answer: B
Explanation: We just have to configure the new client to obtain DNS server address automatically. The DHCP server will provide the correct DNS server address next time the client is restarted or the command IPCONFIG /RENEW is run.

Incorrect answers:
A: Lmhosts files are used for NetBIOS, not host name, to IP address resolution.

It would be awkward to add entries for all computers that have shared resources.

C: Simple TCP/IP services includes Quote of the Day, Echo, Echo and Character Generator. Neither of these services would help resolving host names.

D: Andrea already got a dynamic IP address configured for the network, assuming the DHCP is up and running. Configuring a static IP address would not help Andrea.

Q. 74

You are a network administrator for Contoso Pharmaceuticals. The network consists of a single forest that contains four Windows 2000 domains named contoso.com, domain1.contoso.com, domain2.contoso.com, and domain3.contoso.com. In domain3.contoso.com you administer two Windows 2000 Server computers named ServerA and ServerB. ServerA and ServerB run the DNS server service.

Users on Windows 2000 Professional computers in domain3.contoso.com report that they cannot access resources in domain1.contoso.com. When you escalate the problem to the enterprise administrators, you are informed that the DNS zone for domain3.contoso.com was recently corrupted with erroneous A (host) records. However, after the enterprise administrators correct the A records, users still report that they cannot access resources in domain1.contoso.com

You want users in domain3.contoso.com to be able to immediately access resources in domain1.contoso.com. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Create an Active Directory integrated zone for domain3.contoso.com on Both ServerA and ServerB.
B. Clear the DNS cache on ServerA and ServerB by using the DNS console.
C. Run the **ipconfig/flushdns** command on each user's computer.
D. Run the **ipconfig/release** command on each user's computer.
E. Initiate a scavenging operation of stale resource records on ServerA and ServerB by using the DNS console.

Answer: B, C

Explanation: DNS queries are cached by the resolver in order to reduce network traffic. The resolver can be either the DNS server or a DNS client.

B: The DNS cache at the DNS server may include incorrect entries and should be reset.

C: The local clients have incorrect entries in their DNS client resolver cache. These entries are blocking access to the web site. The ipconfig/flushdns command removes all entries from the local DNS name cache.

Incorrect answers:

A: Creating an Active Directory integrated zone for domain3.contoso.com domain will not help. We need access resources in the domain1.contoso.com.

D: **ipconfig/release** would renew the IP address, but we have a DNS problem not an IP configuration problem.

Q. 75
You are the network administrator for your company's branch office in Chicago. The network in the Chicago office is connected by T1 line to the network in the main office in New York. The network in the New York office contains a Windows 2000 Server computer named NYSrv04, which is a domain controller and hosts an Active Directory integrated DNS zone. All client computers in the New York and Chicago offices use NYSrv04 for name resolution.

The company's network manager decides to place an additional server on the network in the Chicago office to improve network performance. You receive a new Windows 2000 Server computer named CHSrv01 from the main office. CHSRv01 is configured as a domain controller for the company domain and as a DNS server.

You need to configure DNS on CHSrv01 and you need to configure the client computers that are on the network in the Chicago office. You need to ensure that your configuration provides the fastest possible name resolution performance. You need to minimize the amount of DNS traffic sent between the New York and Chicago office.

You configure the client computers in the Chicago office to use CHSrv01 for name resolution. What should you do next?

A. Configure CHSrv01 with a new primary zone, and configure CHSrv01 to forward name resolution requests to NYSrv04.
B. Configure CHSrv01 with a new secondary zone, and configure CHSrv01 to perform zone transfers from NYSrv04.
C. Configure CHSrv01 as a caching-only server, and configure CHSrv01 to forward name resolution requests to NYSrv04.
D. Configure CHSrv01 with an Active Directory integrated zone.

Answer: D
Explanation: To minimize network traffic and to provide fast name resolution we should configure an Active Directory Integrated zone. Compared to a secondary zone it would have the following advantages:

- fast zone transfers
- updates on the local DNS server possible

More advantages exist. The listed advantages decrease network traffic.

Incorrect answers:
A: We must use the existing zone that has been configured on NYSrv04 in New York.
B: A secondary zone would work but would be slower and require more network bandwidth.
C: A caching-only server would be plausible on a slow WAN link, for example on a 56Kbps modem line. A caching-only server avoids zone transfers. In this scenario however we have a T1 (1.44Mbps) line so we don't have to consider a caching-only server.

Q. 76
You are a domain administrator for your company. You install a Windows 2000 Server computer named ServerA. ServerA is a member of the company's Active Directory domain.

You install the DHCP service on ServerA. When you restart serverA, the DHCP service does not start. You want to enable ServerA to start the DHCP service.

What should you do?

A. Configure the DHCP service to use a Domain Administrator account to log on to the domain.
B. Configure the DHCP service to use an Enterprise Administrator account to log on to the domain.
C. Ask a member of the Enterprise Admins group to authorize ServerA as a DHCP server.
D. Ask a member of the local Administrators group to authorize ServerA as a DHCP server.

Answer: C
Explanation: The DHCP server must be authorized in the Active Direcotry. Only Domain Administrators have permission to authorize servers.

Note: The DHCP server typically runs with the Local System Account.

Incorrect answers:
A: The DHCP server should not be run with the Domain Administrator account.
The DHCP server must be authorized.
B: The DHCP server should not be run with the Enterprise Administrator account.
The DHCP server must be authorized.
D: A local administrator would not be able to authorize the DHCP server.

Q. 77
You are an administrator of a Windows 2000 Server computer, which runs the DNS server service. The DNS server is located in one of your company's branch offices. The network in your branch office

contains 100 DNS clients that are all members of the same Windows 2000 Domain. The DNS server is not a member of the domain.

You want the DNS server to perform recursive queries on behalf of the DNS clients for names of hosts that are outside of the domain and on the internet. What should you do?

A. Configure the DNS server to use forwarders to resolve DNS names.
B. Configure the DNS server as a caching-only server.
C. Configure a secondary primary zone on the DNS server for the domain.
D. Configure a primary zone on the DNS server for the domain.

Answer: A
Explanation: The DNS server must be configured to forward queries for external names to an external DNS server, typically the ISP's DNS server.

Incorrect answers:
B: A caching only server would only be able to resolve the queries from the DNS server it uses for name resolution.
C: A secondary zone is just a read-only replica of the primary zone. A secondary zone would not add any name resolving capabilities.
D: We want to resolve names outside the domain. Configuring a primary zone for the domain will not help achieve this goal.

Q. 78
You are the network administrator for your company's branch office. A user named Marc reports that his Windows 2000 Professional computer will not start.

You investigate, and you discover that Marc's computer is displaying the following error message: "Invalid disk or operating system not found." Your computer configuration documentation indicates that Marc's computer is configured as a single NTFS logical volume.

You need to restore Marc's computer to normal operation as quickly as possible. What should you do?

A. Restart the computer by using the Windows 2000 Professional CD-ROM, and select the option for the Recovery Console. Run the **fixmbr** and **fixboot** commands.
B. Restart the computer by using the Windows 2000 Professional CD-ROM, and select the option for the Recovery Console. Run the **enable "Workstation"** command.
C. Restart the computer by using the Windows 2000 Professional CD-ROM, and perform a parallel installation to a different folder on the hard disk

D. Restart the computer by using a floppy disk, and copy the Ntldr file from the Windows 2000 Professional CD-ROM to the root folder of Drive C.

Answer: A
Explanation: We start the recovery console and the use the **fixmbr** command to restore the master boot record, and then the **fixboot** command to restore the boot sector.

Note: The Recovery Console is a command-line interface that can be used to access a hard disk of a Windows 2000 computer system. It can be accessed from the Windows 2000 Professional installation CD-ROM. Boot the computer from the Windows 2000 Professional installation CD-ROM. On the Welcome to Setup screen, click R to open the Repair Options screen, and click C to activate the Recovery Console.

Incorrect answers:
B: This isn't a problem with a service. Starting the Workstation service will not help.
C: We don't have to make another installation just to repair the master boot record and the boot sector.
D: The problem is in the master boot record and in the boot sector (one or both). The error message would tell us if the ntldr file were missing.

Q. 79
You are a network administrator for your company. Users report that an application server named ServerA that runs a customized application is slow to respond. You configure System Monitor on ServerA. The results are shown in the following table:

Counter	Last	Average	Minimum	Maximum
%Disk Time	65	94	15	99
%processor Time	45	10	0	80
Megabytes Total/sec	30	10	4	30
Pages/sec	75	75	5	80

You need to improve the performance of ServerA. What should you do?

A. Add additional RAM to ServerA.
B. Add an additional CPU to ServerA.
C. Add an additional network adapter to ServerA.
D. Add an additional Active Directory domain controller to the network.
E. Upgrade to a faster disk subsystem on ServerA.

Answer: A

Explanation: An average Pages/Sec with 20 or above (here 75) indicates that the system requires more memory.

Incorrect answers:

B: The processor is not overloaded. The processor would be overloaded if the average % Processor Time counter is over 85% (here 10%).

C: The Megabytes Total/sec counter indicates how much network traffic is handled by the network adapter. An average value 10 is normal.

D: An Additional Domain Controller could be considered if either the processor, network card, or the hard disk were overloaded. This is not the case in this scenario.

E: The % Disk Time counter is the percentage of elapsed time that the selected disk drive is busy servicing read or write requests. An average value 90 or above (here 94) would indicate a disk bottleneck. But in this scenario this is not the case since the high %Disk Time value depends on the excessive paging due to lack of RAM. When we increase RAM the %Disk Time would be reduced.

Q. 80

You are a network administrator for your company. The network contains 2,500 Windows 2000 Professional computers, 70 Windows 2000 Server member servers, and 5 Windows 2000 Server domain controllers. All computer accounts are in their default location in Active Directory.

You need to deploy the most recent service pack to all of the computers with the least amount of administrative effort. What should you do?

A. Create a script named Update.bat that runs the Update.exe file from a network share. Create a Group Policy Object and link it to the Computers container. Set the computer configuration to run the Update.bat script on startup. Restart each computer.

B. Create a Group Policy Object and link it to the Domain level. Configure the GPO to assign the Update.msi file under the user configuration logon script. Log on to each computer as Administrator.

C. Create a Group Policy Object and link it to the Domain level. Configure the GPO to assign the Update.msi file under the computer configuration. Restart each computer.

D. Create a Group Policy Object and link it to the Computer container. Configure the GPO to assign the Update.msi file under the computer configuration. Restart each computer.

Answer: C

Explanation: An Update.msi package should be deployed throughout the domain by using a Group Policy deployment. We create a new GPO, link the GPO at the domain level, and configure the GPO to assign the update.msi file under the computer configuration. We then restart the computers. The update.msi file will be applied and the service pack will be installed.

Reference:
Best Practices for Using Windows 2000 Update.msi Package for Service Pack 1 Installation (Q278503)
White Paper, Windows 2000 Service Pack 1 Installation and Deployment Guide
White Paper, Windows 2000 Service Pack 2 Installation and Deployment Guide

Incorrect answers:
A: The script would run every time a computer starts.
B: We should not use a logon script. We should simply assign the Update.msi file.
D You cannot link a GPO to the built-in Computers container.

Q. 81
You are the administrator of a Windows 2000 Server computer named ServerA. The server has dual Pentium II-450 processors, 192 MB of RAM, and two hard disks, which are configured as shown in the following table:

Physical disk	Logical disk	File system	Partition role	Partition size
0	**C**	**NTFS**	**System and boot**	**5GB**
0	**D**	**NTFS**	**Applications**	**25GB**
1	**E**	**NTFS**	**Data storage**	**100GB**

Users report that server performance is acceptable under normal working conditions, such as accessing files and printing documents. However, when a large accounting application is run, performance becomes significantly slower. When the application is processing large amounts of data, users report long waiting periods when they access files stored on the hard disk or when they submit print jobs.

You monitor ServerA by using System Monitor. You discover that when the accounting application is running, the sustained processor utilization on both processors in 100 percent. There are also numerous hard pages faults. When the application is not running, sustained processor utilization drops to 50 percent, but the number of hard pages faults remains high.

You need to improve the performance of ServerA. What should you do?

A. Upgrade the memory in ServerA.
B. Upgrade the processors in ServerA.
C. Move the paging file from the system partition to drive E.
D. Increase the default size of the paging file to at least 384 MB.

Answer: A
Explanation: The numerous hard pages faults indicate that there is a need for more RAM. If we increase RAM the load on the processors would decrease.

Note: Hard page faults are page faults satisfied by the hard disk.

Incorrect answers:
B: The processor is at the extreme high level partly due the excessive page faults. If we increase RAM the load on the processors would decrease.
C: Moving the page file will not decrease the excessive use of it.
D: Numerous hard page faults indicate that the page faults are satisfied by the pagefile on the hard drive. We don't need to increase the size of the page file.

Q. 82
You are a network administrator for your company. A user named Maria reports that her Windows 2000 Professional computer has stopped responding.

You examine the computer and discover that it is displaying a STOP message. Maria reports that the computer has been displaying a STOP message intermittently during the past several days. You restart the computer and it functions normally.

A few minutes later, Maria reports that the computer has stopped responding again. You investigate and discover the same STOP message. The documentation for Maria's computer indicates that a new network adapter card was installed in the computer 10 days ago.

You set up a second Windows 2000 Professional computer for Maria to use. You need to provide access to her original computer so that she can copy three files onto a floppy disk and copy them to the second computer. However, when you restart her original computer, it displays a STOP message after only a few minutes.

You need to provide Maria with access to the files on her original computer. You need to accomplish this task as quickly as possible.

What should you do?

A. Restart the original computer by using safe mode.
B. Restart the original computer by using the last known good configuration.
C. Restart the original computer by using an Emergency Repair Disk.
D. Restart the original computer by using the Windows 2000 Professional CD-ROM, and select the option to repair the installation.

Answer: A

Explanation: We need to get the files on diskette as quickly as possible. By starting the computer in safe mode many device drivers and services will not be loaded. In particular the network adapter driver, which looks like a probable cause of the problems, would not be loaded. In safe mode we would be able to copy the required files to the diskette.

Incorrect answers:
B: The last known good configuration would only restore the computer in the state it had at the previous successful logon which is the same as the current state in this scenario.
C: You cannot start a computer by using an Emergency Repair Disk.
D: Repairing the installation is not a bad idea. But we want to copy the files as fast as possible and repairing the installation could require quite some time.

Q. 83
You are a desktop administrator for your company. All client computers run Windows 2000 Professional.

You are installing a new Plug and Play combination scanner and print device on a user's computer. You connect the print device to the computer's parallel port. However, you discover that Windows 2000 does not detect the new print device.

You open Device Manager on the computer and discover that there is no listing for the printer or for any unidentified devices. You run the Scan for hardware changes command in Device Manager, but no new hardware is detected.

You want Windows 2000 Professional to detect and install drivers for the new print device. What should you do?

A. In the system BIOS, enable Enhanced Parallel Port (EPP) support.
B. In the **Driver Signing Options** dialog box, set File Signature.
C. Use the Add/Remove Hardware wizard to install the manufacturer's printer driver.
D. Turn off the computer, and then turn off the print device, and then turn on the computer.

Answer: A:
Explanation: Windows is unable to detect the plug and play device. We should enable EPP support in BIOS, restart the computer, and attach the device. Windows 2000 would then be able to detect it.

Incorrect answers:
B: Changing Driver signing options would not enable Windows 2000 to find any new hardware devices. Driver signing options are used configure how unsigned drivers will be handled.
C: The device is Plug and Play device so Windows 2000 should have been able to detect it.
D: This is a Plug and Play device. Turning off the computer would not be necessary and it would not help.

Q. 84
You are the administrator of an organizational unit (OU) named Operations. You create a Group Policy Object to publish an application named CorpOps to the users in the Operations OU.

Your company frequently reassigns employees to different departments. When employees are reassigned, their Active Directory user accounts are moved to a different OU. You need to ensure that CorpOps is uninstalled when an employee's user account is moved to a different OU.

What should you do?

A. Write a Microsoft Visual Basic Scripting Edition (VBScript) logoff script that uninstalls CorpOps. Assign the logoff script to the members of the Operations OU.
B. Modify the permissions on the CorpOps installation package so that only members of the Operations OU have the **Read** permission.
C. Configure the Group Policy Object that publishes CorpOps to uninstall the application when it falls out of the scope of management
D. Modify the GPO so that CorpOps is assigned instead of publishes

Answer: C
Explanation: When you originally deploy the software, if you want the application to be removed when a GPO no longer applies, select the **Uninstall This Application When It Falls Out Of The Scope of Management** option.

Incorrect answers:
A: The application should be removed when the users are removed from the OU not when they log off.
B: Modifying the permissions on the package would not, in any magical way, uninstall the application when the users are removed from the OU.
D: Assigning or publishing the application is irrelevant. The application would not be automatically uninstalled.

Q. 85
You are a network administrator for your company. You need to configure offline file settings for all users in the Boston Organizational Unit. You add two new Group Policy Objects named CompGPO and UserGPO and link them to the Boston OU. A representation of the details of the GPOs is shown in the exhibit.

CompGPO

Computer Configuration
- Administrative Templates
  - Network
    - Offline Files
      - Synchronize all offline files before logging off – Enabled
      - Prevent use of Offline Files folder – Enabled
      - Subfolders always available offline – Not Configured

UserGPO

User Configuration
- Administrative Templates
  - Network
    - Offline Files
      - Synchronize all offline files before logging off – Enabled
      - Disable user configuration of offline files – Disabled
      - Prevent use of Offline Files folder – Disabled
      - Administratively assigned offline files – Not Configured

Users report that they cannot synchronize their offline files. You need to ensure that users can synchronize their offline files.

What should you do?

A. Modify the computer configuration for CompGPO by changing the **Prevent use of Offline Files folder** policy to **Not Configured.**
B. Modify the computer configuration for CompGPO by changing the **Subfolders always available offline** policy to **Enabled.**
C. Modify the user configuration for UserGPO by changing the **Administratively assigned offline files** policy to **Enabled.**
D. Modify the computer configuration for CompGPO by changing the **Disable user configuration of offline files** policy to **Enabled.**

Answer: A
Explanation: By examining the exhibit we see that the CompGPO includes the configuration **Prevent use of Offline Files Folder – Enabled**. This setting is preventing the use of offline Files and Folders.

Incorrect answers:
B: **Prevent use of Offline Files Folder** setting would override the **Subfolders always available offline** setting.
C: The CompGPO, not the UserGPO, have to be reconfigured.
D: The **Prevent use of Offline Files Folder**, not the **Disable user configuration of offline files** setting, must be disabled.

Q. 86
You are a member of the Enterprise Admins group for Trey Research. The Active Directory forest consists of a forest root domain named ad.treyresearch.com and two child domains named east.ad.treyresearch.com and west.ad.treyresearch.com. The network consists of four Active Directory sites, with five domain controllers at each site.

You want to restrict the ability to log on locally to all of the domain controllers to members of the local Administrators group. You want to accomplish this goal with the least amount of administrative effort and without affecting other computers in the domain.

What should you do?

A. Create a Group Policy Object that restricts the ability to log on locally to members of the local Administrators group. Link the GPO to the ad.treyresearch.com domain.
B. Create a Group Policy Object that restricts the ability to log on locally to members of the local Administrators group. Link the GPO to the ad.treyresearch.com domain. Enable the **No override** option for the GPO link.
C. Edit the default Domain Group Policy Object in each domain to restrict the ability to log on locally to members of the local Administrators group.
D. Edit the default Domain Controllers Group Policy Object in each domain to restrict the ability to log on locally to members of the local Administrators group.

Answer: D
Explanation: We want to restrict the right to log on locally on the domain controllers. Only local Administrators should have this right. This can be accomplished by configuring the default Domain Controllers Group Policy in each domain.

Note: It is not possible configure GPO at one single place in the domain tree. We must configure it for each domain. Domains functions as security boundaries. Polices will not pass between domains.

Incorrect answers:

A: We must apply the GPO in every domain, not only in the root domain.
B: We must apply the GPO in every domain, not only in the root domain.
C: We should configure the default Domain Controllers GPO in each domain, not the default Domain GPO. We want to restrict logins on the domain controllers, not all computers throughout the domain.

Q. 87
You are the administrator of your company's Active Directory domain. The company recently expanded from one office in London to include new offices in New York and Mexico City. All user accounts for the entire company are currently in the Users container.

Company policy states that network administrators may configure user accounts for only their respective offices. You create an Active Directory group for each of the three offices. The user accounts of the network administrator for each office are members of each respective Active Directory group.

You need to configure Active Directory so that each administrator group can administer the user accounts in only its respective office. What should you do?

A. Run the Delegation of Control wizard at the domain level and delegate the **Full Control** permission to all three of the administrators groups for all child objects.
B. Create a new Organizational Unit for all of the user accounts. Move the user accounts into the new OU. Place all three of the administrators group in the new OU.
C. Create a new organizational unit for each of the three offices. Place each of the three administrators groups in its respective OU. Run the Delegation of Control wizard on each of these OUs and delegate the **Create, delete, and manage user accounts** task to the respective administrators group.
D. Create a new organizational unit for each of the three offices. Move the user accounts to the appropriate OUs. Run the Delegation of Control wizard on each of these OUs and delegate the **Create, delete, and manage user accounts** task to the respective administrators group.

Answer: D
Explanation: We must create OUs for each of the three offices in order to be able to separate the user accounts. After putting each user account in the correct office OU we assign the respective Administrator the appropriate administrative tasks on the OU.

Incorrect answers:
A: We need to put the users into three OUs, one for each office.

B: We need to put the users into three, not one OU, OUs, one for each office.
C: The user accounts, not the administrator's accounts, should be put into the OUs.

Q. 88
You are the desktop administrator for your company. A new shipment of computers arrived recently. These new computers will replace outdated client computers.

You install Windows 2000 Professional on one of the new computers. You attempt to join the computer to the domain. You receive an error message stating that access has been denied.

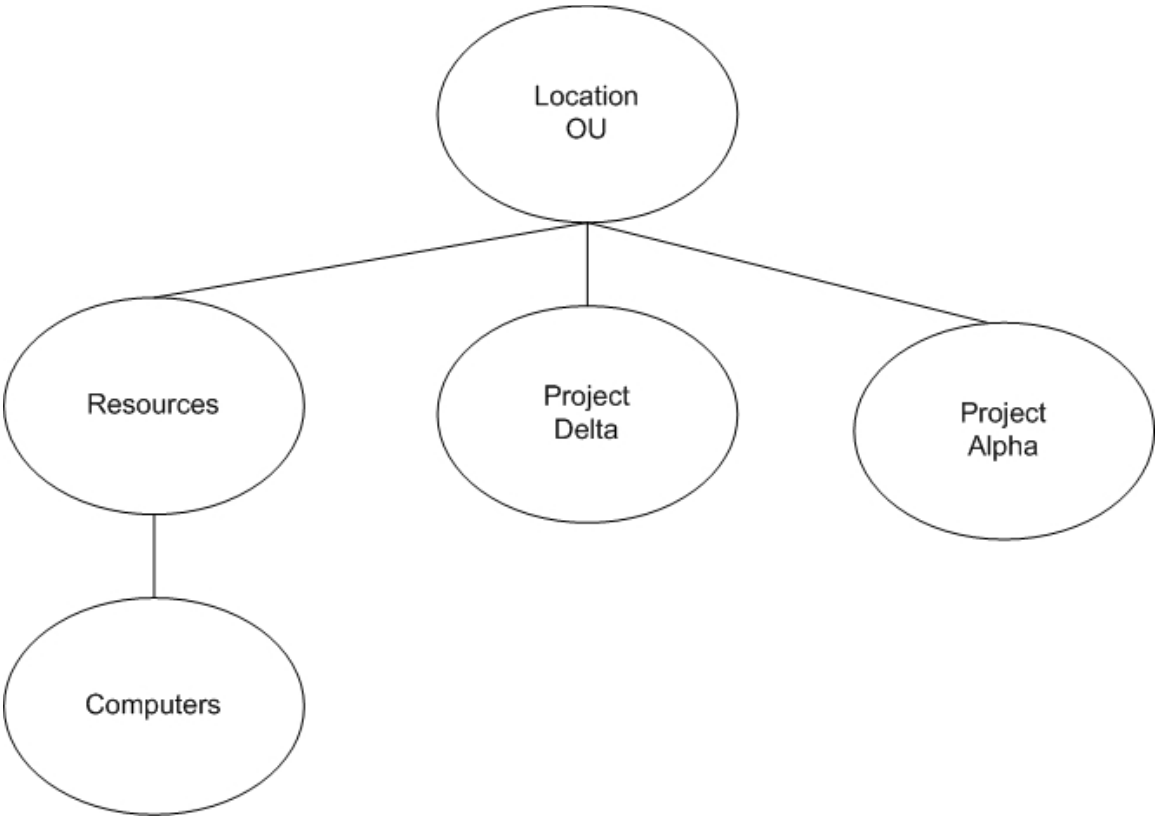
You need to be able to add the new computers to the domain. After you install Windows 2000 Professional on all of the new computers, what should you do?

A. Log on to each computer as local Administrator, and then join each computer to the domain.
B. Obtain permission to create computer objects, and then join each computer to the domain.
C. For each computer, create a computer account in Active Directory, and then join each computer to the domain.
D. Run the **ipconfig/registerdns** command on each computer, and then join each computer to the domain.

Answer: C
Explanation: Computer accounts can be pre-configured in Active Directory. Any user that is able to log on the domain would be able to add the preconfigured computer to the domain.

Incorrect answers:
A: A local administrator would not have permission to join the computer to the domain.
B: The permission to create computer objects would not allow you to join computers to the domain.
D: The **ipconfig/registerdns** command is used to register the client in DNS. But registering the client in DNS would not enable it to join the domain.

Q. 89
You are an organizational unit administrator for your company's Active Directory domain. The top-level OUs in Active Directory are organized by physical location. All OU administrators have permissions to administer only the OUs for which they are responsible. You have organized your OUs and user accounts based on the projects the users are working on. The OU structure is shown in the exhibit.



The OU for your location has a Resources OU under it. The resources OU contains published shared folders and a Computers OU that contains all the computer accounts at your location.

Multiple templates have been created for use with Microsoft Project. These templates are in a file share named Templates that is published to the Resources OU as ProjectTemplates. The ProjectLeads group has permissions for the Template file share. All user accounts in the Project Delta OU are members of the ProjectLeads group and therefore have access to the Templates file share.

You need to ensure that Andrea has access to the Templates file share. What should you do?

A. Delegate control of the Project Alpha OU to the ProjectLeads group.
B. Move Andrea's user account to the Project Delta OU.
C. Assign Andrea the **Allow-Read** permission for the Resources OU.
D. Add Andrea's user account as a member of the ProjectLeads group.

Answer: D
Explanation: The ProjectLeads group has permissions for the Templates file share. Simply adding Andrea to this group would give access to Templates file share.

Reference: Publishing a Shared Folder in Windows 2000 Active Directory (Q234582).

Incorrect answers:
A: Delegating control of an OU would not let a user gain control to a published resource in an OU.
B: Users placed in Project Delta do not have any access to the share.
C: Assigning Andrea read permissions to the Resources OU would let her user account be applied with all GPOs linked to the Resources OU. As far as we know there is no GPO linked to the Resources OU that would give her access to the Template file share. There is a GPO linked the OU which publishes the file share, but Andrea would not be able to access it unless she share permissions to it.

Q. 90
You are the administrator of a Windows 2000 Server computer named ServerA. ServerA runs a custom client/server software application. ServerA is located in your company's New York office.

You install terminal Services on ServerA in remote Administration mode. You can connect to ServerA by using the terminal Services client software installed on your Windows 2000 Professional computer.

A user named Marc is responsible for supporting the client/server application on ServerA. Marc needs to perform administrative tasks on ServerA. Marc is located in your company's London office.

You need to ensure that Marc can connect to ServerA by using Terminal Services. You also need to ensure that Marc does not receive any unnecessary administrative privileges on other servers in your company.

What should you do?

A. Ask a domain administrator to add Marc's domain user account to the Domain Admins user group. Install the Windows 2000 administrative tools on Marc's client computer.
B. Create a local user account named Marc on ServerA. Install the Windows 2000 administrative tools on Marc's client computer.
C. Ask a domain administrator to grant Marc's domain user account permission to connect to Terminal servers. Instruct Marc to use Terminal Services to connect to ServerA, and to log on by using his domain user account.
D. Create a local user account named Marc2 on serverA. Instruct Marc to use Terminal Services to connect to serverA, and to log on by using the Marc2 user account
E. Add Marc's domain user account to the local Administrators group on ServerA. Instruct Marc to use Terminal Services to connect to ServerA, and to log on by using his domain user account.

Answer: E

Explanation: Marc must be able to perform administrative tasks only on ServerA, not on any other servers in the domain. By adding Marc's domain user account to the local Administrators group on ServerA he would be able to perform the required tasks.

Incorrect answers:
A: Adding Marc to the Domain Admins group would, unnecessarily, give him domain administrator permissions and rights.
B: Marc should connect to the server using terminal services, not with Windows 2000 Administration tools. The Windows 2000 Administration tools would enable Marc to administer the server, but we want Marc to run the client/server application on ServerA. It would not be able to do it with the Windows 2000 Administration tool.
C: Marc should not have permissions to connect to all Terminal servers, only to ServerA..
D: Creating a local account for Marc on ServerA would give him access to the server. He would not be able to perform the required administrative tasks (the client/server application) on ServerA though.

Q. 91
You are a domain administrator for your company. The network consists of a single Active Directory domain. The network also contains a Windows 2000 Server computer named ServerA. ServerA has Routing and Remote Access installed and is configured for incoming dial-up connections. Employees use Windows 2000 Professional portable computers to dial in to the network.

You configure a remote access policy that allows members of the Domain Users group to dial in to ServerA between 7:00 A.M and 7:00 P.M every day. To increase dial-up security, the company issues smart cards to all employees.

You need to configure ServerA and the remote access policies to support the use of the smart cards for dial-up connections.
What should you do?

A. Create a remote access policy that requires users to use SPAP for authentication.
B. Create a remote access policy that requires users to use EAP-TLS for authentication.
C. Create a remote access policy that requires users to use MS-CHAP v2 for authentication.
D. Install the Internet Authentication Server (IAS) on ServerA.

Answer: B
Explanation: To be able to use the smart cards we must use the EAP-TLS authentication protocol.

Incorrect answers:
A: SPAP cannot be used for smart card authentication.
C: MS-CHAP v2 cannot be used for smart card authentication.

D: IAS is used to centralize administration and authentication when using several RRAS servers. It would not, by itself, enable support for smart card authentication.

Q. 92
You are the administrator of some of your company's Windows 2000 file servers. The company recently implemented disk quotas.

On one of your file servers, you successfully configure a single quota for all users. However, after further inspection within the Quota Entries Window, you notice that users who have exceeded their quotas can still save files to the server.

You need to ensure that the quota limits prevent each user from saving files to the server after the users' quota limits are met or exceeded. What should you do?

A. Run the **Secedit/configure** command on the server to enforce the Basicws.inf security template.
B. Configure a quota entry for each user individually.
C. Enable the enforcement of quota limits.
D. Upgrade the hard disks on the server to dynamic disks.

Answer: C
Explanation: Enabling quotas would not by itself limit the users from exceeding the predefined limit. We must configure the quota entry to enforce the quota limit.

Incorrect answers:
A: Enforcing the Basicws.inf security template would restore the security settings on the server to the default security setting. It would not affect the quota so that the quota limit would be enforced.
B: The only reason to configure a quota entry for each user would be to have the possibility to give the users different quota limits.
The quota limit must be enforced.
D: Quota can very well be used on basic disks. Upgrading the hard disks to dynamic disks would not enforce the quota limit.

Q. 93
You are the evening-shift administrator of a Windows 2000 Server computer. The server hosts shared files. The server is configured as a single NTFS logical volume.

The day-shift administrator reports that the server displayed a STOP message earlier in the day. The day-shift administrator restarted the server, which resulted in the same STOP message. The

administrator also attempted to perform a repair installation, but the server again displayed the same STOP message. You replace each hardware component in the server with components that are known to function correctly, but the server continues to display the STOP message.

You have a tape backup of the server's shared files from two nights ago. The backup is approximately 400 GB in size.

You need to provide users with access to the shared files as quickly as possible. You need to ensure that the security permissions on the shared files remain the same, and you want to minimize the amount of data that is lost.

What should you do?

A. Restore the shared file from the backup tape to a FAT32 volume on a different Windows 2000 Server computer.
B. Restore the shared files from the backup tape to NTFS volume on a different Windows 2000 Server computer.
C. Restart the server by using the Recovery Console. Copy the shared files onto floppy disks, and then copy the files from the floppy disks onto a different Windows 2000 Server computer.
D. Perform a parallel installation of Windows 2000 Server on the server.

Answer: D
Explanation: The fastest way to access to shared files would be to do a parallel install. This would typically take less than one hour. The NTFS security permission would still be the same. You would have to configure the share permission manually.

Incorrect answers:
A: FAT32 volumes don't support NTFS permissions. All NTFS permissions would be lost if the backup was restored on a FAT32 volume.
B: Restoring the files to a NTFS volume on another computer would work but it would not be the quickest way to recover the files. A fast tape drive could restore 1GB/minute. Restoring 400GB would require more than six hours.
C: Using the Recovery Console you would be able to copy files from a diskette to the hard disk. However, you would not be able to copy anything from the hard disk to a floppy disk.

Q. 94
You are an Organizational unit administrator of your company's Active Directory forest. You accidentally delete the user ID of an employee named Marc. You re-create the user ID with the same name as before. Marc now reports that he does not have the same permissions that he previously had.

You need to ensure that Marc has all of the permissions he had prior to the deletion. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Add Marc's user account back into all the groups it was previously a member of .
B. Ask the domain administrator to move Marc's user account from the LostandFound container back into the OU it was previously a member of.
C. Ask the administrator to delete Marc's user ID from within the LostandFound container.
D. Ask the domain administrator to perform an authoritative restore of Marc's user ID from a backup.
E. Configure Marc's account so that it does not require Kerberos preauthentication.

Answer: D, E
Explanation: We must perform an authoritative restore which only restores the user account of Marc. Then we need to configure Marc's user account to enable the option **Do not require Kerberos preauthentication**. This setting is disabled by default. He might not be able to log in if the Kerberos preauthentication is required. This is due to the fact that a timestamp of his last login is recorded in the Active Directory (see Note 1).

Note 1: Preauthentication is used so the system knows that the login request isn't a replay of a previous request. If preauthentication is enabled, a time stamp will be encrypted using the user's password hash as an encryption key. If the authentication server reads a valid time when using the user's password hash (stored in the Active Directory) to decrypt the time stamp, the authentication server knows that request isn't a replay of a previous request.

Note 2: The LostandFound container only contains objects that were supposed to be moved in the Active Directory, typically with the movetree command, but for some reason couldn't be moved. These objects end up the LostandFound container.

Incorrect answers:
A: Adding Marc's user accounts back to the groups he previously was a member of would enable him to get access to some of the resources he had. He would not be able to access resources explicitly given to the old Marc account since the Security Identifier (SID) has been lost.
B: A deleted object would not be moved to the LostandFound container.
C: Marc's ID would not be present in the LostandFound container.

Reference: HOW TO: Perform an Authoritative Restore to a Domain Controller (Q241594)
Authoritative Restore of Groups Can Result in Inconsistent Membership Information Across Domain Controllers (Q280079)

Q. 95
You are a network administrator for your company. A user named Marc has a local user account on his Windows 2000 Professional computer.

Marc is issued a USB print device. You need to configure Marc's computer so that he can install the new device and appropriate drivers. You log on to Marc's computer and disable the restrictions on loading unsigned drivers. All other local computer policies are configured with default settings. You restart Marc's computer.

Marc connects the print device to his computer. He reports that the printer does not appear in the Printers system folder, and he cannot print any documents.

You need to ensure that Marc can install the printer and can print documents. What should you do?

A. Add Marc to the local Print Operators group on his computer.
B. Add the **/fastdetect** switch in the Boot.ini file on Marc's computer.
C. Disable the **Prevent users from installing printer driver** local security policy setting.
D. In the **Driver Signing Options** dialog box, select the **Apply setting as system default** check box.

Answer: D
Explanation: You only removed the restriction to install unsigned drivers from your user account. You should have selected the **Apply setting as system default** box.

Incorrect answers:
A: The local Print Operators group doesn't have any specific permission to install print drivers.
B: The /fastdetect switch in the Boot.ini file only affects the boot behavior of Windows. It has nothing to do with Windows drivers.
C: Marc would have been able to install the driver if it had been a driver would have been signed. The **Prevent users from installing printer driver** is disabled by default.

Q. 96
You are the desktop administrator for your company. Each of the company's desktop computers has been upgraded from Windows NT Workstation 4.0 to Windows 2000 Professional. The hard disk on each computer has one NTFS partition.

One of the desktop computers has an application that stores its large data files on drive C. Recently the user of this computer has been running out of disk space on drive C. However, the computer's hard disk still contains unallocated space.

You need to increase available disk space on drive C on this computer. What should you do?

A. Create a partition by using unallocated space, and configure this partition as a mount point on drive C.
B. Create a stripe set that includes unallocated space and drive C.

C. Upgrade the hard disk from a basic disk to a dynamic disk.
D. Extend drive C by using unallocated space.

Answer: A
Explanation: The 2nd partition can be formatted and then be mounted to an empty folder on drive C.

Incorrect Answers:
B: To make a stripe set you must you have unpartitioned disk space on at least two disks, typically two physical disks. Here we only have one hard disk with two partitions, and one of the partitions is already used. It would be impossible to make a stripe set.
C: Converting the disk to a dynamic disk would not free any disk space.
D: You can only extend dynamic volumes. Since this computer was upgraded from Windows NT 4.0 it would have a basic disk.

Q. 97
You are the administrator of a Windows 2000 file server named ServerA. ServerA is a member server in a Windows 2000 Domain. You create a folder named H:\SalesHandbook on a volume that is formatted as NTFS. You share the folder as SalesHandbook$.

You want users of Windows 2000 Professional computer to be able to search Active Directory for the share by the name SalesHandbook.

What should you do?

A. Publish the shared folder, and configure the name to be SalesHandbook$ and the path to be \\ServerA\SalesHandbook.
B. Publish the shared folder, and configure the name to be SalesHandbook and the path to be \\ServerA\SalesHandbook$.
C. Publish the shared folder, and configure the name to be SalesHandbook$ and the path to be H:\SalesHandbook.
D. Publish the shared folder, and configure the name to be SalesHandbook and the path to be H:\SalesHandbook.

Answer: B
Explanation: A folder named H:\SalesHandbook is shared with the hidden name SalesHandbook$ on ServerA. To enable users to search for the folder in the Active Directory we must publish it with an alias without a hidden name (without a trailing $-sign), and we must use the path \\ServerA\SalesHandbook$.

Incorrect Answers:

A: Share or alias names ending with a $-sign are hidden. Users would not be able to see the share with a name of SalesHandbook$.
The path is be \\ServerA\SalesHandbook$, not \\ServerA\SalesHandbook
C: Share or alias names ending with a $-sign are hidden. Users would not be able to see the share with a name of SalesHandbook$.
The path to the share is also incorrect.
D: The path to the share is incorrect. The path is ServerA\SalesHandbook$.

Q. 98
You are the administrator of some of your company's file servers. Peter is hired as an intern in the human resources department. Peter needs access to some HR files. He also needs to be able to read the file named Handbook.doc, but he must not be able to make changes to it.

Handbook.doc exists in a folder named HRResources. Peter needs to have Read and Modify permissions for the other files in the HRResources folder.

Peter is a member of the Domain Users group and the HR group. The permissions on the HRResources folder are shown in the following table.

Group	Permission	Type of permission
Domain Users	**Read**	**Share**
HR	**Change**	**Share**
Domain Users	**Read**	**NTFS**
HR	**Modify**	**NTFS**

You need to ensure that Peter can access the appropriate files and that he cannot make changes to Handbook.doc. What should you do?

A. Set the hidden and system attributes on Handbook.Doc.
B. Disable permissions inheritance on Handbook.doc.
C. Assign Peter the **Allow-Read** permission for Handbook.doc.
D. Assign Peter the **Deny-Write** NTFS permission for Handbook.doc.

Answer: D
Explanation: First we calculate Peter's current permissions:
Share permissions: Read + Change = Change
NTFS permissions: Read + Modify = Modify
Share + NTFS = Change + Modify = Modify
Everything is as required except that he only should be allowed to read the Handbook.doc file not to change it. By explicitly assigning Deny Write permissions he would only be able to read this specific file, not change it.

Note: The calculation of effective permission on a share can be done by:

1. Calculate the NTFS permissions. They are accumulative except for DENY that overrides all permissions.
2. Calculate the Share permission. They are accumulative.
3. Combine the calculated NTFS and Share permissions. The result is the most restrictive permission.

Incorrect Answers:
A: Setting the hidden and the system attributes would not prevent Peter from modifying the Handbook.doc file; it would only make it harder.
B: Disabling inheritance of file permissions on the file would not help.
C: We want to prevent Peter from changing the file. He already has change permission. We must remove this change permission.

Q. 99
You are the administrator of your company's Windows 2000 file servers. A user named Maria creates a folder named Data on a file server. She uses Encrypting File System (EFS) to encrypt some of the files in the Data folder.

Now, other users need access to files Maria stores in the Data folder. In order to allow these users access to the files, you share the Data folder. You then assign these users the Allow-Read share permission and the Allow-Read NTFS permission for the shared Data folder.

Maria reports that users can access the unencrypted files in the Data folder, but they cannot access the encrypted files. When users attempt to access the encrypted files, they receive the following error message stating that access is denied.

You need to allow the users to access all of the files in the Data folder. What should you do?

A. Change the NTFS permission to **Full Control.**
B. Change the share permission to **Full Control.**
C. Instruct Maria to decrypt the files.
D. Share Maria's public key with all of the users.

Answer: C
Explanation: Only the owner, in this case Maria, or a Recovery Agent would be able to read the encrypted files. Maria must decrypt the files to enable the other users to access the files.

Incorrect Answers:

A: Even if you had full control permission to an encrypted file you would be unable to open it, unless you were the owner or you were a recovery agent.
B: Even if you hade full share permission to an encrypted file you would be unable to open it.
D: The public key is public to all. You cannot, in general, decrypt files with a public key.

Q. 100
You are the administrator of a Windows 2000 print server named serverA. ServerA is a member of a Windows 2000 Domain. You install a color laser print device on the network. You create and share a printer on ServerA named ColorLsr with the default settings.

You want all of the users in your company to be able to use ColorLsr, but you want the users in the Managers domain local group to always have priority use of the print device.

What should you do?

A. Create and share a second printer for the print device and set the priority level to 1. For the second printer, assign the Everyone group the **Deny–print** permission and assign the Managers group the **Allow-Print** permission. Instruct users in the Managers group to use the second printer.
B. Create and share a second printer for the print device and set the priority level to 1. For the second printer, remove permissions for the Everyone group and assign the Managers group the **Allow-Print** permission. Instruct users in the Managers group to use the second printer.
C. Create and share a second printer for the print device and set the priority level to 99. For the second printer, assign the Everyone group the **Deny–print** permission and assign the Managers group the **Allow-Print** permission. Instruct users in the Managers group to use the second printer.
D. Create and share a second printer for the print device and set the priority level to 99. For the second printer, remove permissions for the Everyone group and assign the Managers group the **Allow-Print** permission. Instruct users in the Managers group to use the second printer.

Answer: D
Explanation: We create a second printer with the highest priority (99) and only allow the Managers group access to it. This way the Managers group would always have higher priority on the print device.

Note: Scheduling priority can be set from 1 to 99 with 99 being the highest priority.

Incorrect Answers:
A: If you deny everyone print permission then no one would be able to print.
B: Setting the priority on the printer to 1 would give it the lowest priority. The manager's printer jobs would have higher priority.
C: If you deny everyone print permission then no one would be able to print.

Q. 101
You are the administrator of a Windows 2000 print server named ServerA. ServerA is a member of a Windows 2000 Domain. You install a high-speed laser print device on the network. You create and share a printer on ServerA named FastLsr with the default settings.

You want all of the users in your company to be able to use to FastLsr. You want the users in the Payroll domain local group to have exclusive use of the print device between the hours of 10:00 A.M and 3:00 P.M and shared use of the print device during all other times.

What should you do?

A. Configure and share FastLsr to be available from 3:00 P.M to 10:00 A.M. For the print device, create a second printer that has default availability. For the second printer, assign the Everyone group the **Deny-Print** permission and assign the Payroll group the **Allow-Print** permission. Instruct users in the Payroll group to use the second printer.
B. Configure and share FastLsr to be available from 3:00 P.M to 10:00 A.M. For the print device, create a second printer that has default availability. For the second printer, remove permissions for the Everyone group and assign the Payroll group the **Allow-Print** permission. Instruct users in the Payroll group to use the second printer.
C. Create and share a second printer device and configure it to be available from 10:00 A.M to 3:00 P.M. For the second printer, assign the Everyone group the **Deny-Print** permission and assign the Payroll group the **Allow-Print** permission. Instruct users in the Payroll group to use the second printer.
D. Create and share a second printer for the print device and configure it to be available from 10:00 A.M to 3:00 P.M. For the second printer, remove permissions for the Everyone group and assign the Payroll group the **Allow-Print** permission. Instruct users in the Payroll group to use the second printer.

Answer: B
Explanation:
Everyone will be able to use the 1st printer which is available only between 3PM and 10AM. The second printer, however, would only be used by the Payroll group. They are able to use it 24 hours a day.

Note:
Print device: the physical printer printing the pages
Printer: Windows object that handles the printing on the print devices.

Incorrect Answers:
A: Denying everyone Print permission on the 2nd printer would not allow anyone print on it since deny overrides other permissions.

C: Denying everyone Print permission on the 2nd printer would not allow anyone print on it since deny overrides other permissions.
It would not be necessary to install another print device. We just need to install another printer.

D: We should have two printers. Even if we had two printers in this solution it would not be so good.
Payroll would be able to print during 10AM to 3PM but at 3PM then would have to switch to the 1st printer to be able to print.

Q. 102
You are a network administrator for your company. The network consists of a single network segment in the company's New York office and a single Active Directory domain. The network contains a Windows 2000 Server computer named NYSrv04, which runs the DNS server service and the WINS server service. All client computers in the New York office use NYSrv04 for name resolution. The network also contains four other Windows 2000 Server computers, which are used for file and print sharing.

The company opens a new office in San Francisco. The San Francisco office has a single network subnet, which contains a Windows 2000 Server computer named SFSrv01, and 10 Windows 2000 Professional computers. SFSrv01 is configured as a domain controller in the company's Active Directory domain. All computers in the San Francisco office are members of the domain.

In accordance with the company's network plan, you install WINS and DNS on SFSrv01. You configure the client computers in the San Francisco office.

You need to ensure that the users in each office can access the computers in both offices. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Configure WINS replication on SFSrv01 and NYSrv04 so that SFSrv01 and NYSrv04 are replication partners.
B. Back up the WINS database on NYSrv04 and restore it on SFSrv01.
C. Configure an Lmhosts file on SFSrv01 that includes the name and IP address of NYSrv04.
D. Configure the DNS server service on both NYSrv04 and SFSrv01 to use Active Directory integrated zones.
E. Configure the DNS server service on SFSrv01 to forward name resolution requests to NYSrv04.

Answer: A, D
Explanation: The WINS servers should be set up as replication partners. This would enable computers to access resources by NetBIOS names in both offices.

The best solution for host name resolution is to set up both DNS servers as Active Integrated DNS zones. They would then replicate zones through the Active Directory replication.

Incorrect Answers:

B: WINS replication, not WINS bakcup, is used to keep two WINS servers exchanging names, and keep them consistent with each other.

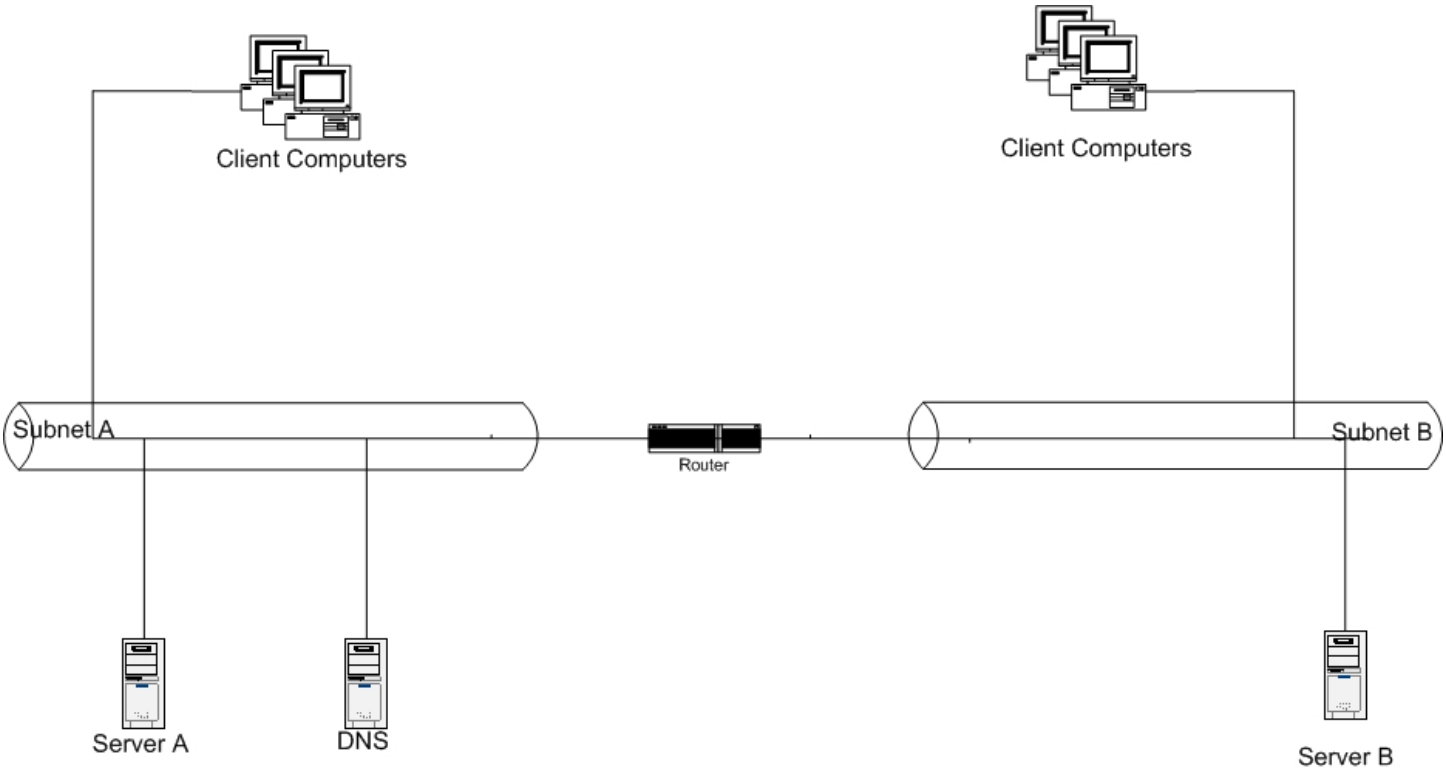
C: An Lmhosts file on SFSrv01 containing a record for NYSrv04 would enable SFrv01 access NYSrv04 with a NetBIOS name. It would not enable SFSrv01 to access other resources in New York by NetBIOS name though. It would not enable the other computers in the San Francisco office to reach the resources in New York either. An Lmhosts file would have to be placed on all computers in San Francisco.

E: Configuring the DNS server in San Fransicisco to forward name resolution requests to New York would enable computers in San Francisco to access resources in New York by host name. However, the New York computers would not be able to access resources in San Francisco by host name.
The zones of the DNS server should be replicated.

Q. 103

You are a domain administrator for your company. The network consists of a single Windows 2000 Domain and two TCP/IP subnets. A server named ServerA provides DHCP services for the network.

You are installing Windows 2000 Server and the DHCP service on a new stand-alone server named ServerB. You configure ServerB with a DHCP scope for both network subnets. The scope on ServerB excludes the addresses that are part of the DHCP scope on ServerA. You configure both DHCP servers with the same scope options. The network is configured as shown in the exhibit.



When you stop the DHCP service on ServerA, client computers on subnet A cannot obtain TCP/IP addresses. However, client computers on subnet B can obtain TCP/IP addresses. You want to enable ServerB to issue TCP/IP addresses to client computers on both subnets.

What should you do?

A. Configure the router to forward BOOTP packets from subnetA to serverB.
B. Configure the File Replication service on ServerA to replicate the DHCP folder to ServerB.
C. Authorize ServerB as a DHCP server.
D. Authorize ServerA as a DHCP server.

Answer: A
Explanation: ServerB is functioning on subnet B but not on subnet A. According to the scenario the scope is correctly set up for subnet A. The most likely cause is the router. Routers must be able to forward BOOTP packers, or be RFC 1542-compliant which is the same thing, in order to forward DHCP traffic between the subnets. If we are lucky this router is RFC 1542 compliant but only needs to be configured to forward the BOOTP packages.

Incorrect Answers:

B: The File Replication service and the DHCP service are not able to interoperate.

C: The DHCP server ServerB is apparently functioning on its own subnet. It must already have been authorized in the Active Directory.

D: ServerA was servicing DHCP clients on Subnet A earlier before it stopped functioning so it must already be authorized.

Q. 104

You are a network administrator for Contoso Pharmaceuticals. The network contains two Windows 2000 Server computers, which run the DNS server service. The DNS servers are domain controllers for a single domain named ad.contoso.com.

The DNS servers use standard zone types for ad.contoso.com. The Windows 2000 Server computers and Windows 2000 Professional computers in the domain are configured to dynamically register with the DNS servers. DNS is the only name resolution service on the network.

A Windows 2000 web server named ServerA contains an employee information Web site. Users report that they attempt to access the Web site; they receive an error message stating that the page cannot be displayed.

You confirm that you can access the web site on ServerA by using the server's IP address. However, when you run the ping ServerA command from the command line the reply you receive contains a different IP address.

You want to correct the name resolution problem and prevent it from happening again. Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

A. Disallow zone transfers for the ad.contoso.com zone.
B. Change the zone type to Active Directory integrated for the ad.contoso.com zone.
C. Allow only secure updates for the ad.contoso.com zone.
D. Disable dynamic updates for the ad.contoso.com zone.
E. Run the **ipconfig/release** command on the computer that responds to the ping. Run the **ipconfig/renew** command on ServerA.
F. Delete the current DNS entry for ServerA. Run the **ipconfig/registerdns** command on ServerA.

Answer: B, C, F

Explanation: There is an incorrect DNS entry in the DNS zone. We must prevent this from happening again in the future. We must also correct this particular DNS entry.

B: First we change the zone to an Active Directory integrated zone. Only Active Directory integrated zones can be configured to only allow secure updates.

C: We must allow only secure updates on the zone to avoid incorrect DNS records from being registered again.
F: The problem must be corrected. We achieve this by deleting the current incorrect DNS entry for ServerA. We then register a new DNS entry for ServerA with the **ipconfig/registerdns**.

Incorrect Answers:
A: Preventing zone transfers would be counterproductive. The DNS servers must be able to replicate the DNS records.
D: Without dynamic updates the administrator would have to manually manage all records in the DNS zone: add, delete, and change for example. This is usually not a good idea and it would not help solving the problem at hand.
E: There is no need to reconfigure the computer that had the same IP address as the server. The server will be registered with a new IP address.

Q. 105
You are the network administrator for your company's New York branch office. You receive three new Windows 2000 Server computers from the main office. Each new server contains a single hard disk, which is configured as a single NTFS logical volume.

You want to ensure that you can continue to access the NTFS volume on each server in the event that Windows 2000 Server fails to start. You want to be able to access each volume without having to start the server from a CD-ROM or a floppy disk.

What should you do on each server?

A. Ensure that the Everyone group has the **Allow-Full Control** permission for the root folder of the hard disk.
B. Copy the i386 folder from the Windows 2000 Server CD-ROM to the folder named \Windows\Options on the hard disk.
C. Place your domain users account in the local Administrators group.
D. Run the **winnt32.exe/cmdcons** command from the Windows 2000 Server CD-ROM**.**

Answer: D
Explanation: The recovery console can be copied from the Windows 2000 Installation CD to the hard disk with the **winnt32.exe/cmdcons** command. Then it would be possible to start the Recovery Console without the use of the Windows 2000 Installation CD.

Note: The Recovery Console is a command-line interface that can be used to access a hard disk of a Windows 2000 computer system. It can be accessed from the Windows 2000 Professional/Server installation CD-ROM

and can be used to repair an installation of Windows 2000 Professional/Server by repairing the registry or by disabling a device driver or service. Usually you start the Recovery by booting the computer from the Windows 2000 Professional installation CD-ROM. On the Welcome to Setup screen, press R to open the Repair Options screen, and press C to activate the Recovery Console.

Incorrect Answers:

A: Assigning permission to the root folder on the hard disk would not make it possible access it when Windows fails to start.

B: Simply copying the i386 folder will not help. The recovery console must be copied to the hard disk by the **winnt32.exe/cmdcons** command.

C: More local Administrators would not help in accessing the hard disk if the Windows 2000 Server fails to start.

Q. 106

You are the administrator of a Windows 2000 Server computer. The server runs a client/server application that is used by 2,000 users in your company.

During a scheduled maintenance period, you install a faster network adapter card in the server, and you install the software drivers provided by the card manufacturer. You remove the server's old network adapter card and uninstall the old drivers.

You restart the server and log on by using the local Administrator account. Shortly after you log on, the server stops responding and displays a STOP message. You restart the server again, and it displays a STOP message a few seconds after it displays the logon screen.

You remove the new network adapter card and reinsert the original card. You restart the server and it again displays the STOP message a few seconds after it displays the logon screen.

You need to return the server to normal operation as quickly as possible. What should you do?

A. Restart the server using the last known good configuration. Reinstall the drivers for the original network adapter card.

B. Restart the server by using safe mode. Uninstall the new network adapter card drivers, and restart the computer. Reinstall the drivers for the original network adapter card.

C. Restart the server by using the Windows 2000 Server CD-ROM, and select the option to repair the installation. Restart the server. Reinstall the drivers for the original network adapter card.

D. Restart the server by using the Windows 2000 Server CD-ROM, and select the option for the Recovery Console. Copy the drivers for the original network adapter card from the CD-ROM provided by the network adapter card manufacturer.

Answer: B
Explanation: Safe Mode can be used to disable or uninstall device drivers that don't function.

Incorrect Answers:
A: The Last Known Good Configuration was replaced when you were able to log on. It cannot be used to revert to the state before the new network adapter device driver was installed.
C: Repairing the installation would be a long process. It is simpler just disabling the device driver.
D: The Recovery Console could also be used, but we should then use it to disable the device driver. It is not possible to install a device driver using the Recovery Console.

Q. 107
You are a desktop administrator for your company. All client computers run Windows 2000 Professional with the default installation settings.

Users in the sales department use portable computers. The users require dial-up access to the company network when they are out of the office. You are asked to configure network dial-up access for a new sales employee named Peter.

You insert a PC Card modem into Peter's computer. You then restart the computer and log on as a local administrator. You start the Network Connection wizard, but the modem does not appear in the list of devices that you can select for marketing the dial-up connection.

You need to be able to install the modem in Peter's computer. What should you do?

A. In the system BIOS, reserve an IRQ for the COM port that is used by the modem.
B. In the **Driver Signing Options** dialog box, set File Signature Verification to **Ignore.**
C. Use Device Manager to disable the computer's built-in serial ports.
D. Manually install the modem device driver provided by the manufacturer.

Answer: D
Explanation: We should simply install the device drivers manually. Some PC cards are not detected automatically on all computers.

Incorrect Answers:
A: It would not be necessary to reserve an IRQ for the COM port in BIOS.
B: This is not a driver signing issue. The device has not even been detected by Windows.
C: It would not be necessary to disable the built-in serial port. We must just supply the correct device drivers manually.

Q. 108
You are a network administrator for your company. A new company policy requires that new server installations include the most recent services pack. Company executives plan 100 new server installations during the next three months.

You need to deploy the new servers with the least amount of administrative effort. What should you do?

A. When each new computer is delivered, install Windows 2000 Server on it. Then run the **update.exe** command from the service pack CD-ROM.
B. When each new computer is delivered, install Windows 2000 Server on it. Then run the **setup.exe** command from the service pack CD-ROM.
C. When the first new computer is delivered, install Windows 2000 Server on it. On drive C, create a folder named Win2000 and copy the contents of the Windows 2000 Server CD-ROM into this folder. Run the **update.exe –s:c:\Win2000** command from the service pack CD-ROM. Create a new installation CD-ROM that contains the contents of the Win2000 folder, and use this CD-ROM for all subsequent new server installations.
D. Install Windows 2000 Server on an existing server. On drive C, create a folder named i386 and copy the contents of the Windows 2000 Server CD-ROM into this folder. Run the **setup.exe –s:c:\i386** command from the service pack CD-ROM. Create a new installation CD-ROM that contains the contents of this folder, and use this CD-ROM for all subsequent new server installations.

Answer: C
Explanation: We slipstream the service pack into the Windows 2000 Server installation directory with the command **update.exe –s:c:\Win2000.** The –s switch is used for slipstreaming.

Note: The slipstreaming requires that Windows 2000 already be installed on the computer.

Incorrect Answers:
A: Manually applying the service packs would take a lot of time and effort.
B: Service packs are applied by starting the utility update.exe, not setup.exe.
D: To slipstream a service we should use the **update.exe** utility not **setup.exe**.

Note: The naming of the folder **i386** suggests that only the files of the **i386** would be copied to the hard drive. It would be better to copy all files from the CD-ROM.

Q. 109
You are a network administrator for your company. The network consist of a single domain that contains an Organizational Unit (OU) named New York. All user accounts in the domain are in the New York OU.

You configure a Group Policy Object named StartMenuGPO and link it to the New York OU. StartMenuGPO redirects the Start menu to a shared network folder. You want all user accounts except the domain administrator accounts to have StartMenuGPO applied.

You notice that on your computer, the Start menu has been redirected. You need to ensure that no administrator accounts have StartMenuGPO applied. You also need to ensure that the domain administrators can administer all GPOs.

What should you do?

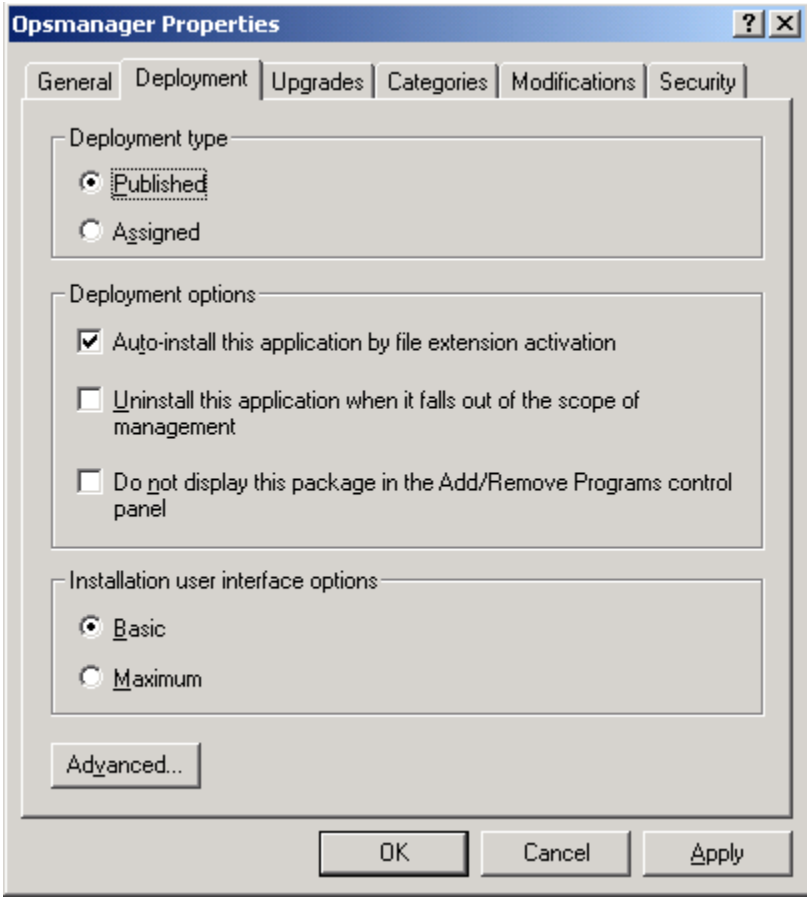
A. Modify the permissions on StartMenuGPO by configuring the **Read** permission for the Domain Admins group to **Deny.**
B. Modify the permissions on StartMenuGPO by configuring the **Apply Group Policy** permission for the Domain Admins group to **Deny.**
C. Remove StartMenuGPO. Move the administrative accounts to the Users container. Create a new GPO and link it to the domain level to redirect the Start menu.
D. Create a new GPO and link it to the New York OU. Configure the Start menu to be redirected to the C:\Documents and Settings\Administrator folder. Assign the Domain Admins group **Allow-Full Control** permission for this GPO.

Answer: B
Explanation: The **Apply Group Policy** permissions for a User or Group on a GPO would enable the GPO to be applied to the User or Group. By denying the **Apply Group Policy** permissions on the GPO for the Domain Admins group the GPO would not be applied these users.

Incorrect Answers:
A: The Administrators must have read access in order to administer the GPO.
C: The Administrators would still be applied with the GPO when it is linked at the domain level.
D: The old GPO would still be applied to the Domain Admins group.

Q. 110
You are the administrator of an Organizational unit (OU) named Operations. You need to provide a new software application to the users in the Operations OU. You want the shortcut for the new application to appear on every user's Start menu, and you want the application to be installed the first time a user clicks the shortcut.

You configure a Group Policy Object (GPO) to deploy the application, as shown in the exhibit.



Users report that the shortcut for the new application does not appear on their Start menus. You need to ensure that the shortcut appears on every user's Start menu, and that the application is installed the first time a user clicks the shortcut.

What should you do?

A. Modify the GPO by selecting the **Maximum** option under **Installation user interface options.**
B. Modify the GPO by selecting the **Assigned** option under **Deployment Type.**
C. Move the application's installation package to a network share.
D. Share the folder that contains the application's installation package, and publish the shared folder in Active Directory.

Answer: B
Explanation: Currently the application is published. A published application is not installed automatically. You would have to manually install it from the Control Panel.

An assigned application on the other hand appears on the Start menu and the installation of the application starts when this short cut is used or when a document associated with the application is opened.

Incorrect Answers:

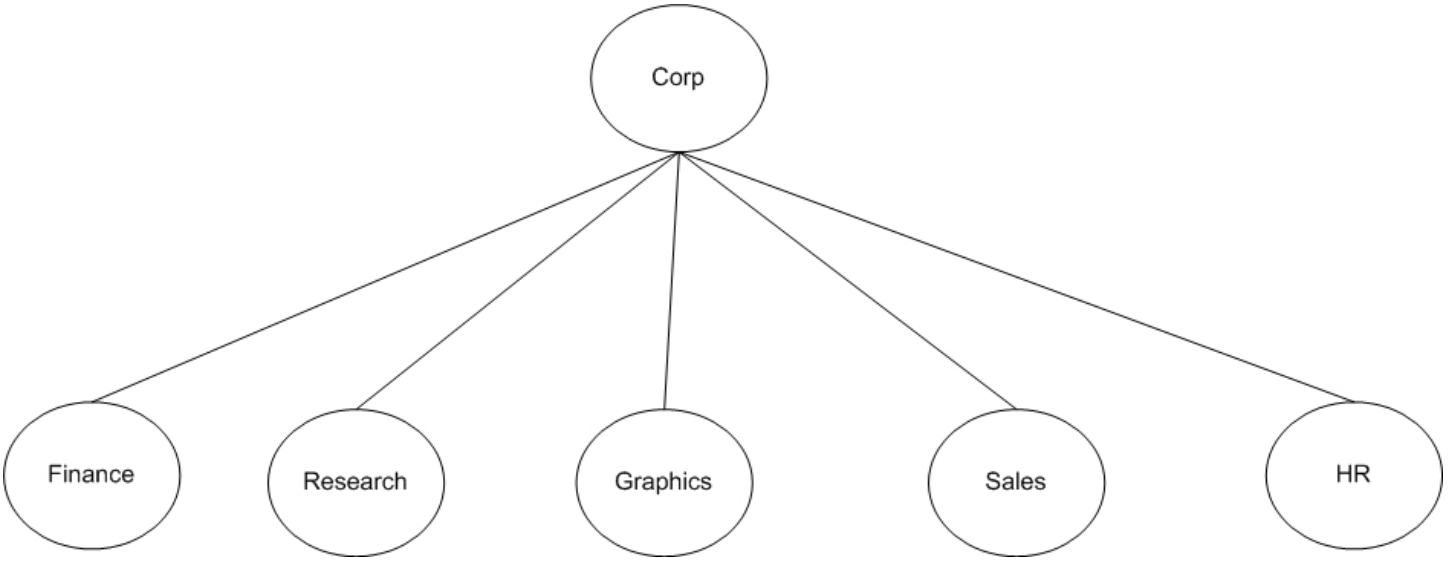
A: The Maximum **Installation user interface options** option should only be used when the user is an Administrator.

C: The primary problem is that the application is published not assigned.

D: The shared folder doesn't have to be published in the Active Directory.
The application must be assigned.

Q. 111

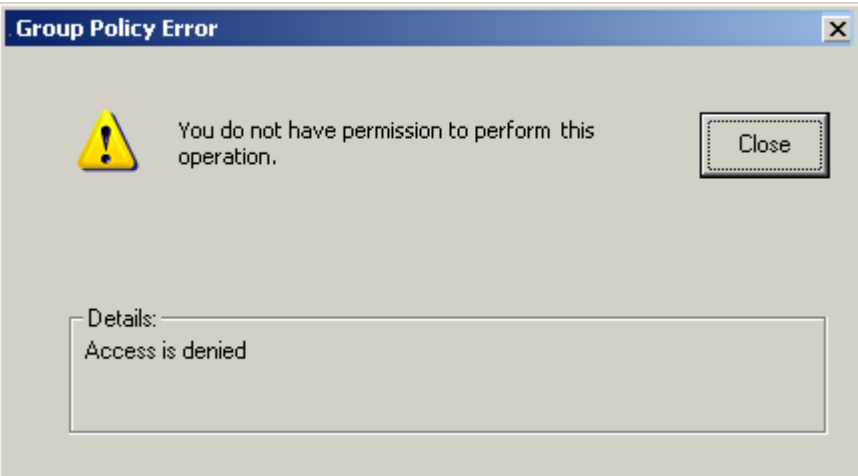
You are domain administrator for your company. The network consists of a single Windows 2000 domain. The domain contains and organizational unit (OU) structure as shown in the OU structure exhibit.



Each department has its own departmental administrators who are responsible for the administration of resources in their respective departments. Company Policy requires that these departmental administrators have control of the objects only in their respective OUs.

You use the Delegation of Control Wizard to delegate complete control of the each departmental OU to the administrative staff in the respective department. The departmental administrators can successfully create users, groups, and printers in their respective OUs.

Maria is an administrator in the sales department. Maria reports that she cannot create a Group Policy Object in the Sales OU. When she attempts to create a Group Policy new GPO in the OU, she receives the error message shown in the GROUP POLICY ERROR exhibit.



You verify that Maria has the Allow- Full Control permission for the Sales OU, but she still cannot create the GPO.

You need to resolve this problem. What should you do?

A. Add Maria to the Domain Admins Security Group.
B. Add Maria to Group Policy Creator Owner Security group.
C. Assign Maria the **Allow- Create Child Objects** permission for the Corp OU.
D. Assign Maria the **Allow-Modify Ownership** permission for the sales OU, and instruct here to take ownership of the OU.

Answer: B
Explanation: In order to create a GPO, a user must be a member of the built-in group called Group Policy Creator Owner. Only Domain Administrators and Enterprise Administrators can create GPOs by default.

Incorrect Answers:
A: Adding Maria the Domain Admins Group would give her too much permissions and rights throughout the domain.
C: We want Maria to be able to link a newly created GPO to the OU, not to create child objects in the OU. A GPO is not a child object to an OU. A GPO is linked to an OU.
D: We don't want Maria to take ownership of the OU. We only want her to administer it.

Q. 112

You are the network administrator for your company. You create a global distribution group named ITStaff, the ITStaff group is a member of a domain local group named Public. You create a global distribution group named Public. The Public Group has the READ permission for a resource on the domain controller. The resource is named Res1.

Ten employees in the IT department need access to Res1. You add the user accounts for the 10 employees to attempt to access Res1 immediately. They report that they cannot access Res1.

You need to ensure that the 10 employees can access Res1. What should you do?

A. Configure the ITStaff group's group scope to be a universal group and instruct 10 employees to logout and to log in again.
B. Configure the Public group's group scope to be a universal group, and instruct the 10 employees to log out and to log in again.
C. Configure the ITStaff group's group scope to be a security group, and instruct 10 employees to logout and to log in again.
D. Move the user accounts of the 10 employees so that the accounts are in the same organizational unit (OU) as the ITStaff group, and instruct 10 employees to log out and log in again.

Answer: C
Explanation: A distribution group is only used by applications, for example to distribute e-mail to a group of users, and not by Windows 2000. Windows 2000 use security groups instead. You cannot assign rights or permissions to a distribution group.

Incorrect Answers:
A, B, D: A distribution group cannot be assigned rights or permissions. A security group must be used instead.

Q. 113
You are a network administrator for your company. The company has offices in five cities. There is an Organizational Unit (OU) for each office.

You install a new file server named ServerB. ServerB will host the My Documents folder for all users in the New York OU.

At the domain level there is a Group Policy Object (GPO) Named AllMyDocumentsGPO that redirects the My Documents folder to \\ServerA\users\%username%. There is a separate GPO named SettingsGPO that configures the desktop settings and removes the Run command that is configured at the domain level.

You configure a GPO named NYMyDocumentsGPO that redirects the My Documents folder for the users in the New York office to \\ServerB\users\%username%. You verify that the My Documents folder has been redirected. However, you notice that users in the New York office do not have the corporate desktop settings and that the users can use the Run command.

You need to ensure that the My Documents folder for every user account in the NY OU is redirected to ServerB. You also need to ensure that the users in the New York office receive the corporate desktop settings and that the users cannot use the run command.

What should you do?

A. On the New York OU, configure Group Policies to not block inheritance.
B. On the New York OU, remove the NYMyDocumentsGPO and then configure Group Policies to not block inheritance.
C. On AllMyDocumentsGPO, modify the permissions by adding a NYUsers group and assigning it the Deny –Apply Group Policy permission.
D. At the domain level, configure a new GPO for the croporate desktop settings. Add a NYUsers group and assign it the Allow – Apply Group Policy permission for the new GPO.

Answer: A
Explanation: Apparently something is blocking the SettingsGPO which is applied at the Domain level and should be applied to all users in the domain. This blocking seems to be related to New York OU. There is no similar behavior reported from the other offices. It would therefore be wise to configure GPOs on the New York OU not to block inheritance.

Incorrect Answers:
B: The NYMYDocuments GPO should not be removed. The New York users should have their My Documents folder redirected to not **\\ServerA\users\%username%.**
C: The AllMyDocumentsGPO doesn't include the Desktop settings, the SettingsGPO do.
D: There is already a GPO at domain level with these settings. This GPO would be applied to all users in the domain unless something prevented from being applied.

Q. 114
You are a network administrator for your company. You are responsible for a child domain in your enterprise. The human resources (HR) department uses this child domain. The domain contains Windows 2000 domain controllers and Windows NT 4.0 member servers.

The HR department institutes a new employee review process. Under the new process, documents that are used for performance reviews will be stored in the shared folder, and managers will be the only personnel who will have access to that shared folder.

In that organizational unit (OU) named Mgr1, existing global groups for managers are the IT Managers group, the HR Managers group, the Finance Managers group and the Manufacturing Managers group.

You want to add these managers groups to a new security global group named All Managers. The All Managers group is in a separate OU named AllMgr. However, when to attempt to add each of the managers groups to the All Managers group, you notice that only individual users accounts are available to be added and the managers group are not available to be added.

What should you do?

A. Move the All Managers group to the Mgr1 OU.
B. Ask the domain administrator to switch the domain to native mode.
C. Change the All Members group from a global group to a universal group.
D. Ask the domain administrator to assign you the **Allow – Change** permission for each of the managers global groups.

Answer: B
Explanation: We want to add global groups into another global group. This is called group nesting. Group nesting is only possible in native mode. Though it isn't stated explicitly stated in the scenario, it seems likely that this domain is running in mixed mode.

By changing to native mode we would be allowed to nest global groups.

Incorrect Answers:
A: Moving the groups to another OU wouldn't accomplish much.
C: Universal groups can only be used in native mode. In native mode it is possible to add global groups to other global groups. A universal group would not be necessary, global groups would support group nesting.
D: Permissions to group cannot be assigned.
Typically you add user and groups to OUs. Then you assign permission to the OU.

Q. 115
You are the administrator of a Windows 2000 Server computer named ServerA. ServerA runs Terminal Service. Company users log on to Terminal Services to run custom Windows-based applications that are installed on ServerA.

A user named Maria works in a branch office. Maria reports that she is having problems using one of the applications on ServerA. You attempt to troubleshoot the problem by talking to Maria over the telephone, but she cannot provide sufficient information about what the application is doing.

You need to see how Maria is using the application in order to resolve the problem. What should you do?

A. Use Terminal Services to log on to ServerA from your client computer. Use Terminal services Manager to shadow Maria's session and troubleshoot the problem.
B. Log on to ServerA's console. Use Terminal Service Manager to shadow Maria's session and troubleshoot the problem.
C. Ask a domain administrator to modify Mara's user account so that its Terminal Services disconnect time is at least one hour. Instruct Maria to log off of ServerA. Then, use Terminal Services from your client computer to log on to ServerA by using Maria's user account, and run the application.
D. Ask a domain administrator to modify Mara's user account so that its Terminal Services idle time is at least one hour. Instruct Maria to disconnect from ServerA. Then, use Terminal Services from your client computer to log on to ServerA by using Maria's user account, and run the application.

Answer: A
Explanation: Shadowing allows you to remotely control an active session of another user. You can either view or actively control the session. If you choose to actively control a user's session, you will be able to input keyboard and mouse actions to the session.

Incorrect Answers:
B: It would not be necessary to physically logon the ServerA at the console. Instead it would more practical to logon remotely using Terminal Services.
C: Using shadowing you would able to log on directly and control and check Maria's session.
D: Using shadowing you would able to log on directly and control and check Maria's session.

Q. 116
You are the administrator of an organizational unit (OU) named WebServers. The WebServers OU contains 20 Windows 2000 Web servers. The WebServers OU is an immediate child OU of an OU named Servers. The Servers OU has a Group Policy Object (GPO) named IPSecurity linked to it. The No Override option is not selected on IPSecurity. IPSecurity settings must always apply to the servers in the WebServers OU.

All of the web sites on the servers in the WebServers OU are configured to allow only anonymous users connections.

A domain administrator applies a new GPO named LogonLocally at the Servers OU. LogonLocally restricts the ability to log on locally to members of the local Administrators group. Users report that they can no longer access any of the Web sites on the servers in the WebServers OU.

You need to ensure that users can access the Web Sites on the servers in the WebServers OU. What should you do?

A. Configure the properties for the WebServers OU to block policy inheritance.

B. Link LogonLocally to the WebServers OU and select the **No Override** option.
C. Create a GPO that allows members of the local Administrators and Guests groups to log on locally Link the GPO to the WebServers OU.
D. Create a GPO that allows members of the local Administrators and Users groups to logon locally. Link the GPO to the WebServers OU.

Answer: C
Explanation: We want to grant the guest account the right to log on locally so that the Web servers can be accessed using anonymous authentication. This can be done by creating a GPO that allows the guest group (and the local Administrators group) the right to log on locally, and linking the GPO to the WebUsers OU. This GPO would override the LogonLocally GPO, since the more local GPO will be applied last. And as the guest account is a member of the guest group anonymous access to the Web servers would be enabled.

Incorrect Answers:
A: Blocking policy inheritance on theWebServers OU would block the LogonLocally policy which is applied at the Servers OU. The IPSecurity GPO would be blocked as it is configured with the Override option. We would not achieve the required result.
B: We don't want the LogonLocally GPO to be applied to the WebServers OU. Linking it to the OU doesn't make any sense.
D: In order to enable anonymous access we should allow the Guest account to logon on locally. Making the local Administrators and Users groups log on locally would not allow guests, and it would not allow anonymous access to the Web Servers.

Q. 117
You are a domain administrator for your company. The network contains a Windows 2000 Server computer named ServerA. ServerA has Routing and Remote access installed and has twelve 56-Kbps dial-up modems attached. The company has 25 employees who use Windows 2000 Professional portable computers to dial in to the network by using ServerA.

The 25 employees report that they are unable to connect to ServerA. You discover that all the modems on ServerA are being used by other dial-in users. You examine the Routing and Remote Access Server event logs and notice that some users have been connected for more than six hours.

You want to increase the availability of dial-up connections on ServerA. You want to ensure that employees do not stay connected on ServerA during periods of inactivity.

What should you do?

A. Configure the remote access policy on ServerA to enable an Idle Timeout setting of 15 minutes.

B. Configure the remote access policy on ServerA to enable logon hour restriction no longer than three hours.
C. Configure the dial-in user's domain user accounts with logon hour restrictions no longer than three hours.
D. Configure the dial-in user's domains user accounts with location logon restrictions that include the MAC address of ServerA.

Answer: A
Explanation: We configure the Remote Access Policy to drop the connection after 15 minutes of inactivity. We use the **Disconnect if idle for:** option.

Incorrect Answers:
B: We want to disable inactive connection, not long active connections.
C: Logon hour restrictions cannot be configured in dial-in user account properties. A remote access policy must be used.
We want to configure the idle setting anyway.
D: We should configure the **Disconnect if idle for:** setting in the Remote Access policy.