QUESTION NO: 1
You are the administrator of Chinatag'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.

QUESTION NO: 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 Chinatag'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?

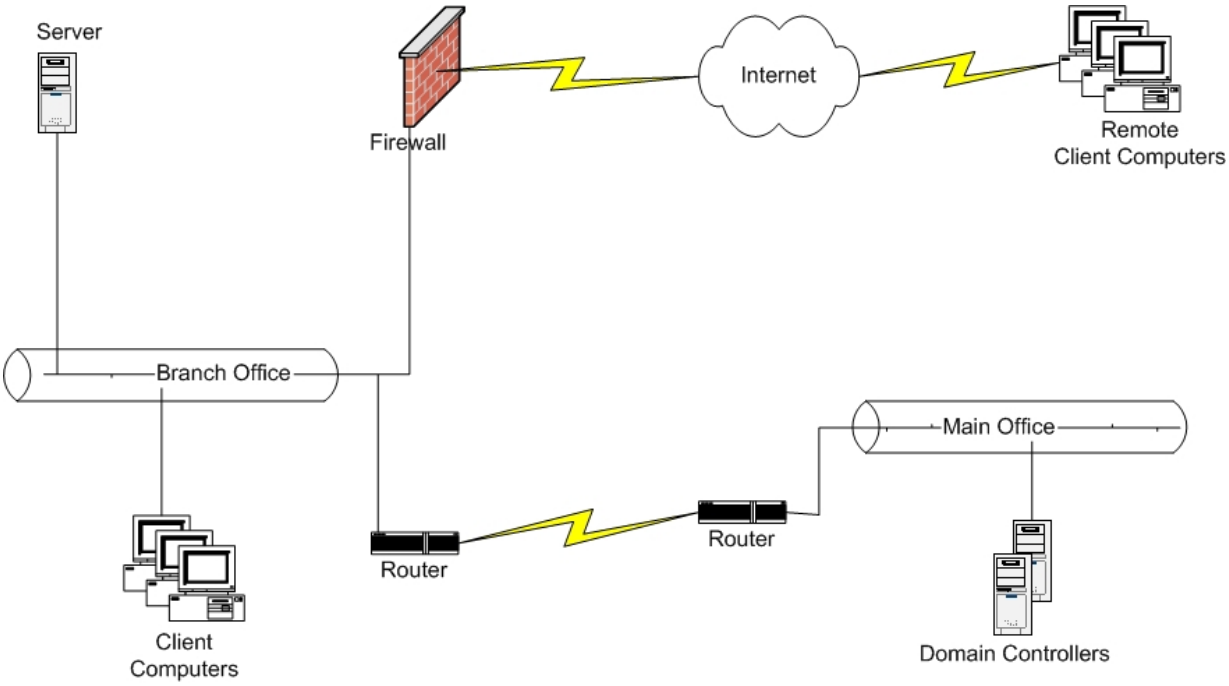
A. Install a Web server certificate and enable Digest authentication.
B. Install a Web server certificate and enable SSL for the new Web site.
C. Configure the new web site to use Integrated Windows authentication.
D. Configure the new Web site folder to enable Encrypting File System (EFS).

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 Chinatag 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.

QUESTION NO: 3
You are a network administrator for Chinatag. 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 (GPO) 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 (GPO) 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.

QUESTION NO: 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.

QUESTION NO: 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.

QUESTION NO: 6
You are a network administrator for Chinatag. 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 rig It is an object access event. We should therefore audit Object Access.

QUESTION NO: 7
You are the desktop administrator for Chinatag. 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 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, howe ver 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, howe ver allow the clients to use Dfs.

QUESTION NO: 8
You are a domain administrator for Chinatag. 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 ha ve Full Access (we know this from the exhibit).

QUESTION NO: 9
You are a network administrator for Chinatag. 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.

QUESTION NO: 10

You are a domain administrator for Chinatag. 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.

QUESTION NO: 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 Chinatag'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 o server certificate, an optional client certificate, and various digital keys.