Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure

Number: 070-217
Passing Score: 800
Time Limit: 120 min
File Version: 11.0

Important Note
Please Read Carefully

Study Tips
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 cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Further Material
For this test TestKing also provides:
* Study Guide. Concepts and labs.
* Interactive Test Engine Examinator. Check out an Examinator Demo at http://www.testking.com/index.cfm?pageid=724

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestKing an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Member zone/Log in**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Exam A

QUESTION 1
You are configuring a Windows 2000 DNS Server on your company network. The network consists of one Windows NT domain.

You already have DNS installed on a Windows NT Server on the Windows NT domain. You want to use dynamic updates on a DNS database, but company management will not allow an upgrade or decommission of the Windows NT DNS server. All DNS information must be synchronized between the two DNS servers.

What do you do to accomplish these goals? (Choose three)

A. Create a standard primary zone on a Windows 2000 DNS Server and import the existing zone file.
B. Create a standard secondary zone on a Windows 2000 DNS Server.
C. Delete and re-create the primary zone on the NT DNS Server.
D. Delete the existing zone and create a new secondary zone on the NT DNS Server.
E. Configure the primary zone on the NT DNS Server as the master zone for the secondary zone on the Windows 2000 DNS Server.
F. Configure the secondary zone on the NT DNS Server to use the Windows 2000 Standard primary zone as its master zone.

Answer: ADF
Section: (none)

Explanation/Reference:
Explanation:
A: Dynamic updates are a new feature of Windows 2000 DNS. They are not supported by NT DNS. To enable dynamic updates we need to create a primary DNS zone on the Windows 2000 server. A secondary zone will not do because only the primary DNS zone is updateable. We can import the zone data from the NT server to avoid having to create a new zone file.

D: We need to delete the primary zone on the NT server and create a secondary zone. The NT server must have a secondary zone to enable the server to transfer zone files from the now primary Windows 2000 server.

F: We can now set the secondary zone on the NT server to use the primary zone on the Windows 2000 server. The Windows 2000 DNS zone will be dynamically updated. The new information will then be replicated to the Windows NT Server.

Incorrect Answers:
B: The Windows 2000 server must have a primary zone to support dynamic updates, as only a primary zone is updateable. Furthermore, the primary zone must reside on the Windows 2000 computer because Windows NT Server does not support dynamic updates.

C: The primary zone must reside on the Windows 2000 computer because Windows NT Server does not support dynamic updates. We thus cannot delete and recreate the primary zone on the Windows NT Server.

E: The primary zone must reside on the Windows 2000 computer because Windows NT Server does not support dynamic updates. Furthermore, the Windows NT Server requires a secondary zone to pull DNS information from the Windows 2000 server. A primary zone cannot pull zone data from a secondary zone.

QUESTION 2
You are the administrator of your company's network. The network consists of one Windows 2000 domain that spans multiple subnets. You are configuring DNS for hostname resolution throughout the network.

You want to achieve the following goals:

- DNS zone transfer traffic will be minimized on the network.
- Administrative overhead for maintaining DNS zone files will be minimized.
- Unauthorized host computers will not have records created in the zone.
- All zone updates will come only from authorized DNS servers.
- All zone transfer information will be secured as it crosses the network.

You take the following actions:

- Create an Active Directory integrated zone.
- In the Zone Properties dialog box, set the Allow Dynamic Updates option to Yes
- On the Name Servers tab of the Zone Properties dialog box, enter the names and addresses of all DNS servers on the network.
- On the zone transfers tab of the zone properties dialog box, select the Allow Zone transfers only to the servers listed on the Name servers tab option

Which result or results do these actions produce? (Choose all that apply)

A. DNS zone transfer traffic is minimized on the network.
B. Administrative overhead for maintaining DNS zone files is minimized.
C. Unauthorized host computers do not have records created in the zone.
D. All zone updates come only from authorized DNS servers
E. All zone transfer information is secured as it crosses the network.

Answer: ABDE
Section: (none)

Explanation/Reference:
Explanation:
A: Active Directory integrated zones use IXFR, which are incremental transfers. This means that only the records that have changed since the last replication are replicated. This makes the replication of Active Directory integrated zones more efficient because the whole zone file is replicated during standard primary zone replication.

B: Dynamic updates is the process of a client computer updating it is own record in the DNS zone file. This will prevent the need to manually enter records in the DNS zone.

D: Selecting the “Allow Zone transfers only to the servers listed on the Name servers tab” option prevents unauthorized servers from updating the zone. Dynamic updates have been enabled.

E: Active Directory DNS zones replicate their data as part of Active Directory replication. Active Directory replication uses a secure RPC channel to replicate data.

Incorrect Answers:
C: The “Only Secure Updates" option must be selected to be sure that no unauthorized DNS records are created in the zone. Secure updates specify that only users, groups or computers that have been granted the right to write to the zone or record have the ability to update the record.

QUESTION 3
You are the administrator of a Windows 2000 network for Miller Textiles. The network configuration is shown in the exhibit.

The millertextiles.com domain is hosted on Server1 as an Active Directory integrated zone, and on Server3 as a secondary zone.

All the client computers on Segment B are Windows 2000 Professional computers. All the client computers on Segment A are down-level client computers. All the client computers use DHCP.

You share some network resources on several of the client computers on Segment A. Several days later you attempt to connect to those shared resources from client computers running on segment B, but you are unable to resolve the host names of client computers on Segment A.

How should you correct this problem?

Exhibit:

A. On the DHCP server, set the DNS Domain Name scope option to millertextiles.com.
B. On Server1 for the millertextiles.com zone, change the value of **Allow Dynamic Updates** from the default settings to **Yes**.
C. Configure the millertextiles.com domain to allow zone transfers to all the computers on the network.
D. On server2, enable updates for DNS clients that do not support dynamic updates.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: When a client on Segment B wants to access a shared resource on a computer on Segment A, it must first resolve the host name of the computer on Segment A to an IP address. This type of name resolution is performed by DNS. In this scenario, however, the clients are unable to resolve the host names to IP addresses because there are no entries in the DNS for the clients on Segment A. The clients on Segment A are down-level clients and are therefore unable to update DNS with information about the resources and services running on the machines. This problem can be overcome by manually entering the appropriate records in the DNS zone, or by configuring the DHCP server to update the records for the down-level clients. Enabling Server2, which is the DHCP server, to update DNS for the clients will enable the clients on Segment B to resolve their host names.

Incorrect Answers:
A: The millertextiles.com domain is hosted on Server1 as an Active Directory integrated zone, and on Server3 as a secondary zone. Therefore, the DNS Domain Name scope option is set to millertextiles.com on the DHCP server. This will therefore not update the DNS zones for the down-level clients. We should instead configure the DHCP server to update the records for the down-level clients.

B: Server1 has an Active Directory integrated zone, which would require that the value of Allow Dynamic Updates be set to Yes. As an Active Directory integrated zone, this option is already set. This will therefore not update the DNS zones for the down-level clients. We should instead configure the DHCP server to update the records for the down-level clients.

C: Configuring the millertextiles.com domain to allow zone transfers to all the computers on the network will not affect the down-level client's ability to update DNS. To enable the down-level clients to update DNS we should configure the DHCP server to update the records for the down-level clients.

QUESTION 4
You are the administrator of a Windows 2000 network. Your network consists of five sites in one domain. The Chicago, Los Angeles, and New York sites will have DNS running on their Domain Controllers. Miami and Seattle will have DNS running on dedicated member servers.

You want to allow client computers in the Chicago, Los Angeles, and New York sites to perform secure dynamic updates to the DNS server. You want to configure your DNS servers so that each site has a replicated copy of the DNS zone.

What should you do?

To answer, click the Select and Place button, and then drag the appropriate zone type to each site. (Note: zone types can be used more than once)

Place Zone Type Here
Los Angeles
Place Zone Type Here
Miami
Place Zone Type Here
Chicago
Place Zone Type Here
New York
Place Zone Type Here
Seattle

Select from
Active
Inte
Pr
Sec
Cac

Answer:

Section: (none)

Explanation/Reference:
Chicago: Active Directory integrated zone. Only Active Directory integrated zones support secure updates. Primary and secondary zones do not support secure updates. Cache only zones only keep records that have been resolved by passing the DNS query to a primary, secondary or Active Directory integrated zone.

Los Angeles: Active Directory integrated zone. Only Active Directory integrated zones support secure updates. Primary and zones do not support secure updates. Cache only zones only keep records that have been resolved by passing the DNS query to a primary, secondary or Active Directory integrated zone.

Miami: Secondary zone. A secondary zone is required for full zone replication. The question states a requirement for each location to have a full copy of the zone files. Only a secondary zone can receive a full

copy of a zone file from a primary or Active Directory integrated zone.

New York: Active Directory integrated zone. Only Active Directory integrated zones support secure updates. Primary and zones do not support secure updates. Cache only zones only keep records that have been resolved by passing the DNS query to a primary, secondary or Active Directory integrated zone.

Seattle: Secondary zone. A secondary zone is required for full zone replication. The question states a requirement for each location to have a full copy of the zone files. Only a secondary zone can receive a full copy of a zone file from a primary or Active Directory integrated zone.

QUESTION 5
You are the network administrator for Arbor Shoes. Part of your multisite Windows 2000 network configuration is shown in the exhibit.

Server1 is configured with the primary zone for arborshoes.com. Server3 and Server5 are configured with secondary zones for arborshoes.com.

You discover an error in several host records that is preventing client computers in Atlanta from accessing some shared resources. You make the necessary corrections on Server1.

You want these changes to be propagated to Atlanta immediately. What should you do?

A. On the **Action** menu for the arborshoes.com zone, click **Update Server Data Files**.
B. At server5, perform the **Transfer from master** action for the arborshoes.com zone.
C. At server1, stop and start the DNS server service.
D. At server5, select **Allow zone transfers** on the arborshoes.com zone.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: In this scenario we need to pull the new zone information from the primary server with immediate effect. This can be done through full zone replication by performing the transfer from master action for the arborshoes.com zone. This process is accomplished by the following actions:

1. Click Start, point to Programs, click Administrative Tools, and then double-click DNS to open the DNS Management Console.
2. In the navigation pane, expand the DNS server.
3. Expand the Forward Lookup Zones folder, and then find the secondary zone that you want to change.
4. Right-click the zone and then click "Transfer from master".

Incorrect Answers:
A: The Action menu is not used to initiate zone replication. For standard primary zones, this procedure causes the DNS server to immediately write its in-memory changes out to disk for storage with the zone file. Normally these changes are only written at predefined update intervals and when the DNS server is shut down.
C: In this scenario we need to pull the new zone information from the primary server with immediate effect. This can be done through full zone replication by performing the transfer from master action for the arborshoes.com zone. Stopping and restarting the DNS service will not force replication.
D: The “Allow zone transfers on the arborshoes.com zone” option is already set. This option also does not force replication.

QUESTION 6
Your company's network consists of two domains: contoso.com and sales.contoso.com. The contoso.com domain contains three Domain Controllers and one member server. The sales.contoso.com domain is a new

domain that contains one Domain Controller and one member server. You are a member of the Domain Admins group in sales.contoso.com.

You want sales.contoso.com to contain two Domain Controllers. Which two actions can you take? (Each correct answer presents a complete solution. Choose two)

A. Manually install a new server in sales.contoso.com. During the installation process, install the server as a Domain Controller.
B. Manually install a new member server in sales.contoso.com. After it is installed, promote the server to a Domain Controller.
C. Move the domain membership of the member server in contoso.com to sales.contoso.com by using **System Properties** in Control Panel.
D. Move the domain membership of the Domain Controller in contoso.com to sales.contoso.com by using **System Properties** in Control Panel.
E. Run DCPromo.exe on the member server in sales.contoso.com and provide credentials of a user in the Domain Admins group in sales.contoso.com
F. Run DCPromo.exe on the member server in contoso.com and provide credentials of a user in the Domain Admins group in contoso.com

Answer: BE
Section: (none)

Explanation/Reference:
Explanation:
B: To install a new Domain Controller we must first install a computer as a member server and then promote it to a Domain Controller. To promote a member server to a Domain Controller, we need to run the Active Directory installation wizard. We can do this by clicking Start, Run and typing DCPROMO and following the instructions in the wizard to install Active Directory.
E: We can also promote an existing member server to a Domain Controller at any time by running the Active Directory installation wizard.

Incorrect Answers:
A: Manually installing a new server as a Domain Controller during the server installation process was used on Windows NT 4.0 Server to install a Domain Controller. This process has changed in Windows 2000. We thus cannot install Windows 2000 as a Domain Controller during the installation process Instead we must first install a computer as a member server and then promote to a Domain Controller.
C: We cannot change the domain membership of a Domain Controller by using the control panel. We can use the System control panel on a Windows 2000 client to change its domain membership but not to create a Domain Controller.
D: We cannot change the domain membership of a Domain Controller by using the control panel. To change the domain membership of a Domain Controller, we would have to demote it to a member server first and then re-promote it to a Domain Controller in the new domain.
F: To run DCPromo.exe on a member server, you need to be an administrator of that domain, not the parent domain.

QUESTION 7
You are the administrator of your company's Windows 2000 network. Their network consists of four domains and five Active Directory sites. The network is configured as shown in the exhibit.

Each domain contains 500 Windows 2000 Professional computers. Each domain contains Human Resources administrators who must perform file maintenance on HR member servers located in Alabama.

In each domain, you create a global security group for all the HR administrators in that domain. In marketing. contoso.com you create a domain local security group named HRadmins. Then, you add the global security groups from each domain to HRadmins.

You want to ensure that only the designated global groups from each domain are members of the HRadmins group. What should you do?

Exhibit:

A. Create a Group Policy Object for marketing.contoso.com that restricts group access to the HRadmins group.
B. Create an OU name HRservers that contains only the HR member servers, and then create a Group Policy Object that restricts group access to the HRadmins group.
C. In each domain except marketing.contoso.com, create a Group Policy Object that restricts group access to the HRadmins group.
D. In each domain, create a Group Policy Object that restricts group access to the global security group in that domain.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: We can use the Restricted Groups option in group policy to restrict membership of a group. The Restricted Groups option controls two group settings. These are **Members** and **Members of.** If someone else tries to join a restricted group, they will be removed by group policy. Likewise, if someone's name is missing from the group, the name will be re-entered by the group policy. The Restricted Groups policy also restricts which groups the restricted group can be a member of. For example, if a restricted global group is a member of a domain local group, the restricted groups policy will enforce that group membership.

Incorrect Answers:
B: Placing the HR servers into an OU will not restrict access to the group.
C: In this scenario the Restricted Groups policy must be placed in the marketing.contoso.com domain and not the other domains since HRAdmins is a domain local group of the marketing.contoso.com domain.
D: In this scenario we must restrict access to the domain local group in the marketing.contoso.com domain, not the global groups.

QUESTION 8
Your company's network consists of a single Windows 2000 domain named contoso.com. You are a member

of the Domain Admins group. Employees in the Northeast region often modify their display settings, which is against company policy.

You link a Group Policy Object named NoDisplay to an OU named NorthEast. The NoDisplay Group Policy Object removes the Settings tab from Display in Control Panel. However, when you attempt to use Display in Control Panel to change the Display settings on your own computer, the Settings tab is gone.

You want only members of the Domain Admins group to be able to use the Settings tab in Display in Control Panel. Which two courses of action can you take?

(Each correct answer presents a complete solution. Choose two)

A. Create a security group named NorthEast, and add all nonadministrative users accounts in the Northeast OU to the NorthEast group.
   Grant only the NorthEast group the apply group policy permissions and the read permission for the NoDisplay GPO.
B. Create a security group named NorthEast, and add all nonadministrative computer accounts in the Northeast OU to the NorthEast group.
   Grant only the NorthEast group the apply group policy permissions and the read permission for the NoDisplay GPO.
C. Remove the Domain Admins group from the security list in the NoDisplay GPO.
D. Remove the Creator Owner group from the security list in the NoDisplay GPO.
E. Grant the Domain Admins group the Full Control: Allow permission for the NoDisplay GPO.
F. Grant the Domain Admins group the apply policy:Deny permission for the Nodisplay GPO.

Answer: AF
Section: (none)

Explanation/Reference:
Explanation:
A: We want only members of the Domain Admins group to be able to use the Settings tab in Display in Control Panel therefore the Group Policy Object named NoDisplay must not be applied to the admins group. One way is to place all the northeast users in one group and filter the policy to that group through the use of permissions. To be affected by a group policy, a user or group needs to have the Read and Apply Group Policy permissions. By giving these permissions to everyone in the northeast OU except the admins, we can ensure the policy does not affect the admins group.

F: To be affected by a group policy, a user or group needs to have the Read and Apply Group Policy permissions. Granting the Domain Admins group the deny permission for the group policy object will stop the policy applying to them. The deny permission overrides all other permissions on the group policy that the members of the Domain Admins group might have in other security contexts.

Incorrect Answers:
B: Adding all nonadministrative computer accounts to the security group named NorthEast, and granting only the northeast group the apply group policy permissions and the read permission for the NoDisplay Group Policy Object will apply the policy on a computer basis and not a user basis. In other words, the policy will affect the computers. Members of the Domain Admins group will not see the tab on computers that have been affected by the policy while all users will be able to access the tab on should they log on to computers that have not been affected by the policy.
C: The default for a GPO is to apply to the authenticated users group. The Domain Admins group is a member group of this group. Therefore the policy would apply to them as well.
D: Removing the Creator Owner group from the security list in the NoDisplay Group Policy Object will not prevent the policy from being applied to the admins group.
E: A user or group needs to have the Read and Apply Group Policy permissions to be affected by a group policy therefore we need to deny the admins apply permission to the GPO, not allow it.

QUESTION 9
You are the administrator of your company's Windows 2000 network. The company has two offices that are connected by a WAN link. Each office is configured as an Active Directory site. Both company offices share an Active Directory application. During business hours, the application generates large amounts of changes in Active Directory.

You need to reduce the amount of WAN bandwidth used by these changes during business hours. What should you do?

A. Configure the intrasite replication topology generation to occur less frequently during business hours.
B. Enable slow link detection in the Default Domain Group Policy Object (GPO)
C. Enable slow link detection in the Default Domain Controllers Group Policy Object (GPO)
D. Configure intersite replication to occur less frequently during business hours.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: A site is comprised of one or more Internet Protocol (IP) subnets that are tied together by highspeed and reliable connections. We can configure the replication schedule over site links. Replication between sites is called intersite replication. Furthermore, by reducing the replication frequency during business, we will reduce the competition for resources and network bandwidth.

Incorrect Answers:
A: Intrasite refers to replication within a site. This type of replication does not make use of the WAN connection. Configuring replication within a site to occur less frequently will thus not reduce network traffic across the WAN and so will not affect WAN bandwidth. Instead, we should configure intersite replication to reduce the bandwidth being used by the WAN link.
B: Slow link detection is a mechanism used by Active Directory to determine the application of group policy. This mechanism is not used to reduce the network traffic by reducing the frequency of replication.
C: Slow link detection is a mechanism used by Active Directory to determine the application of group policy. This mechanism is not used to reduce the network traffic by reducing the frequency of replication.

QUESTION 10
You are a member of Enterprise Admins group in your company's network. The company office in Dublin has its own organizational unit (OU) named Dublin.

You hire Sophie as a LAN administrator for the Dublin office. Sophie needs to create user accounts in the Dublin OU. You do not want Sophie to have permissions to make any other changes to Active Directory.

In the Active Directory Users and Computers snap-in, you need to assign appropriate permissions entries for the Dublin OU. You need to decide where these permissions should be applied.

Which option should you choose?

A. The **Child objects only** option.
B. The **This object and all child objects** option.
C. The **User objects** option.
D. The **Organizational Unit objects** option.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: Sophie needs to be able to create user accounts in the Dublin OU only. She must not have permissions to make any other changes to Active Directory. We therefore need to restrict her permissions in the Dublin OU and any child OUs that may be added in the future. We can accomplish this by applying the appropriate permissions to the object and to its child objects.

Incorrect Answers:

A: Applying the appropriate permissions to the child objects only will prevent Sophie from creating objects in any child OUs; however, this restriction will be applied at the level of the child objects only. Sophie will therefore still not be able to create objects in the Dublin OU.
C: This is a bit of a trick question. Sophie needs to be able to create user accounts so that it is easy to think the permissions must be applied to the User objects. The question is asking where the permissions should be applied, not what they should be applied on. We need to restrict her access in the Dublin OU.
D: Sophie needs the appropriate permissions only in the Dublin OU. We must thus restrict her access to the Dublin OU only, and not all OUs.

QUESTION 11
You are the administrator of your company's Windows 2000 network. The network contains a UNIX server that is running BIND DNS and three Windows 2000 Domain Controllers. The Domain Controllers have DNS installed and are configured with Active Directory integrated zones. On the Windows 2000 DNS Domain Controllers, zone transfers are restricted to name servers for the domain.

You need to add the UNIX server as a backup DNS server and configure replication so that the data on the server is updated automatically.

What should you do?

A. On the UNIX server, create a secondary zone for the domain, and then change the SOA (Start of authority) record for the domain to the UNIX server.
B. On the UNIX server, create a secondary zone for the domain, and then add the UNIX server to the list of name servers.
C. On the UNIX server, create a standard primary zone.
On a Windows 2000 Domain Controller, add the UNIX server to the list of name servers, and then configure notifications to point to the UNIX server.
D. On the UNIX server, create a standard primary zone.
On a Windows 2000 Domain Controller, convert the Active Directory integrated zone to a secondary zone and direct it to the UNIX server to zone transfers.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: To ensure automatic zone replication, the UNIX server must have a secondary zone for the domain. It must also be added to the authorized list on the Windows 2000 servers.

Incorrect Answers:
A: The start of authority (SOA) record will not allow the server to pull zone data from the Windows 2000 servers. The SOA record should not be placed on a secondary DNS server.
C: The UNIX server needs a secondary zone, not a primary, as the UNIX servers are required as backup DNS servers.
D: The UNIX server needs a secondary zone, not a primary, as the UNIX servers are required as backup DNS servers.

QUESTION 12
You are the administrator of your company's Windows 2000 network. The network consists of three domains, and each domain contains computer accounts. The network is configured as shown in the exhibit.

Members of the Domain Admins group and the Help Desk group need to add client computers to each domain. You need to give these employees exclusive permissions to accomplish this task.

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

Exhibit:

A. In the **Add workstations to domain** policy for litware.com, replace the Authenticated Users group with the Help Desk group.
B. In the **Add workstations to domain** policy for each domain, replace the Authenticated Users group with the Help Desk group.
C. For each domain, remove permissions for the Authenticated Users group from the Computers container, and grant the Help Desk group the Full Control permission for the Computers container.
D. For litware.com, remove permissions for the Authenticated Users group from the Computers container, and grant the Help Desk group the Full Control permission for the Computers container.
E. In the **Bypass traverse checking** policy for litware.com, replace the Authenticated Users group with Help Desk group.
F. In the **Bypass traverse checking** policy for each domain, replace the Authenticated Users group with Help Desk group.

Answer: BC
Section: (none)

Explanation/Reference:
Explanation: As members of the Domain Admins group and the Help Desk group need to add client computers to each domain they will require the Add workstations to domain right for each domain and the permissions to create objects in the computers container.

Incorrect Answers:

A: In this scenario the policy must be applied in all domains, not just the root domain. Therefore, replacing the Authenticated Users group with the Help Desk group in the litware.com domain only will not meet the requirements of this scenario.
D: In this scenario the permissions must be applied in all domains, not just the root domain. Therefore, replacing the Authenticated Users group with the Help Desk group in the litware.com domain only will not meet the requirements of this scenario.
E: The bypass traverse checking right is a folder browsing issue and is thus not relevant to this scenario.
F: The bypass traverse checking right is a folder browsing issue and is thus not relevant to this scenario.

QUESTION 13
You are the network administrator for the Lucerne Real Estate Company. The network consists of one Windows 2000 domain named lucernerealestate.local. The network is not currently connected to the Internet.

You are installing a new domain named lucernerealestate1.local. During the promotion process, you receive the following error message: “The domain name specified is already in use on the network”.

What is the most likely cause of the problem?

A. The default-generated DNS domain name is already in use.
B. DNS domain names cannot be named iteratively
C. The default-generated NetBIOS domain name is already in use.
D. NetBIOS domain names cannot be named iteratively.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: The default NetBIOS name would be the first 15 characters of the DNS name. This would be the same as the one already used by the first domain. Both lucernerealestate.local and lucernerealestate1 will be truncated to the same NetBIOS name. This name would be lucernerealesta.

Incorrect Answers:
A: The DNS domain is a new domain. Therefore it is not yet in use.
B, D: This is not the problem at hand.

QUESTION 14
You are the enterprise administrator of a Windows 2000 domain. The domain has three Domain Controllers named DC1, DC2, and DC3.

Because of changed hardware requirements, you want to replace the Domain Controller named DC1 with a newer computer named DC4. You want DC4 to be a Domain Controller in the domain. You no longer want DC1 to function as a Domain Controller.

What should you do?

A. Install DC4 as a stand-alone server in a workgroup named WG. Restore a System State data backup of DC1 on DC4. On DC1, Use the Active Directory Installation wizard to remove Active Directory from DC1.
B. Install DC4 as a stand-alone server in a workgroup named WG. Disconnect DC1 from the network. Rename DC4 to DC1. On DC2, force replication of Active Directory to all its replication partners.
C. Install DC4 as a member server in the domain. On DC4, use the Active Directory installation wizard to install Active Directory on DC4. On DC1 use the Active Directory Installation wizard to remove Active Directory from DC1.

D. Install DC4 as a member server in the domain. On DC1 use the Ntdsutil to copy the Active Directory files to DC4. Use the Active Directory Installation wizard to remove Active Directory from DC1.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: To install a Domain Controller, we must first install the computer as member server. There after we can run the Active Directory installation wizard to promote the server to a Domain Controller.

By running the Active Directory installation wizard on a Domain Controller we would be able to demote the computer back to a member server.

Incorrect Answers:
A: The machine must be installed as a member server, not a stand-alone server, and then promoted to a Domain Controller.
B: The machine must be installed as a member server, not a standalone server, and then promoted to a Domain Controller.
D: You cannot promote DC4 to a Domain Controller by using Ntdsutil and copying the Active Directory files to DC4. The Ntdsutil is used to physically move the DNS database. We must run the Active Directory installation wizard on DC4 to promote it to a Domain Controller.

QUESTION 15
You are the administrator of a domain named fabrikam.com. The domain contains an OU named Finance that has 20 users. In the Active Directory Users and Computers console on a Domain Controller named DC1, you inadvertently delete the Finance OU. You want to reinstate the Finance OU.

What should you do?

A. Move the tombstoned Finance OU from the LostAndFound container to the original location.
B. Copy the sales OU from another Domain Controller in the contoso.com domain to DC1.
C. Perform an authoritative restore of the Finance OU from the last backup.
D. In the Active Directory Sites and Services console. Force replication from another Domain controller in the fabrikam.com domain.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: We need to perform an authoritative restore of the Sales OU so that the restored OU does not get deleted again when Active Directory next replicates.

Incorrect Answers:
A: The LostAndFound container is used by the Movetree utility. Movetree is used to move objects between domains. When some objects and information are not moved, these are classified as orphaned objects and are placed in an "orphan" container in the LostAndFound container in the source domain. However, the Sales OU was deleted therefore it will not be in the LostAndFound container.
B: The deletion of the Sales OU will be replicated to the other Domain Controllers. The other Domain Controllers will therefore also not have a copy of the Sales OU.
D: If you force a replication, the deletion of the Sales OU will be replicated to the other Domain Controllers because this was the last change to the Active Directory.

QUESTION 16
You are the administrator of your company's WAN. Your company has four locations connected by dedicated

256-Kbps leased lines. You install and configure a Windows 2000 Domain Controller at each location. For network performance reasons, you want to control the bandwidth usage and replication schedule of directory information to each Domain Controller in each location.

What should you do? (Choose two.)

A. Create a site for each location.
B. Create a site that spans all the locations.
C. Create server objects for each Domain Controller in every site.
D. Create server objects for each Domain Controller in its own site.
E. Copy all server objects from Default-First-Site-Name to each site.
F. Move each server object from Default-First-Site-Name to the appropriate site.

Answer: AF
Section: (none)

Explanation/Reference:
Explanation:
A: To control replication we must create a site so that we can schedule replication between the sites. In so doing we can reduce network traffic.
F: By default, all computers are in the Default-first-site-name. This is because they must be associated with a site. When we create a new site, we must associate the servers with the new site.

Incorrect Answers:
B: We must create a site at each location so that we can schedule replication between them, and in this reduce intersite communication.
C: We already have the server objects. We need to move the server objects to their respective sites. There should also only be one server object for each physical server.
D: We already have the server objects. We need to move the server objects to their respective sites. There should also only be one server object for each physical server.
E: The servers must be moved from the Default-First-Name-Site to the new site. They should not be copied, as they would then be associated with two sites. Furthermore, there should be only one server object for each physical server.

QUESTION 17
You are the administrator of your company's network. Your company has its main office in North America and has branch offices in Asia and Europe. The locations are connected by dedicated 256-Kbps lines. The network consists of one Windows 2000 domain. To minimize logon authentication traffic across the slow links, you create a site for each office and configure the site links between the sites.

Users in the branch offices report that it takes a long time to log on to the domain. You monitor the network and discover that all authentication traffic is still being sent to the Domain Controllers in the North America site.

What should you do to correct this problem?

A. Schedule replication to occur more frequently between the sites.
B. Schedule replication to occur less frequently between the sites.
C. Create a subnet for each physical location, associate the subnets with the North America site, and move server objects to the North America site.
D. Create a subnet for each physical location, associate each subnet with its respective site, and move each server object to its respective site.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: Sites define sets of Domain Controllers that are well connected in terms of speed and cost. A site is the equivalent of a set of one or more IP subnets. Subnets and servers need to be associated with sites otherwise the sites do not mean anything. The sites are used by the Active Directory service to schedule its replication of the Active Directory database. They are also used to make clients use local resources instead of remote resources. By associating subnets with sites there will be less network traffic.

Incorrect Answers:
A: In this scenario we are required to stop authentication traffic crossing the site links. Active Directory replication traffic is not relevant to authentication traffic.
B: In this scenario we are required to stop authentication traffic crossing the site links. Active Directory replication traffic is not relevant to authentication traffic.
C: The subnets and servers must be placed in their respective sites and should not be associated with the North America

QUESTION 18
You are the network administrator for your company. Your company's main office is in Seattle. Branch offices are in New York, Rome, and Tokyo. The local administrators at each branch office need to be able to control local resources.

You want to prevent the local administrators from controlling resources in the other branch offices. You want only the administrators from the main office to be allowed to create and manage user accounts. You want to create an Active Directory structure to accomplish these goals.

What should you do?

A. Create a domain tree that has a top-level domain for the main office and a child domain for each branch office. Grant the local administrators membership in the Domain Admins group in their child domains.
B. Create a domain tree that has a top-level domain for the main office and a child domain for each branch office. Grant the local administrators membership in the Enterprise Admins group in the domain tree.
C. Create a single domain. Create a group named Branch Admins. Grant the local administrators membership in this group. Assign permissions to the local resources to this group.
D. Create a single domain. Create an organizational unit (OU) for each branch office and an additional OU named CorpUsers. Delegate authority for resource administration to the local administrators for their own OUs. Delegate authority to the CorpUsers OU only to the Domain Admins group.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: With Active Directory, we can use Organizational Units as a basis for the delegation of authority. In this scenario, we could create a single domain with an Organizational Unit for each branch office. We could then delegate authority for resource administration, but not user administration, to the local administrators for their own OUs. This will permit the local administrators of each branch office to manage resources in that region but would not allow them to manage user accounts. By creating another OU and delegating authority to that OU only to the Domain Admins group we will allow only the Domain Admins group to administer user accounts.

Incorrect Answers:
A: It is not necessary to create multiple domains. We could instead create a single domain with an Organizational Unit for each branch office. We could then delegate authority for resource administration, but not user administration, to the local administrators for their own OUs. In addition, we could create another OU and delegate authority to that OU only to the Domain Admins group. This will allow the Domain Admins group to administer user accounts. Furthermore, the creation of multiple domains would increase administrative

requirements.
B: By granting the local administrators membership in the Enterprise Admins group in a domain tree that has a top-level domain for the main office and a child domain for each branch office, we allow the local administrators to manage resources and user accounts in the forest.
C: Create a single domain. Create a group named Branch Admins. Grant the local administrators membership in this group. We must use Organizational Units as a basis for the delegation of authority for resources.

QUESTION 19
You are the administrator of a Windows 2000 domain. The domain has two Domain Controllers named Server1 and Server2. The volume that contains the Active Directory database file on Server1 is running out of disk space. You decide to move the database file to an empty volume on a different disk on Server1.

What should you do?

A. Restart Server1 in directory services restore mode. Use the Ntdsutil utility to move the database file to the empty volume.
B. Use Windows Backup to create a backup of the System State data of Server1. Restart Server1 in directory services restore mode. Restore the system State data to the empty volume.
C. Use the Disk Management console to mount the empty volume in the folder that contains the Active Directory database file.
D. Stop the Net logon service on Server1. Use Windows Explorer to move Ntds.dit to the empty volume. Start the Net Logon service again. Force replication from server2.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: The Ntdsutil command-line utility in Directory Services Restore mode is used to move the Active Directory database. This utility automatically updates the registry keys so that Active Directory will start from the location it was moved to. We can enter the Directory Services Restore Mode by pressing F8 to display the Windows 2000 Advanced options menu. We must logon using the Administrators account and type NTDSUTIL at the command prompt, specify files, then type 'MOVE DATABASE TO [drive letter:\directory name]'. Finally, we must reboot the Domain Controller for the changes to take effect.

Incorrect Answers:
B: Although it is possible to restore the System State data to a new location, Active directory will still use the original database, as this was not removed. Should we delete the original database, we would need to alter the registry keys manually so that Active Directory can start from the new location. This is a daunting task that could render the computer unbootable if the registry is incorrectly altered. This is thus not recommended procedure. We should therefore use the Ntdsutil command-line utility instead.
C: We can only mount a volume to a folder that is empty. We would therefore have to move the database first.
D: It is possible to copy the Ntds.dit file to another volume but we would also have to alter the registry keys manually so that Active Directory can start from the new location. This is a daunting task that could render the computer unbootable if the registry is incorrectly altered. This is thus not recommended procedure. We should therefore use the Ntdsutil command-line utility instead.

QUESTION 20
You are the administrator of your company's network. Your company has two domains in six sites as shown in the exhibit.

Each site has one or more Domain Controllers. For fault-tolerance and load-balancing purposes, one Domain Controller in each site is configured as a Global Catalog server. Users report that, several times a day, network performance and data transfer for an application located in SiteA are extremely poor.

You want to improve network performance. What should you do?

Exhibit:

A. Configure at least two Domain Controllers in each site as Global Catalog servers.
B. Configure the Domain Controllers in only one site as Global Catalog servers.
C. Create site links between all sites and use the default replication schedules.
D. Create site links between all sites and set less frequent replication schedules.
E. Create connection objects between each Domain Controller. Use RPC as the transport protocol.
F. Create connection objects between each Domain Controller. Use SMTP as the transport protocol.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: When we create sites, we must also create site links, as site links are used to facilitate and configure replication between sites. We can set the replication schedule over site links and can reduce the frequency of replication, which will improve network performance.

Incorrect Answers:
A: In this scenario, Active Directory replication is the cause of the network traffic. Adding more Global Catalog servers will thus not reduce network traffic. Furthermore, there should be no need for more than one Global Catalog server at each site.

B: Configuring the Domain Controllers in only one site as Global Catalog servers would result in an increase in network traffic, as logon information would need to cross the site links.
C: In this scenario we need to configure the replication to be less frequent.
E: The network protocols have a minor affect on bandwidth usage in comparison to the replication frequency. We should thus configure the replication to be less frequent instead.
F: The network protocols have a minor affect on bandwidth usage in comparison to the replication frequency. We should thus configure the replication to be less frequent instead.

QUESTION 21
You are the administrator of a Windows 2000 domain. The domain has a Windows 2000 Server computer named Central.

Users in the domain frequently work on different Windows 2000 Professional desktop and portable computers. They use the Windows 2000 Professional portable computers to dial in to the network when they are travelling. All Windows 2000 Professional computers are in the domain.

You want to accomplish the following goals:

- All users in the domain will be able to work on all Windows 2000 Professional desktop and portable computers and have their own desktop settings available on all computers.
- All users in the domain will be able to access their documents in the My Documents folder from any computer, including the portable computers when users dial in to the network.
- When users dial in to the network, the logon and logoff times will not be delayed because of the transfer of the contents of the My Documents folder

What should you do? (Choose two.)

A. Configure a roaming Profile for each user in the domain.
Use \\Central\Profiles\%Username% as the Profile path.
B. Configure a home folder for each user in the domain.
Use \\Central\Home\%Username% as the home folder path.
C. Create a new Group Policy object (GPO) named Offdocs.
Assign the Offdocs GPO to the domain.
Configure the Offdocs GPO to prevent the use of the Offline Files folder.
D. Create a new Group Policy object (GPO) named Redocs.
Assign the Redocs GPO to the domain.
Configure the Redocs GPO to redirect the My Documents folder to the \\Central\Docs\%Username% location.
E. Create a new Group Policy object (GPO) named Async.
Assign the Async GPO to the domain.
Configure the Async GPO to apply Group Policy Object settings for users asynchronously when they log on.

Answer: AD
Section: (none)

Explanation/Reference:
Explanation:
A: We must create roaming profiles, as they are required by users who logon to the network from different locations or computers but who require the same desktop setting regardless of where they logon.
D: We must then redirect the logon to the My Documents folder so that the files in the My Documents do not get downloaded as part of the roaming profile logon process. By redirecting the My Documents folder, the roaming profile will access the folder on the network location rather than down loading it onto the logon computer. This will reduce network traffic.

Reference:

Configuration of the My Documents Folder (Q221837)
Windows 2000 Server documentation, Folder Redirection

Incorrect Answers:
B: Home folders are not appropriate to this scenario. We need to redirect My Documents.
C: Offline files are not appropriate to this scenario. We need to redirect My Documents.
E: The GPO will not redirect the My Documents folder and so will not affect the logon speed.

QUESTION 22
You are the administrator for your company. You are deploying Windows 2000 Professional on your network by RIS. Your company has several departments.

To expedite the deployment of Windows 2000 and other third party application, you have created a group named Department Managers. You want to allow members of the Department Managers group access to create custom images and post them to the RIS servers for deployment. In addition, you want to allow members of the group to install client computers from the RIS server.

What should you do?

A. Grant the Department Managers group Read and Write permissions to the Remoteinstall folder.
B. Grant the Department Managers group Read and Write permissions to the OSChooser folder.
C. Grant the Department Managers group Full Control permissions to the RIPrep.exe.
D. Grant the Department Managers group Full Control permissions to the SysPrep utility.
E. Grant the Department Managers group Read and Write permissions to the Admin folder.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: To write images to the RIS folder, the members of the Department Managers group require write permissions to the Remoteinstall folder. To install the RIS image on the computers, the members of the Department Managers group require read permissions to the Remoteinstall folder.

Incorrect Answers:
B: The members of the Department Managers group do not require full control access to the RIPrep.exe utility. They only require read permissions to the utility to be able to execute it in order to create the RIS images.
C: The sysprep utility is used to remove the unique security identification information from a computer. It is not required for the installation of Windows 2000 Professional using RIS images.
D: The members of the Department Managers group require the appropriate permissions on the Remoteinstall folder and not the admin folder.

QUESTION 23
You are the administrator of a Windows 2000 domain. The domain has an Organizational Unit (OU) named Staff. Users in the Staff OU frequently work on different Windows 2000 Professional computers. All Windows 2000 Professional computers are in the domain. The domain also has a Windows 2000 Server computer named ServerA.

You want to accomplish the following goals:

- Users in the Staff OU will receive their user profile settings at every Windows 2000 Professional computer in the domain
- Each user in the Staff OU will be able to gain access to the documents in the user's My Documents folder from any Windows 2000 Professional computer in the domain
- To reduce network traffic, documents in users' My Documents folders will not be automatically copied to or

from the server when users logo on to or log off of the domain

What should you do? (Choose all that apply)

A. Configure a roaming profile for each user in the Staff OU.
   Use \\ServerA\Profiles\%Username% as the profile path.
B. Create a new Group Policy Object named Profile.
   Assign the profile GPO to the staff OU.
   Configure the profile GPO to redirect the Desktop folder to \\ServerA\Profiles\%Username%
C. Create a new Group Policy Object named Redirect.
   Assign the Redirect GPO to the staff OU.
   Configure the Redirect GPO to redirect the My Documents folder to \\ServerA\Profiles\%Username%
D. On the Windows 2000 Professional computers, share the My Documents folder.
   Configure the My Documents share to prevent files in the shared folder from being cached.

Answer: AC
Section: (none)

Explanation/Reference:
Explanation:
A: We must create roaming profiles, as users who logon to the network from different locations or computers but who require the same desktop setting regardless of where they logon require them.

C: We also need to redirect the My Documents folder to the profile folder so that the users can access their files wherever they logon from. This is accomplished by creating a new GPO, configuring the GPO to redirect My Documents folders to a specific network share for each individual user, and assigning the GPO to the appropriate OU.

Note:
The redirection of my Documents folder will:
I. Force the contents of My Documents folder to be moved to the network share.
This move will only occur once.
II. Change the destination path of the My Documents shortcut. Instead of a shortcut to a folder on the local hard drive the My Documents shortcut will point to a network share.

The user will transparently be redirected to the files and folders in the network share when he uses the My Documents folder. Notice that the files in the My Documents folder in the network share will not be copied during logon and logoff. No extra network traffic will occur. Only the shortcut path of the My Documents folder needs to be configured.

Reference:
Configuration of the My Documents Folder (Q221837)
Windows 2000 Server documentation, Folder Redirection

Incorrect Answers:
B: The desktop folder is already part of the roaming profile therefore we do not have to redirect the desktop folder.
D: It is not necessary to share the My Documents folders because they can be redirected to the server.

QUESTION 24
Your company is deploying Windows 2000 Professional on a network of 300 computers. The network has two Windows 2000 Server computers. You have only enough Windows 2000 Professional licenses for 250 users.

You need to restrict the department so that Windows 2000 Professional can be installed on only the licensed computers. You will need to minimize user intervention during the deployment and centralize the installation

files.

What should you do?

A. Create a shared folder on one of the servers. Copy the source files from the Windows 2000 Professional CD-ROM to the shared folder. Allow users to perform attended installations from the shared folder on only the licensed computers.
B. Install RIS on one of the servers. Create user accounts for all the licensed users. Configure the RIS sever to accept the connections from only known computers. Perform unattended installations for all connecting computers.
C. Create a shared folder on one of the servers. Restrict access to the share so that only 250 users can connect. Copy the source files from the Windows 2000 Professional CD-ROM to the shared folder. Allow users to perform unattended installation from the shared folder.
D. Install RIS on one of the servers. Create computer accounts in the domain for only the licensed computers. Configure the RIS server to accept connections from only known computers. Perform unattended installations from the shared computers.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: By creating computer accounts in the domain for only the licensed computers, i.e. using prestaged computer accounts, we can restrict which computers Windows 2000 Professional will be installed on.

Incorrect Answers:
A: As all users will have access to the shared folder to which the files from the Windows 2000 Professional CD-ROM have been copied, they will be able to install Windows 2000 Professional on any of the computers, not just those for which licenses exist.
B: Only computer accounts can be used when making use of prestaged accounts. We must therefore create computer accounts and not user accounts.
C: As all users will have access to the shared folder to which the files from the Windows 2000 Professional CD-ROM have been copied, they will be able to install Windows 2000 Professional on any of the computers, not just those for which licenses exist. By restricting the number of simultaneous connections to the folder to 250 we would restrict access to 250 users at any one time. However, as soon as a user disconnects from the folder another user can connect to it and will be able use the RIS image to install Windows 2000 Professional on any computer.

QUESTION 25
You are the administrator of a Windows 2000 Domain. The domain has an Organizational Unit (OU) named Support. Users in the Support OU frequently use their portable computers when they are not connected to the network. The portable computers are Windows 2000 Professional computers in the support Organizational Unit.

The domain also has a Windows 2000 Server computer named data3. The \\data3\Supfiles share contains files that are needed by users in the Support Organizational Unit.

You want to accomplish the following goals:

- Users in the Support Organizational Unit will be able to access files at \\Data3\SupFiles when they use their portable computers while they are not connected to the network.
- The total disk space used on portable computers to automatically store files from the \\Data3\SupFiles share and other server locations will not exceed 5% of the hard disk space.

What should you do? (Choose all that apply)

A. Configure the SupFiles share on the Data3 server to cache documents automatically.
B. Create a new Group Policy Object (GPO) named EXfolder.
Assign the EXfolder GPO to the Support OU.
Configure the EXfolder GPO to exclude the \\Data3\SupFiles from the roaming profiles.
C. Create a new Group Policy Object named Maxdisk.
Assign the Maxdisk GPO to the Support OU.
Configure the Maxdisk Group Policy Object to limit the automatically cache off line files to 5% of the hard disk space.
D. Create a new Group Policy Object named Maxsize.
Assign the Maxsize GPO to the Support OU.
Configure the Maxsize GPO to limit the size of each user Profile to 5% of the hard disk space.

Answer: AC
Section: (none)

Explanation/Reference:
Explanation:
A: By configuring the SupFiles share on the data3 server to cache documents automatically, we would make the files in the SupFiles share available for offline use.
C: We can then limit the hard drive space that the offline files occupy by creating a Group Policy Object, assigning it to the OU and configuring the Group Policy Object to automatically cache off line files up to a maximum of 5% of the hard disk space.

Incorrect Answers:
B: The files in the \\data3\supfiles will not be part of the profiles. It will therefore not be necessary to create a GPO that will be configured to exclude those files.
D: In this scenario we must limit the size of the offline files, and not the size of the profiles. We must therefore create a Group Policy Object, assign it to the OU and configure the Group Policy Object to automatically cache off line files up to a maximum of 5% of the hard disk space.

QUESTION 26
Your company's Windows 2000 Domain contains an Organization Unit named Shipping. The domain is in native mode. You want to delegate the control of the group policy setting for the shipping OU to a global group named Help Desk.

Members of the Help Desk group need to able to create and edit new GPOs and assign these GPOs to the shipping OU. You do not want these members to assign GPOs to other OUs.

What should you do? (Choose two)

A. Add the Help Desk group to the Group policy Creator Owners security group.
B. Create a new security group name group policy administrator in the shipping OU. Add the Help Desk group to this new group.
C. On the existing GPO, assign read and write permission to the Help Desk group.
D. On the shipping OU, assign the apply group policy permission in the Help Desk group.
E. On the shipping OU, delegate the predefined task Manage group policy links to the Help Desk group.
F. On all the OUs in the domain accept the shipping OU, deny write permissions to the Help Desk group.

Answer: AE
Section: (none)

Explanation/Reference:
Explanation: By default, only Domain Administrators, Enterprise Administrators, Group Policy Creator Owners, and the operating system can create new Group Policy objects. If the domain administrator wants a

non-administrator or group to be able to create Group Policy objects, that user or group can be added to the Group Policy Creator Owners security group. When a non-administrator who is a member of the Group Policy Creator Owners group creates a Group Policy object, that user becomes the Creator Owner of the Group Policy object. Then the user can edit the Group Policy object. Being a member of the Group Policy Creator Owners group gives the non-administrator full control of only those Group Policy objects that the user creates or those explicitly delegated to that user. It does not give the user full control of any other Group Policy objects, and does not allow the user to link Group Policy objects to sites, domains, or organizational units.

Active Directory supports security settings on individual properties. Thus, a non-administrator can be given Read and Write access to specific properties. If non-administrators have Read and Write access to the gPLink and gPOptions properties, they can manage the list of Group Policy objects linked to that site, domain, or organizational unit. To give a user Read and Write access to these properties, use the Delegation of Control Wizard and select the Manage Group Policy links predefined task. In this scenario we must give nonadministrators, the help desk group, rights and permissions on a specific OU. The helpdesk group needs to be able to create new GPOs; edit existing GPOs linked to the OU; and link new GPOs to the OU.

Incorrect Answers:
B: The help desk employees have already been placed in a group. Permissions and rights can be assigned to this group. It is therefore not necessary to create another group to place the Helpdesk group in.
C: If the help desk group had read and write permissions on the OU, they would be able to create any objects within the OU.
D: All authenticated users have the apply group policy permission by default. Therefore it is not necessary to assign the apply group policy permission in the help desk group.
F: Assigning the deny write permissions to the help desk group on all the OUs in the domain accept the shipping OU, would be a daunting administrative task, and would have to be done every time new a OU is created in the domain.

QUESTION 27
You are the administrator of Windows 2000 Domain. You want to deploy a new application named Finance that will be used by all users in the domain. The vendors of the Finance application supplied a Microsoft Windows Installer package for the application.

You decide to deploy the Finance application in two phases. During phase 1, only members of a security group named Finance Pilot will use the Finance application. During phase 2, all users in the domain will be able to install the Finance application.

You want to accomplish the following goals:

- During phase 1, the Finance application will not be installed automatically when users logon.
- During phase 1, users who are members of Finance Pilot group will be able to install the Finance application by using a Start menu short cut.
- During phase 1, users who are not members of the Finance Pilot group will not be able to install the Finance application by using a Start menu short cut.
- The Finance application will be installed automatically the first time any user in the domain logs on after phase 2 has begun.

You take the following actions:

- Create a new Group Policy Object (GPO) named Deploy Finance App and link the Deploy Finance App GPO to the domain.
- Configure the Deploy Finance GPO to assign the Finance application to users.
- For phase 1, create a software category named Finance Pilot. Assign the Finance application to the Finance Pilot software category.
- For phase 2, remove the finance application from the finance Pilot software category.

Which result or results do these actions produce? (Choose all that apply)

A. During phase 1, the Finance application will not be installed automatically when users logon.
B. During phase 1, users who are members of Finance Pilot group can install the Finance application by using a **Start** menu short cut.
C. During phase 1, users who are not members of the Finance Pilot group cannot install the Finance application by using a **Start** menu short cut.
D. The Finance application will be installed automatically the first time any user in the domain logs on after phase 2 has begun.

Answer: AB
Section: (none)

Explanation/Reference:
Explanation:
A: Only applications assigned to computers will be automatically installed and during phase 1 we only assign the application to users.

B: The application is assigned to users. Therefore, all users would be able to install the application, including the users in the Finance Pilot group.

Note 1: In this scenario the finance application was assigned and not published to users. The application will therefore not be automatically installed when users log on but will be advertised to the user the next time the user logs on to the network regardless of which computer the user actually uses to log on. The application is installed the first time the user activates the application on the computer, either by selecting the short cut to application on the start menu or by activating a document associated with the application.

Note 2: In Windows 2000 we can manage the installation of software on a client computer centrally by assigning applications to users or computers or by publishing applications for users. When we assign an application to a user, the application is advertised to the user the next time the user logs on to the network regardless of which computer the user actually uses to log on. The application is installed the first time the user activates the application on the computer, either by selecting the short cut to application on the start menu or by activating a document associated with the application. When we assign an application to a computer, the application is advertised and is installed when there are no other applications running on the computer. This usually occurs when the computer next starts up. When we publish an application to a user, the application does not appear installed on the users' computers and no shortcut to it is visible on the desktop or the start menu. Instead, the application is available for the user to install using Add/Remove Programs in Control Panel or by clicking a file associated with the application. We cannot publish an application to a computer.

Incorrect Answers:
C: The GPO was applied to the domain therefore everyone will be able to install the application.
D: For the finance application to be installed automatically the first time any user in the domain logons, the GPO would have to be assigned to computers.

QUESTION 28
You are the administrator of a Windows 2000 domain. You want to deploy an application named Travel that will be used by all users in the domain. The vendor of the application did not provide a Microsoft Windows installer package for the application. When the application is installed, it uses the .tvl file name extension. You want to use group policy to deploy the application.

You want to accomplish the following goals:

- Users will be able to install the application by using Add/Remove Programs.
- Users will be able to install the application by using a Start menu shortcut.
- Users will be able to install the application by using document invocation.
- The application will be automatically reinstalled if key application files are missing.

You take the following actions:

- Create a zero administration package (.zap) text file that specifies how to install the travel application.
- Copy the .zap file to a shared folder on the network.
- Create a new Group Policy Object named Install Travel and assign the Install Travel Group Policy Object to the domain.
- Configure the Install Travel Group Policy Object to publish the travel application to users by using the .zap file.

Which result or results do these actions produce? (Choose all that apply)

A. Users can install the application by using **Add/Remove programs**.
B. Users can install the application by using a **Start** menu shortcut.
C. Users can install the application by using document invocation.
D. The application is automatically reinstalled if key application files are missing.

Answer: AC
Section: (none)

Explanation/Reference:
Explanation:
A: The application is published so you are able to install it through the Add/Remove programs Control Panel applet.
C: Published applications can be installed by document invocation.

Note: In Windows 2000 we can manage the installation of software on a client computer centrally by assigning applications to users or computers or by publishing applications for users. When we assign an application to a user, the application is advertised to the user the next time the user logs on to the network regardless of which computer the user actually uses to log on. The application is installed the first time the user activates the application on the computer, either by selecting the short cut to application on the start menu or by activating a document associated with the application. The latter means of installation is called document invocation. When we assign an application to a computer, the application is advertised and is installed when there are no other applications running on the computer. This usually occurs when the computer next starts up. When we publish an application to a user, the application does not appear installed on the users' computers and no shortcut to it is visible on the desktop or the start menu. Instead, the application is available for the user to install using Add/ Remove Programs in Control Panel or by document invocation. We cannot publish an application to a computer. In this scenario the application was publish to the user. It will thus appear in Add/remove programs. Furthermore, when an application is assigned or published, it can be installed by document invocation.

Incorrect Answers:
B: In this scenario we published the application to the users. When we publish an application to a user, the application does not appear installed on the users' computers and no shortcut to it is visible on the desktop or the start menu. Instead, the application is available for the user to install using Add/Remove Programs in Control Panel or by document invocation. A start menu shortcut would only appear if we assigned the application to the user.

D: Only applications that have been installed with a Microsoft Installer package, i.e. applications that have been installed by using the .msi file, can be automatically reinstalled if key application files are missing. In this scenario a .zap file was used to install the application. The application therefore cannot be automatically repaired.

QUESTION 29
You are the administrator of a Windows 2000 network. You are configuring RIS to deploy Windows 2000 Professional on new client computers. New users report that when they attempt to install their computers, they are unable to get an IP address.

What should you do?

A. Authorize the DHCP server in DHCP console.
B. Configure each computer to boot from a remote installation boot disk.
C. Create a reservation in DHCP for each client.
D. Start the Boot Information Negotiation Layer (BINL) service on the RIS server.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: When a client is unable to acquire an IP address during startup the problem usually concerns the DHCP server or connectivity to the DHCP server. An unauthorized DHCP server might cause this problem. You authorize a DHCP Server in the Active Directory through the DHCP console.

Note: Remote boot load sequence:
1. Client receives IP address
   Problems in this step might include: unavailable DHCP server, unauthorized DHCP server, incorrectly configured DHCP server.
2. Client contacts remote installation service.
3. Client receives the first image file files.
   Problems in this step might include a stopped BINL service.
4. Client installation Wizard starts.

Reference: Windows 2000 Documentation, Troubleshooting Remote Installation Services

Incorrect Answers:
B: It is not necessary to create boot disks for the computers. If the clients were not PXE-compliant, they would receive boot error messages.
C: The RIS server does not require the creation of a reservation in DHCP for each client.
D: A stopped BINL service could cause this problem, but it less likely and it would result in a more specific error message.
Note: The BINL service is added during the RIS installation process and provides overall management of the RIS environment. The BINL service is responsible for answering client computer network service requests, querying Active Directory on behalf of the client computer, and ensuring that the correct policy and configuration settings are applied to the client computer during the OS installation. The BINL service makes sure the client is passed the correct files and, in the case of a prestaged client, makes sure it is serviced by the correct RIS server. If the client computer has not been prestaged, BINL creates the client computer account object within Active Directory.

QUESTION 30
You are the administrator for your company's network. You are deploying Windows 2000 on your network of 10,500 users. There are 15 departments in your company. Each department needs to use specific features of Windows 2000 and custom third-party applications.

You want to minimize the administrative time required to set up the client computers. You also want to provide customized software installations to the users.

What should you do?

A. Install and configure a RIS Server on your network.
   Use RIPrep.exe to create multiple images for each department.
   Connect the client computers to the RIS Server and deploy the custom images.

B. Install and configure a RIS Server on your network.
Create different installation script files for each department.
Deploy the computers by using RIS.

C. Create a shared folder on one of the servers.
Copy the source files from the Windows 2000 Professional CD-ROM to the shared folder.
Perform unattended installations from the shared folder by using script files, and then install the thirdparty applications.

D. Create a shared folder on one of the servers.
Copy the source files from the Windows 2000 Professional CD-ROM to the shared folder.
Perform attended installations from the shared folder, and then select only the components you need for each department.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: The quickest way to create an image of each configuration in this scenario would be to install and configure a RIS Server on our network and use the RIPrep.exe utility to create multiple images for each department. We can then connect the client computers to the RIS Server and deploy the custom images.

When creating the RIS image we must;
1. Use Remote Installation Services to remotely install the base Windows 2000 Professional operating system.
2. Install client computer applications that do not adhere to the Windows Installer technology.
3. Configure the source computer to conform to any company desktop standards required. For example, you might want to define specific screen colors, set the background bitmap to a company-based logo, remove any games installed by the base operating system, and configure Internet Explorer proxy settings.
4. Close all applications and run the Remote Installation Preparation (RIPrep) wizard.
5. The wizard configures the source computer to a generic state, removing anything that is unique to the client installation, such as the computer's unique security ID (SID), computer name, and any registry settings unique to the client source computer.
6. The wizard prompts us for the installation information required by the image conversion process. This information includes the location where the client installation image should be replicated, the name of the directory it should be copied to on the server, and a friendly description and associated Help text describing the installation image to users running the Client Installation wizard.
7. After the replication is complete, the installation image is automatically added to the list of available operating system installation options and is available to client computers that use the remote boot technology.

Incorrect Answers:
B: Windows 2000 does not make provision for the use of scripts when performing RIS installations.
C: Performing unattended installations from a shared folder by using script files and then installing the thirdparty applications on each computer would not be a fully unattended installation. It would also require extensive administrative effort.
D: Performing attended installations from a shared folder, and then selecting only the components required for each department would not be a fully unattended installation. It would also require extensive administrative effort.

QUESTION 31
You are the administrator of a Windows 2000 domain. The domain has an organizational unit named Help Desk. A Group Policy Object (GPO) named disable Regedit is assigned to Help Desk OU. The only policy defined in the disable Regedit GPO is the policy setting that disables the use of registry editing tools.

For performance reasons, your company wants to minimize the number of GPOs that are processed at logon. The company also decides that the restriction on the use of the registry editing tools must no longer apply to the users in the Help Desk OU.

What should you do to accomplish these goals?

A. Remove the disable Regedit Group Policy Object from the Help Desk OU.
B. Assign a new Group Policy Object to the Help Desk OU that enables the use of registry editing tools.
C. On the computers used by users in the Help Desk OU, edit the registry to allow the use of registry editing tools.
D. On the computers used by users in the Help Desk OU, configure the local Group Policy Object to allow the use of registry editing tools.
E. On the computers used by users in the Help Desk OU, delete the Registry.pol file from the systemroot/ system32/GroupPolicy folder.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: When a Group Policy Object is no longer required it can simply be removed. This will improve the logon process, as the GPO will no longer have to be processed when a user logs on to the network.

Incorrect Answers:
A: Adding a GPO, which would change the settings in the existing GPO, is unnecessary as we can simply remove the existing GPO. Furthermore, the order in which these two GPOs are processed would be crucial as to which GPO settings are set. Should the disable Regedit Group Policy Object be processed after the new GPO, the setting prescribed by the disable Regedit Group Policy Object would be in effect.
B: In this scenario it would not be possible to use the registry tools, as the disable Regedit Group Policy Object has disabled the Regedit utility.
C: Configuring the local Group Policy Object to allow the use of registry editing tools would not solve the problem in this scenario as the disable Regedit Group Policy Object would override the local configuration.
D: The Administrative Templates extension of Group Policy saves information in Registry.pol files. These files cannot be used to remove the restrictions put in place by the disable Regedit Group Policy Object.

QUESTION 32
You are the administrator for Coho Vineyard. You are using RIS to deploy Windows 2000 on your network. You want to direct your client computers to specific RIS servers for deployment. You cannot find the GUIDs on several of the client computers. You need the GUIDs to finish your deployment process.

What should you do?

A. Use Network Monitor to capture the DHCPDiscover frames from the client computers. Search the data fields for the GUIDs in hexadecimal format.
B. Use Network Monitor to capture the DNS frames from the client computers. Search the data fields from the GUIDs in hexadecimal format.
C. Use Network Monitor to capture the DHCPRequest frames from the client computers. Search the data fields for the GUIDs in hexadecimal format.
D. Use Network Monitor to capture the DHCPOffer frames from the client computers. Search the data fields for the GUIDs in hexadecimal format.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: When a client requires an IP address, it broadcasts a DHCPDISCOVER packet, which includes the Globally Unique Identifier (GUID), to find a DHCP server. The DHCP server then responds by sending a DHCPOFFER packet to which the client answers: with a DHCPREQUEST packet. Finally the DHCP server acknowledges the lease with DHCPACK packet.

Incorrect Answers:
A: The Globally Unique Identifier (GUID) is included in the DHCPDISCOVER packet and not in the DNS frames.
B: The Globally Unique Identifier (GUID) is included in the DHCPDISCOVER packet and not in the DHCPRequest frames.
C: The Globally Unique Identifier (GUID) is included in the DHCPDISCOVER packet and not in the DHCPOffer frames.

QUESTION 33
You are the administrator of a Windows 2000 Domain. You want to deploy a new application named Finance that will be used by all users in the domain. The vendors of the finance application supplied a Microsoft Windows installer package for the application.

You decide to deploy the Finance application in two phases. During phase 1, only members of a security group named Finance Pilot will use the Finance application. During phase 2, all users in the domain will be able to install the finance application.

You want to accomplish the following goals:

- During phase 1, the Finance application will not be installed automatically when users logon.
- During phase 1, users who are members of Finance Pilot group will be able to install the finance application by using a Start menu short cut.
- During phase 1, users who are not members of the Finance Pilot group will not be able to install the Finance application by using a start menu short cut.
- The Finance application will be installed automatically the first time any user in the domain logs on after phase 2 has begun.

You take the following actions:

- Create a new Group Policy Object (GPO) named Finance App and link the Finance App GPO to the domain.
- Configure the Finance App GPO to publish the Finance application to users.
- For phase 1, configure the Finance App GPO permissions. Remove the apply group policy permission for the Authenticated users group. Grant the apply group policy permission for the Finance Pilot group.
- For phase 2, configure the Finance App GPO permissions. Grant the apply group policy permissions for the Authenticated users group. Remove the apply group policy permissions for the Finance Pilot group.

Which result or results do these actions produce? (Choose all that apply)

A. During phase 1, the Finance application will not be installed automatically when users logon.
B. During phase 1, users who are members of Finance Pilot group can install the Finance application by using a **Start** menu short cut.
C. During phase 1, users who are not members of the Finance Pilot group cannot install the Finance application by using a **Start** menu short cut.
D. The Finance application will be installed automatically the first time any user in the domain logs on after phase 2 has begun.

Answer: AC
Section: (none)

Explanation/Reference:
Explanation:
A: Only applications assigned to computers (here it is published to users) will be installed automatically the next time the computer restarts.
C: The computer is only published to the Finance Pilot group during phase 1 (not assigned to authenticated

users) so no one can install the application using a start menu short-cut.

Note: In Windows 2000 we can manage the installation of software on a client computer centrally by assigning applications to users or computers or by publishing applications for users. When we assign an application to a user, the application is advertised to the user the next time the user logs on to the network regardless of which computer the user actually uses to log on. The application is installed the first time the user activates the application on the computer, either by selecting the short cut to application on the start menu or by activating a document associated with the application. When we assign an application to a computer, the application is advertised and is installed when there are no other applications running on the computer. This usually occurs when the computer next starts up. When we publish an application to a user, the application does not appear installed on the users' computers and no shortcut to it is visible on the desktop or the start menu. Instead, the application is available for the user to install using Add/Remove Programs in Control Panel or by clicking a file associated with the application. We cannot publish an application to a computer. In this scenario the application was published via a GPO that was assigned to the finance group users therefore it will not install when users log in.

Incorrect Answers:
B: When we assign an application to a user, the application is advertised to the user the next time the user logs on to the network regardless of which computer the user actually uses to log on. The application is installed the first time the user activates the application on the computer, either by selecting the short cut to application on the start menu or by activating a document associated with the application.
D: When we assign an application to a computer, the application is advertised and is installed when there are no other applications running on the computer. This usually occurs when the computer next starts up.

QUESTION 34
You are the administrator of a Windows 2000 network. You create global groups and domain local groups for the accounts payable and accounts receivable departments.

The domain local group named AP has Change permission for the Accounts Payable folder. The Accounts Payable folder is a subfolder of the Accounting folder. The Accounts Payable global group is a member of the AP Domain Local group. Fred's user account is a member of the Accounts Payable global group.

Fred moves from the Accounts payable department. Fred now needs to access only accounts receivable information. You remove Fred's user account from the Accounts Payable global group, but Fred is still able to access documents in the Accounts Payable folder.

What are two possible causes of this problem? (Choose Two)

A. Fred's user account has explicit permissions on the Accounts Payable folder.
B. Fred's user account belongs to another group that gives him permission on the Accounts Payable folder.
C. The Accounting folder is not published in Active Directory.
D. The Accounts Payable folder is on a FAT32 partition
E. The AP Domain Local group is not a member of the Accounts Payable global group

Answer: AB
Section: (none)

Explanation/Reference:
Explanation:
A. Fred would still be able to access documents in the Accounts Payable folder if his user account has explicit permissions to access the folder.
B. Or if he belongs to another group that has explicit permissions to access the folder.

Incorrect Answers:
C: Whether the Accounting folder is published in Active Directory or not does not affect Fred's access to it, as

permissions to access a folder are granted to user accounts and user groups and are set on the folder and not in Active Directory.
D: To assign permissions to files and folders, the files and folders must be located on an NTFS partition. We cannot apply permissions to files and folders that are located on FAT32 partitions.
E: Whether the AP Domain Local group is a member of the Accounts Payable global group or not would not affect Fred's ability to access the Accounting folder.

QUESTION 35
You are the administrator of a Windows 2000 network named contoso.com. Your network is configured as shown in the Exhibit.

Your company plans to open a new office in Dallas. Members of your IT staff will be on-site in Dallas next week to install the new 10.1.3.0/24 network. You want to prepare the network in advance so that when the IT staff install a new Domain Controller, it will automatically join the appropriate site.

What should you do?

Exhibit:

A. Delete the Default-First-Site-Name object in Active Directory Sites and Services.

B. Create a new subnet for the Dallas network. Create a new site and associate the new subnet with the new site.
C. In the Domain Controllers OU, create a computer account that has the name of the new Domain Controller.
D. Use RIS to prestage the new Domain Controller.
E. Copy the installation source files to the new Domain Controller. Create an unattended install file with an automated DCPromo bat file.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: By associating a subnet with a new site, any computer configured with an IP address in that subnet will be associated with that site.

Incorrect Answers:
A: Deleting the Default-First-Site-Name object in Active Directory Sites and Services would not automatically result in the computers being associated with a site. We would need to add the subnet to a new site.
C: This will not associate the Domain Controller with a site. We should instead add the subnet that the Domain Controller is installed on to a new site.
D: RIS cannot be used to install a Domain Controller. Furthermore, installing a Domain Controller will not result in the association of the computer with a site. We should instead add the subnet that the Domain Controller is installed on to a new site.
E: DCPromo is a command-line utility that can be used to install Active Directory. There is however, no PCPromo.bat file in Windows 2000.

QUESTION 36
You are the administrator of the Arbor Shoes company network. There is one domain containing three sites named Geneva, Milwaukee and Portland.

Each site has two Domain Controllers from the arbroshoes.com domain. Geneva and Portland each have 1,000 users. Milwaukee has 500 users. There are two IP site links: Geneva_Portland and Milwaukee_Portland. You want to add another Domain Controller in each site to handle all replication from each site.

What should you do?

A. Configure each new Domain Controller to be the IP preferred bridgehead Server for its site.
B. Create a connection object from each Domain Controller in each site to the new Domain Controller in each site.
C. Create a new site link that has a lower cost than the existing site links.
D. Delete the existing connection objects in each site and manually start the Knowledge Consistency Checker (KCC).

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Site links direct information arbitrarily to any Domain Controller in a site. Establishing a bridgehead server provides some ranking or criteria for choosing which Domain Controller should be preferred as the recipient for inter-site replication. This bridgehead server then subsequently distributes the directory information via intra-site replication. Therefore, when a preferred bridgehead server has been defined at a site, all site replication from and to this site will pass through the preferred bridgehead server.

Incorrect Answers:
B: We want replication occur between one server at each site.

C: Creating a new site link that has a lower cost than the existing site links will not cause replication to use the new site link. We should define a preferred bridgehead instead.
D: Deleting the existing connection objects in each site and manually starting the Knowledge Consistency Checker (KCC) will not cause replication to use the new site link. We should define a preferred bridgehead instead.

QUESTION 37
You are the administrator of a Windows 2000 network. Your Windows 2000 Domain Controller has been in operation for one year. During that year, you have deleted numerous objects. However, the Ntds.dit file is the same size it was before you deleted any objects.

You want to reduce the size of the Ntds.dit file. What should you do? (Choose two)

A. Delete all the log files from the NTDS folder and restart the server.
B. Use the Ntdsutil utility to perform an authoritative restore.
C. Run the Esentutl utility by using the **/d** switch.
D. Restart the server in directory services restore mode.
E. Use the Ntdsutil utility to compress the database to another drive.

Answer: DE
Section: (none)

Explanation/Reference:
Explanation: The Ntdsutil command-line utility in Directory Services Restore mode can be used to compress the Active Directory database. We can enter Directory Services Restore mode by pressing F8 to display the Windows 2000 Advanced options menu. We must the logon using the Administrators account and type NTDSUTIL at the command prompt, specify files, then type 'COMPACT TO C:\TEMP'. We must then move the compressed NTDS.DIT file from the C:\temp folder to the location of the original NTDS.DIT file and allow the new file to overwrite the existing file. The existing NTDS.DIT file is usually located in the C:\WINNT \system32 folder.

Reference: Appendix C - Active Directory Diagnostic Tool (Ntdsutil.exe)

Incorrect Answers:

A: The log files are not part of the Active Directory database therefore deleting the log files from the NTDS folder will not compress the Active Directory database.
B: Using the Ntdsutil utility to perform an authoritative restore would result in the restoration of the deleted objects.
C: We cannot run the Esentutl independently. We must use the Ntdsutil command-line utility to run the Esentutl utility.

QUESTION 38
You are the administrator of a Windows 2000 domain. All the domain resources are defined in two toplevel OUs. The OUs are named West and East. William is the administrator of the resources in only the West OU. Evert is the administrator of resources only in the East OU.

You move Printer1 from the West OU to the East OU. After you move the printer, Evert can administer it. However, William reports that he can still remove print jobs from Printer1. You want Evert to be the only one that can administer Printer1.

What should you do?

A. Use the delegation of control wizard on the East OU to assign printer1 permission to Evert.

B. Configure the security properties for Printer1 to disallow inheritable permissions to propagate to Printer1.
C. Remove the permissions for William from Printer1.
D. Configure the printer permissions on the West OU to apply to only the West OU.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: When objects are moved between OUs, they retain the permissions associated with them. We must remove the permissions associated with objects manually.

Incorrect Answers:
A: Evert can administer Printer1 therefore Evert does have the required permissions to administer the printer. It is thus not necessary to assign printer1 permission to Evert. We must however, prevent William from administering Printer1.
B: The permission must have been explicitly set so that they are not inherited.
D: We cannot set printer permissions on OUs.

QUESTION 39
You are the administrator of a Windows 2000 network. The network's domain structure is shown in the exhibit.

The us.litware.com and the eur.litware.com domains are in mixed mode. The litware.com and the treyresearch.com domains are in native mode. The us.litware.com domain has two Windows NT 4.0 BDCs that supply legacy applications.

When users from the us.litware.com domain attempt to access a shared folder in the litware.com domain, they receive an error message stating that access is denied. There is a universal group that has Read permission to the Sales folder. Sales is assigned Read permission for the shared folder. When you logon as a member of the Sales group from the litware.com domain, you are able to access the shared folder.

What should you do to correct this problem?

Exhibit:

A. Switch the us.litware.com domain to native mode.
B. Add a Global Catalog Server to the us.litware.com domain.
C. Create a global group in the us.litware.com domain.
Add the user accounts that need access to the shared folder to the global group.
Add the global group to the universal group.
D. Create a universal group in the us.litware.com domain.
Add the user accounts that need access to the shared folder to the universal group.
Grant Read permissions to the universal group for the shared folder in the litware.com domain.
E. Create a global group in the us.litware.com domain.
Add the user accounts from the us.litware.com domain to the global group.
Grant Read permissions to the global group for the shared folder.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: In this scenario, some users in the mixed-mode domain us.litware.com want to have read access to a folder in the native mode domain litware.com. We can accomplish this by creating a new Global Group, to which all appropriate users in the us.litware.com domain are added, in the us.litware.com domain and add this Global group to the universal group in the litware.com domain that has read access to the folder. Even though the mixed-mode domain does not allow universal groups, a global group from a mixed-mode domain can be added to a universal group in another domain.

Incorrect Answers:
A: We cannot switch the us.litware.com domain to native mode because we have Windows NT 4.0 BDCs in the domain. When a domain has both Windows NT 4.0 and Windows 2000 servers, it must run in mixed mode.
B: The us.litware.com domain already contains a Global Catalog server. Therefore we need not add another Global Catalog server to the domain, as a domain does not require more than one Global Catalog server.
D: A mixed mode domain does not allow us to create a universal group.
E: Global groups are restricted to permissions and rights to resources within the domain. We cannot assign permissions to resources in other domains to global groups. In other words, a global group in the us.litware.com domain cannot be assigned read permissions on a shared folder in the litware.com domain.

QUESTION 40
You are the network administrator for Arbor Shoes. The network's domain structure is shown in the exhibit.

The development team is working on a project that involves Arbor Shoes and Contoso, Ltd., a European subsidiary of Arbor Shoes. The development team is located in North America. All the user accounts for the team are in the na.arborshoes.com domain. Most of the resources the development team accesses are in na.arborshoes.com.

Members of the development team report that it is taking longer than normal to access resources in eur.contoso.com. Network utilization is at 5 percent. You want to improve network performance.

What should you do?

Exhibit:

A. Move the development team user accounts from na.arborshoes.com to eur.contoso.com.
B. Create a shortcut trust between na.arborshoes.com and eur.contoso.com.
C. Install a Domain Controller for eur.contoso.com in the same site as na.arborshoes.com.
D. Create a new domain under eur.contoso.com named dev.eur.contoso.com.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: We can explicitly create shortcut trusts between Windows 2000 domains in the same forest. A shortcut trust is a performance optimization that shortens the trust path for Windows 2000 security to take for authentication purposes. The most effective use of shortcut trusts is between two domain trees in a forest. Thus, by creating a shortcut trust between the two domains, authentication would travel along the shortcut trust as opposed to travelling up and down the domain trees.

Incorrect Answers:
A: Moving the development team user accounts from na.arborshoes.com to eur.contoso.com would increase network activity as the development team work in na.arborshoes.com.
C: Installing a Domain Controller for eur.contoso.com in the same site as na.arborshoes.com would cause excessive replication traffic.
D: A new Domain Controller will not reduce network traffic regardless of its name.

QUESTION 41
You are the administrator of your company's network. The network consists of one Windows 2000 domain that spans multiple subnets. You are configuring DNS for hostname resolution throughout the network.

You want to accomplish the following goals:

- DNS zone transfer traffic will be minimized on the network.
- Administrative overhead for maintaining DNS zone files will be minimized.
- Unauthorized host computers will not have records created in the zone.

- All zone updates will come only from authorized DNS servers.
- All zone transfer information will be secured as it crosses the network.

You take the following actions:

- Create an Active Directory integrated zone.
- In the Zone Properties dialog box, set the Allow Dynamic Updates option to Only Secure Updates.
- On the Name Servers tab of the Zone Properties dialog box, enter the names and addresses of all DNS servers on the network.
- On the Zone Transfers tab of the Zone Properties dialog box, select the Allow zone transfers only to the servers listed on the Name Servers tab option

Which result or results do these actions produce? (Choose all that apply)

A. DNS zone transfer traffic is minimized on the network.
B. Administrative overhead for maintaining DNS zone files is minimized.
C. Unauthorized host computers do not have records created in the zone.
D. All zone updates come only from authorized DNS servers
E. All zone transfer information is secured as it crosses the network.

Answer: ABCDE
Section: (none)

Explanation/Reference:
Explanation:
A: Active Directory integrated zones use IXFR, which are incremental transfers. This means that only the records that have changed since the last replication are replicated. This makes the replication of Active Directory integrated zones more efficient because the whole zone file is replicated during standard primary zone replication.
B: Dynamic updates is the process of a client computer updating it is own record in the DNS zone file. This will prevent the need to manually enter records in the DNS zone.
C: The “Only Secure Updates" must be selected to be sure of no unauthorized DNS records in the zone. Secure updates specify that only users, groups or computers that have been granted the right to write to the zone or record have the ability to update the record.
D: Selecting the Allow Zone transfers only to the servers listed on the Name servers tab option prevents unauthorized servers from updating the zone. Dynamic updates have been enabled.
E: Active Directory DNS zones replicate their data as part of Active Directory replication. Active Directory replication uses a secure RPC channel to replicate data.

Incorrect Answers:
All alternatives are correct.

QUESTION 42
You are the administrator of a Windows 2000 domain. Your current Domain Controller's hard disk drive is failing. You install a new server as a Domain Controller to replace the failing Domain Controller.

You ran DCPromo.exe on the failing Domain Controller in your domain to remove Active Directory. While you are running DCPromo.exe, the hard disk drive fails. The server will not reboot. However, the objects for the failed server are still appearing in Active Directory. You are using the Ntdsutil utility to remove the objects.

You want to remove the old server from Active Directory. What option should you use?

A. metadata cleanup.
B. semantic database analysis.

C. security account management.
D. domain management.
E. authoritative restore.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Ntdsutil is a command-line tool that provides directory service management. It maintains the Active Directory store, manages and controls Flexible Single Master Operations masters, and purges metadata left behind by abandoned Domain Controllers (which are removed from the network without being uninstalled).

Incorrect Answers:
B: Semantic database analysis is used to for diagnostic purposes, not to remove objects in Active Directory.
C: Security account management is the process of managing user and group accounts. It is not used to manage Active Directory or to remove objects in Active Directory.
D: Domain management forms part of the job functions of a network administrator. It is not an operating system tool that can be used to remove objects in Active Directory.
E: An authoritative restore refers to the restoration of Active Directory. It is used when the restored version of Active Directory must be replicated to other servers despite its datestamp which would indicate that the restored version of Active Directory is older than the current version of Active Directory that is in use on the

QUESTION 43
You are the administrator of a Windows 2000 network. Recently, your network security was compromised and confidential data was lost. You are now implementing a stricter network security policy. You want to require encrypted TCP/IP communication on your network.

What should you do?

A. Create a GPO for the domain, and configure it to assign the Secure Server IPSec Policy.
B. Create a GPO for the domain, and configure it to assign the Server IPSec Policy and to enable **Secure channel: Require strong session key**.
C. Implement TCP/IP packet filtering, and open only the ports required for your network services.
D. Edit the local security policies on the servers and client computers, and enable **Digitally sign client and server communications.**

Answer: A
Section: (none)

Explanation/Reference:
Explanation: IPSec is an industry standard for encrypting TCP/IP traffic. By assigning the Secure Server IPSec Policy we can ensure that the computers on the network will only accept encrypted TCP/IP traffic.

Incorrect Answers:
B: Windows 2000 does not support a Server IPSec Policy. It only supports a Secure Server IPSec Policy.
C: Implementing TCP/IP packet filtering and opening only the required ports would not encrypt the network traffic. In this scenario encryption is a requirement.
D: Editing the local security policies on the servers and client computers, and enabling **Digitally sign client and server communications** is a huge administrative task. It is therefore not a recommended solution.

QUESTION 44
You are the administrator of your company's network. The network consists of one Windows NT 4 domain. You create and implement a security policy that is applied to all Windows 2000 Professional computers as they are

staged and added to the network.

You want this security policy to be in effect at all times on all client computers on the network. However, you find out that administrators periodically change security settings on computers when they are troubleshooting or doing maintenance.

You want to automate the security analysis and configuration of client computers on the network so that you can track changes to the security policy and reapply the original security policy when it is changed.

What should you do?

A. Use Windows NT System Policy to globally configure the security policy settings on the client computers.
B. Use Windows 2000 Group Policy to globally configure the security policy settings on the client computers.
C. Use the Security and Configuration Analysis tool on the client computers to analyze and configure the security policy.
D. Schedule the **Secedit** command to run on the client computer to analyze and configure the security policy.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: Secedit is a command line utility that is used to configure the security policy. We could write a batch file containing the commands and schedule the batch file.

Incorrect Answers:
A: System policies do not apply to Windows 2000 computers.
B: Configuring the security policy settings on the client computers will not prevent Administrators from making changes to the security policy and will not enable us to track security policy changes.
C: In this scenario we want to automate the process of analyzing and configuring the security policy on client computers. The solution provided by this option does to automate the process.

QUESTION 45
You are the administrator for a Windows 2000 network. Your network consists of one domain and two Organizational Units (OUs). The OUs are named Corporate and Accounting.

A user recently reported that she was not able to log on to the domain. You investigate and find out that the user's account has been deleted. You have been auditing all objects in Active Directory since the domain was created. But you cannot find a record of the user account deletion. You want to find a record that identifies the person who deleted the account.

What should you do?

A. Search the security event logs on each Domain Controller for account management events.
B. Search the security event logs on each Domain Controller for object access events.
C. Search the Active Directory Users and Computers console on each Domain Controller for the user's previous account name.
D. Search the Active Directory Users and Computers console on each Domain Controller for the user's computer account.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: As the process of deleting or creating a user account is an account management event, we

should use security event logs on each Domain Controller for account management events.

Incorrect Answers:
B: Object access events log access to network resources such as files and printers. It does not log account management events.
C: Searching the Active Directory Users and Computers console on each Domain Controller for the user's previous account name would not indicate who deleted the user account.
D: Searching the Active Directory Users and Computers console on each Domain Controller for the user's computer account would not indicate who deleted the user account.

QUESTION 46
You are the administrator of a Windows 2000 network for Lucerne Real Estate. The network has 1,200 users. You are delegating part of the administration of the domain to three users.

You delegate the authority to create and delete computer accounts to Carlos. You delegate the authority to change user account information to Julia. You delegate the ability to add client computers to the domain to Peter. You want to track the changes made to the directory by these three users.

What should you do?

A. Create a Group Policy object (GPO) for the Domain Controllers.
   Assign Read and Apply Group Policy permissions to only Carlos, Julia, and Peter.
   Configure the GPO to audit directory services access and account management.
B. Create a Group Policy object (GPO) for the domain.
   Assign Read and Apply Group Policy permissions to only Carlos, Julia, and Peter.
   Configure the GPO to audit directory services access and audit object access.
C. Create a Group Policy object (GPO) for the Domain Controllers.
   Assign Read and Apply Group Policy permissions to only Carlos, Julia, and Peter.
   Configure the GPO to audit directory services access and audit object access.
D. Create a Group Policy object (GPO) for the domain.
   Assign Read and Apply Group Policy permissions to only Carlos, Julia, and Peter.
   Configure the GPO to audit object access and process tracking.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: To track the changes made to the directory by these three users we must audit directory services access for computer accounts and account management for user accounts.

Incorrect Answers:
B: Object access refers to the access to network recourses such as files and printers. Thus, auditing object access we could discover who is accessing which network resources. We must however track changes made to the directory. We should therefore audit account management and directory services access, not directory services access and audit object access.
C: Object access refers to the access to network recourses such as files and printers. Thus, auditing object access we could discover who is accessing which network resources. We must however track changes made to the directory. We should therefore audit directory services access and account management, not directory services access and audit object access.
D: Object access refers to the access to network recourses such as files and printers. Thus, auditing object access we could discover who is accessing which network resources. We must however track changes made to the directory. We should therefore audit account management and directory services access, not object access and process tracking.

QUESTION 47
You are the administrator of your company's network. Your event log shows that hackers are using brute force attacks to attempt to gain access to your network. You do not want user accounts to be easily accessible. You want to strengthen security to protect against brute force attacks.

What should you do? (Choose two.)

A. Enable the **Users must log on to change the password** setting.
B. Enable the **Store password using reversible encryption for all users in the domain** setting.
C. Enable the **Password must meet complexity requirements** setting.
D. Increase minimum password length.
E. Increase minimum password age.

Answer: CD
Section: (none)

Explanation/Reference:
Explanation:
C: By enabling the **Password must meet complexity requirements** setting we would ensure that users would implement complex passwords with a mix of capital letters, lower case letters and numbers. Passwords with a mix of theses characters cannot easily be hacked by brute force attacks.
D: By increasing the minimum password length we would require users to specify longer passwords. This would make it more difficult for a hacker to access the network by using a brute force attack.

Incorrect Answers:
A: By enabling the **Users must log on to change the password** setting we will not increase the complexity requirement of the passwords and thus would not make passwords more secure. We would however require users to change their passwords if the hacker had managed to gain access to our network.
B: The **Store password using reversible encryption for all users in the domain** setting is used for CHAP authentication. It is not used to increase password complexity.
E: Increasing the minimum password age would enable users to keep the same passwords for longer. This is generally not a good practice and is not recommended.

QUESTION 48
You are the administrator of your company's network. The network consists of one Windows 2000 domain that has organizational units (OUs) as shown in the exhibit.

All Domain Controllers in the domain are in OU1. Resources for two separate office buildings are in OU2 and OU3. Nonadministrative users, groups, and computers are in OU4 and OU5. Administrative users, computers, and resources are in OU6.

You are designing a domain-wide security policy.

You want to accomplish the following goals:

- The same password and account lockout policies will be applied to all users.
- Different security settings will be applied to administrative and nonadministrative computers.
- Strict audit policies will be enforced for only Domain Controllers and servers.
- The number of Group Policy object (GPO) links will be minimized.

You take the following actions:

- Create a single GPO.
- Create one security template that has all required settings.
- Import the security template into the GPO.

- Link the GPO to the domain.

Which result or results do these actions produce? (Choose all that apply.)

Exhibit:

A. The same password and account lockout policies are applied to all users.
B. Different security settings are applied to administrative and nonadministrative computers.
C. Strict audit policies are enforced for only Domain Controllers and servers.
D. The number of GPO links is minimized

Answer: AD
Section: (none)

Explanation/Reference:
Explanation: As the GPO was applied to the domain, all users will be affected by it. The minimum number of GPO links is one. We cannot have less than one GPO. As we have only one GPO, the number of GPO links is minimised.

Incorrect Answers:
B: As the GPO was applied to the domain, all users will be affected by it and thus all users will receive the same security settings.
C: As the GPO was applied to the domain, all users will be affected by it and thus all users will receive the same audit policies.

QUESTION 49
You are the Windows 2000 network administrator for your company. You are implementing the company's network security model. You network has several servers that contain sensitive or confidential information. You want to configure security auditing on these servers to monitor access to specific folders. You also want to prevent users from gaining access to these servers when the security logs become full.

What should you do?

A. Create a Group Policy object (GPO) that applies to the servers.
   Configure the GPO to enable auditing for object access.
   Set up the individual objects to be audited in Windows Explorer, and then customize the Event Viewer logs to limit the size of the security log to 1,024 KB.

B. Create a Group Policy object (GPO) that applies to the servers.
Configure the GPO to enable auditing for directory services access.
Set up the individual objects to be audited in Windows Explorer, and then customize the Event Viewer logs to limit the size of the security log to 1,024 KB.
Configure the security event log so that it does not overwrite events.

C. Create a Group Policy object (GPO) that applies to the servers.
Configure the GPO to enable auditing for directory service access.
Set up the individual objects to be audited in Windows Explorer.
Configure the security event log so that it does not overwrite events.
Then configure the GPO to enable the **Shut down the system immediately if unable to log security audits** setting.

D. Create a Group Policy object (GPO) that applies to the servers.
Configure the GPO to enable auditing for object access.
Setup the individual objects to be audited in Windows Explorer.
Configure the security event log so that it does not overwrite events.
Then configure the GPO to enable the **Shut down the system immediately if unable to log security audits** setting.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: The GPO enables auditing of object access on all servers. Configuring the sensitive folders to be audited and configuring the computer to shut down when the logs are full, which would result in auditing being stopped, will ensure that no unaudited access is possible to the sensitive folders.

Incorrect Answers:
A: Setting up the individual objects to be audited in Windows Explorer, and then customizing the Event Viewer logs to limit the size of the security log to 1,024 KB will not prevent access to the sensitive folders should auditing stop due to the event log becoming full.
B: Object access refers to the access to network resources such as files, folders and printers. As we must audit folder access, we are required to audit object access and not directory services access.
C: Object access refers to the access to network resources such as files, folders and printers. As we must audit folder access, we are required to audit object access and not directory services access.

QUESTION 50
You are the administrator of a newly installed Windows 2000 network for a call centre. You need to rename the Administrator account on all computers on your network. You do not want to manually edit each account. Because of a recent security breach, you must implement this policy immediately.

What should you do? (Choose all that apply.)

A. Use Group Policy to rename the Administrator account at the Default Domain Group policy.
B. Use Group Policy to implement a user logon script.
C. Send a network message to all users to restart their computers.
D. Use Group Policy to force all users to log off within 30 minutes.

Answer: AC
Section: (none)

Explanation/Reference:
Explanation: We can automatically rename the Administrator account on all computers on our network by using group policy at the Default Domain Group policy. We would then have to restart all the computers in the network so that the new policy can be applied.

Incorrect Answers:
B: It is not necessary to implement a user logon script as the passwords can be changed by using a GPO.
D: It is not possible to create a Group Policy that forces users to log off within 30 minutes. Furthermore, requiring users to log off within 30 minutes would not ensure that the policy is applied immediately.

QUESTION 51
Your company's network consists of two Windows 2000 domains, contoso.com and sales.contoso.com. You are a member of the Domain Admins group in sales.contoso.com. The sales.contoso.com domain contains an Organizational Unit (OU) named Traveling.

Users in the Traveling OU use portable computers to connect to the network while at home, in hotels, and in the office. You use Internet Explorer maintenance in Group Policy to apply Favourites settings for members of the Traveling OU.

Users in the Traveling OU report problems with their Favourites settings when connecting to the company network. When users connect by means of dial-up connections, Favorites settings are not updated. When users connect by means of broadband connections from home, Favorites settings are not always updated. When users connect from the office, Favorites settings are always updated.

You need to ensure that Favorites settings are always applied when users log on to the network. How can you configure the Traveling OU? (Each correct answer presents a complete solution. Choose two)

A. Enable the **Internet Explorer Maintenance policy processing** policy to allow processing across a slow network connection.
B. Enable the **Enable Active Desktop** policy.
C. Enable the **Group Policy slow link detection** policy to change the definition of a slow connection.
D. Set the **Group Policy refresh interval for computers** policy to 0 minutes.
E. Set the **Group Policy refresh interval for users** policy to 0 minutes.
F. Enable the **Apply Group Policy for computers asynchronously during startup** policy for the computer policies.
G. Enable the **Slow network connection timeout for user profiles** policy.

Answer: AC
Section: (none)

Explanation/Reference:
Explanation: In this scenario we are required to apply a GPO to the portable computers of the users in the travelling OU. This GPO should be applied whenever the users connect to the network. In this scenario the policy is correctly applied when the travelling users connect from the office. However, when they connect over the broadband WAN connection the GPO is not applied at times, and is never applied when they dial into the network.

A: By enabling the Internet Explorer Maintenance policy processing policy, and then to set it to allow processing across a slow network connection, the GPO would be allowed to be transferred over the slow dial-in connection.

C: In addition, by enabling the Group Policy slow link detection policy, and then changing the definition of a slow connection, the Domain Controller could get proper settings so that it can decide that all broadband connections should be considered to be as slow connections. The default setting is 500kbps. This should be lowered.

Incorrect Answers:
B: Active Desktop settings are used to configure the Desktop, not configure slow WAN connections.

D: By setting the **Group Policy refresh interval for computers** policy to 0 minutes, the computer tries to update the Group Policy every 7 seconds. This would require a lot of bandwidth and is not a good solution.

E: By setting the **Group Policy refresh interval for users** policy to 0 minutes, the computer tries to update the Group Policy every 7 seconds. This would require a lot of bandwidth and is not a good solution

F: On Windows 2000 clients, Group Policies are handled synchronously by default. All Group polices have to be applied before the logon process ends. By enabling **Apply Group Policy for computers asynchronously during startup** the users might access the desktop before all the group polices have been applied. This makes the logon process faster. It would not help to solve the problems with the WAN links.

G: Enabling and setting the **Slow network connection timeout for user profiles** policy would result in a failure of the users to logon to the network once the timeout setting has expired. Users would then have to attempt to logon to the domain again.

QUESTION 52
You are a member of the Enterprise Admins group in your company's Windows 2000 network. The network contains two Active Directory sites: Cairo and London. Each site has its own domain that operates in native mode. The network is configured as shown in the exhibit.

Occasionally, the WAN link between Cairo and London stops functioning, and users in London report that they cannot log on to the network. However, users in Cairo report no problems.

You want to ensure that problems with WAN connectivity do not prevent users from logging on to the network. What should you do?

A. Configure the network as a single Active Directory site, and then associate all subnets with that site.
B. Configure DC2 as a Global Catalog server.
C. Configure DC2 as a PDC emulator.
D. Create a new Group Policy Object in the London site to enable slow link detection on client computers.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: On domains that operate in native mode, i.e. domains in which there are only Windows 2000 computers, we require a Global Catalog server to log on. A Global Catalog server enables Active Directory Search queries and must be present to allow clients to successfully logon. They also hold a copy of all objects of the whole forest but hold only a subset of the Attributes.

Reference: Global Catalog Server Requirement for User and Computer Logon (Q216970)

Incorrect Answers:
A: One site would not affect logging on if the WAN link were down.
C: Configuring DC2 as a PDC emulator would only be required for down-level clients. In native mode a PDC emulator handles the password changes. Without a PDC emulator password changes would be impossible, but clients would still be able to log on to the network.
D: Creating a GPO for slow link detection would not solve the problem posed in this scenario as the link is already down.

QUESTION 53
Your company's network consists of a single Windows 2000 domain named contoso.com. You are a member of the Domain Admins group.

Contoso Ltd., wants to create a new division named Fabrikam Inc. The new division will consist of two domains: fabrikam.com and sales.fabrikam.com. You need to create these two new domains. You need to configure all three domains so that they can share resources by using the least amount of administrative effort.

What should you do?

A. In the contoso.com domain tree, create a new child domain named fabrikam.com. Create a new child domain for fabrikam.com named sales.fabrikam.com
B. In the contoso.com domain tree, create a new child domain named sales.fabrikam.com. Create a new parent domain for sales.fabrikam.com named fabrikam.com
C. In the existing forest, create a new domain tree for fabrikam.com. Create a new child domain for fabrikam.com named sales.fabrikam.com
D. In a new forest, create a new domain tree for fabrikam.com. Create a new child domain for fabrikam.com named sales.fabrikam.com

Answer: C
Section: (none)

Explanation/Reference:
Explanation: In this scenario we require a new tree so that the top-level domain can be called fabrikam.com. Then we can create a child domain for sales.fabrikam.com.

Incorrect Answers:
A: In this scenario we require a new tree so that the top-level domain can be called fabrikam.com. We do not require a new child domain. Furthermore, the new child domain name must be appended to the top-level domain. Therefore we cannot create a new child domain named fabrikam.com.
B: In this scenario we require a new tree so that the top-level domain can be called fabrikam.com. We cannot create a parent domain of an existing child domain. We can only create top-level domains.
D: In this scenario we require a new tree so that the top-level domain can be called fabrikam.com. This new tree must be created in the same forest and not in a new forest.

QUESTION 54
Your company's network consists of a single Windows 2000 domain named sports.contoso.com. You and another employee named Maria are members of the Domain Admins group.

Maria creates a domain local security group named Teams. You create three global distribution groups: Bowling, Tennis, and Volleyball. You add these three groups to the Teams group. You create a shared folder named Schedule and grant the Teams group the Change permission for the Schedule shared folder.

Users in the Bowling, Tennis, and Volleyball groups report they cannot access the Schedule shared folder. You need to enable users to access the shared folder.

What should you do?

A. Grant the Bowling, Tennis, and Volleyball groups the Change permission for the Schedule shared folder.
B. Grant the Bowling, Tennis, and Volleyball groups the Full Control permission for the Schedule shared folder.
C. Convert the Teams group to a global distribution group.
D. Convert the Teams group to a universal distribution group.
E. Convert the bowling, tennis, and volleyball groups to global security groups.

Answer: E
Section: (none)

Explanation/Reference:
Explanation: Windows 2000 uses only security groups to assign permissions to gain access to resources. Applications use distribution groups as lists for nonsecurity-related functions. We can use distribution groups when the only function of the group is nonsecurity-related, such as sending e-mail messages to a group of users at the same time. We cannot use distribution groups to assign permissions. The groups need to be security groups to inherit the permissions from the domain local group.

Incorrect Answers:
A: We can use distribution groups when the only function of the group is nonsecurity-related, such as sending e-mail messages to a group of users at the same time. We cannot use distribution groups to assign permissions.
B: We can use distribution groups when the only function of the group is nonsecurity-related, such as sending e-mail messages to a group of users at the same time. We cannot use distribution groups to assign permissions.
C: We can use distribution groups when the only function of the group is nonsecurity-related, such as sending e-mail messages to a group of users at the same time. We cannot use distribution groups to assign permissions.
D: We can use distribution groups when the only function of the group is nonsecurity-related, such as sending e-mail messages to a group of users at the same time. We cannot use distribution groups to assign permissions.

QUESTION 55
You are the enterprise administrator of a Windows 2000 network. The network has three domains named contoso.com, west.contoso.com, and east.contoso.com. All three domains are in a site named Boston. All three domains contain OUs.

You want to implement new desktop policies for all users on the network. The policies are configured in a Group Policy Object named GPdesktop.

You also want to implement a logon script for users from the W2 OU. The logon script policy is configured in a GPO named GPscript. The users from the W2 OU always log on to Windows 2000 Professional computers defined in the W3 OU. You do not want to use Group Policy filtering.

What should you do?

To answer Click the Select and Place button, and then drag the GPdesktop and GPscript GPOs to the correct locations.

Boston Site
C1
Contoso.com
West.contoso.com
W1
East.con
E1
W2
W3
E2
E3

Answer:

Section: (none)

Explanation/Reference:
Explanation: In this scenario we have a large site, which includes three domains. Therefore two different Group Policy Objects must be applied to this site.

The GPdesktop Group Policy
The GPdesktop group policy must be implemented for all users on the network. By applying it to the site level it would be applied to the domain hierarchy including all OUs. This is the best solution with least administrative effort.

The GPO could also be applied to all domains of the site. This would require more administrative effort and it is not the best solution.

The GPscript Group Policy
The **GPscript** group policy, which includes logon scripts, should be applied to users of the OU named W2. All users of the W2 OU always use computers in the W3 OU. It seems that there is a choice between the OU W2 and the OU W3.

By linking the GPscript to the W2 OU only users in the W2 OU would be affected.
By linking the GPscript to the W3 OU all users using computers in W3 OU would be affected.
Applying the GPscript to the W2 OU is more restrictive and is therefore the preferred solution.

QUESTION 56
You are the administrator of a Windows 2000 domain. The domain has an OU named Help Desk. All users in the help desk OU use an application named PhoneID.

The PhoneID application is deployed by using a Group Policy Object named Phone App on the Help Desk OU. The Phone App GPO is configured to publish the PhoneID application to users by using a Microsoft Windows installer package for the application.

Currently, only the users in the Help Desk OU can start the PhoneID application. You want all users in the domain to be able to install the PhoneID application by using the Start menu shortcut.

What should you do?

A. Remove the Phone App GPO link to the Help Desk OU. Assign the Phone App GPO to the domain. Change the configuration of the Phone App GPO to assign the PhoneID application to users.
B. Create a new GPO named Phone For All. Assign the Phone App GPO to the domain. Configure the Phone For All GPO to assign the PhoneID application to computers.
C. Configure the Phone App GPO to assign the PhoneID application to users. Configure the permissions on the Phone App GPO to assign Apply Group Policy permission to the Authenticated Users group.
D. Configure the Phone App GPO to assign the PhoneID application to computers. Configure the PhoneID Windows Installer package to upgrade the installed PhoneID application. Set the Windows Installer policy to disable rollback.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: In this scenario the GPO must be linked to the domain so that it affects all users and the application must be assigned to users so that it appears as a shortcut in the users start menus.

Note: In Windows 2000 we can manage the installation of software on a client computer centrally by assigning applications to users or computers or by publishing applications for users. When we assign an application to a user, the application is advertised to the user the next time the user logs on to the network regardless of which computer the user actually uses to log on. The application is installed the first time the user activates the application on the computer, either by selecting the short cut to application on the start menu or by activating a document associated with the application. When we assign an application to a computer, the application is advertised and is installed when there are no other applications running on the computer. This usually occurs when the computer next starts up. When we publish an application to a user, the application does not appear installed on the users' computers and no shortcut to it is visible on the desktop or the start menu. Instead, the

application is available for the user to install using Add/Remove Programs in Control Panel or by clicking a file associated with the application. We cannot publish an application to a computer.

Incorrect Answers:
B: If we assign the application to computers it will be automatically installed the next time the computer is restarted, but we only want users to be able to install it when they use a shortcut in the Start menu.
C: We must link the policy to the domain to ensure that it affects all users. The application must be assigned, not published to users.
D: The application should be assigned to users to not computers.

QUESTION 57
You are the administrator of your company's Windows 2000 network. The network contains four Windows 2000 Domain Controllers. Each Domain Controller contains one hard disk that is configured as drive C.

You install an application that uses Active Directory frequently. After the installation, a Domain Controller begins to respond slowly to network logon requests. You discover excessive hard disk activity on the Domain Controller.

You want to maximize Active Directory performance. What should you do?

A. Add two new hard disks to the Domain Controller. Mirror the new hard disks and configure the volume as drive D. Move the Sysvol shared folder to drive D. Enable the indexing service on both hard disks.
B. Add two new hard disks to the Domain Controller. Format each new hard disk separately and configure one volume as drive D and the other volume as drive E. Move the Ntds.dit file to drive D and the log files to drive E
C. Add one new hard disk to the Domain Controller. Format the new hard disk and configure the volume as drive D. Move the Netlogon shared folder to drive D. Enable the indexing service on both hard disks.
D. Add one new hard disk to the Domain Controller. Format the new hard disk and configure the volume as drive D. move the Sysvol and Netlogon shared folders to drive D.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: With Windows 2000 it is possible to place the ntds.dit file, which is the Active Directory database, and the log files on separate drives. This will improve system performance.

Incorrect Answers:

A: Mirrored disks will not improve performance, as the changes to the system must be written to both hard drives. This will in fact reduce system performance. Mirrored disks are thus not used to improve system performance. They are however used for fault tolerance.
C: Moving netlogon will not improve performance as it is neither a log file nor is it the Active Directory database.
D: Moving netlogon and sysvol will not improve performance as they are neither a log file nor are they the Active Directory database.

QUESTION 58
You are a member of the Enterprise Admins group in your company's Windows 2000 network. The network consists of two Active Directory sites: Chicago and Dallas. Site Link A connects the Chicago and Dallas sites. Site link A has a replication schedule of 4:00 am to 8:00 am.

Your company opens a new office in Miami. You create a new Active Directory site named Miami. You also create a new site link named site link B. Site link B connects the Chicago and Miami sites. Site link B has a

replication frequency of 90 minutes and a replication schedule of 2:00am to 6:00 am.

Users in Dallas and Miami report that changes in Active Directory sometimes take two days to replicate across the network. You want to ensure that all directory changes replicate in one day.

Which two actions can you take? (Each correct answer presents a complete solution. Choose two)

A. Change the replication frequency of site link A to 60 minutes.
B. Change the replication frequency of site link B to 15 minutes.
C. Change the replication schedule of site link A to 4:00 am to 9:30 am.
D. Change the replication schedule of site link B to 1:30 am to 6:00 am.
E. Change the replication schedule of site link B to 2:00 am to 7:30 am.

Answer: AE
Section: (none)

Explanation/Reference:
Explanation: In this scenario there are three sites connected by two site links. We are required to change the configuration of the network so that all directory changes replicate within one day. Currently site link A has a replication schedule of 4:00 am to 8:00 am. We assume the default replication frequency of 180 minutes. While site link B has a replication frequency of 90 minutes and a replication schedule of 2:00am to 6:00 am. The overlapping time is between 2:00 am and 4:00 am. We must increase the replication frequency on site link A to 60 minutes. As site link B has a replication frequency of 90 minutes and would only have time to replicate once during the overlapping time we must increase the replication schedule of site link B to 2:00 am to 7:30 am to achieve an overlapping time of 3.5 hours. Two replications can be made on both site link A and site link B during this period, and the goal of ensuring that all directory changes replicate within one day is met.

Incorrect Answers:

B: Decreasing the replication frequency of site link B to 15 minutes could help, but it would cause a lot of replication traffic on the network. This is therefore not the best solution.
C: Changing the replication schedule of site link A to 4:00 am to 9:30 am would not increase the overlapping time between 2:00 am and 4:00 am.
D: Changing the replication schedule of site link B to 1:30 am to 6:00 am would not increase the overlapping time between 2:00 am and 4:00 am.

QUESTION 59
You are the administrator of your company's network. The network consists of one Windows 2000 domain. The domain consists of a single top-level OU named Main and five child OUs. The child OUs are named after the company's five departments: Finance, Marketing, Sales, HR, and IT.

The accounts for all users and computers in each department are defined in the OU for that department. All users and computers in the Finance, Marketing, Sales and HR OUs require the same desktop settings. Users and computers in the IT OU require less restrictive settings.

You want to accomplish the following goals:

- All the assigned Group Policy settings as defined by the administrator in the Main OU will be applied to all users and computers in the Finance, Marketing, Sales, and HR OUs.
- Group Policy from the Main OU will not be applied to the IT OU.
- Administrators in the IT OU will be able to change the Group Policy settings.
- When new child OUs under the Main OU are added to the domain, the Group Policy will be applied to them automatically.
- Users will not be able to change their Group Policy settings.

You take the following actions:

- Create the GPO, configure the appropriate settings, and link the GPO to the Main OU.
- In the Group Policy Options dialog box for the Main OU, select the No Override check box.
- In the Group Policy dialog box for the IT OU, select the Block Policy inheritance check box.
- Grant the Authenticated Users group Full Control permission to the GPO.

Which result or results do these actions produce? (Choose all that apply)

A. All the assigned Group Policy settings as defined by the administrator in the Main OU are applied to all users and computers in the Finance, Marketing, Sales, and HR OUs.
B. Group Policy from the Main OU is not applied to the IT OU.
C. Administrators in the IT OU can change the Group Policy settings.
D. When new child OUs under the Main OU are added to the domain, the Group Policy is applied to them automatically.
E. Users cannot change their Group Policy settings.

Answer: ACD
Section: (none)

Explanation/Reference:
Explanation:
A: We have created a GPO, configured the appropriate settings, and linked the GPO to the Main OU, which consists of the Finance OU, the Marketing OU, the Sales OU, the HR OU, and the IT OU. Therefore the GPO has been applied to all users.
C: Users have been assigned Full Control permission of the GPO, and are therefore able to change its settings. This includes the administrators in the IT department. Therefore, the IT administrators can change the Group Policy settings.
D: By default, child OUs inherit the GPO settings assigned to the top-level OU unless the **Block Policy inheritance** check box is selected in the **Group Policy dialog** box for the child OU.

Incorrect Answers:
B: The GPO is applied to all OUs. The **No Override Group Policy** setting at the Main OU overrides the **Block Policy Inheritance** setting of the IT OU.
E: Users have been assigned Full Control permission of the GPO, and are therefore able to change its settings.

QUESTION 60
You are the administrator of your company's Windows 2000 network. The network consists of a single DNS domain named contoso.com. The domain contains a UNIX server named UnixServer1 and a Windows 2000 Server computer named WinServer1. UnixServer1 is running BIND DNS and holds the SOA (Start of authority) record for the DNS domain. You want to configure WinServer1 as a DNS server for the domain, but UnixServer1 must retain the SOA record for the domain.

You install DNS on WinServer1 and configure the server to contain a primary zone for contoso.com. After the installation, you discover that DNS record changes on UnixServer1 are not being replicated to this new primary zone.

You need to enable DNS replication between Unixserver1 and WinServer1. What should you do?

A. On WinServer1, add UnixServer1 to the list of servers that are permitted to perform zone transfers.
B. Add WinServer1 to the DNSUpdateProxy group, and then restart the DNS server service.
C. Delete the DNS domain from WinServer1, and then create a new secondary zone that is linked to UnixServer1.

D. On WinServer1, convert the primary zone to an Active Directory integrated zone.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: In this scenario we must delete the DNS domain from WinServer1, and then create a new secondary zone that is linked to UnixServer1 as only a secondary zone can receive zone transfers from a primary zone.

Incorrect Answers:
A: A primary zone will not replicate to another primary zone; only a secondary zone can receive zone transfers from a primary zone.
B: The DNSUpdateProxy group is not related to zone transfers. Thus this solution is not appropriate to the problem.
D: Active Directory integrated zones can only receive zone transfers from other Active Directory integrated zones.

QUESTION 61
You are the administrator of your company's Windows 2000 network. The network consists of a single domain named litware.com. All client computers are running Windows 2000 Professional and are members of the domain. All users are members of the Power Users group on their computers. A portion of the network is configured as shown in the exhibit.

A client computer named Client4 has dial-up access to the internet. You do not want other users to share the Internet connection that is configured for Client4.

What should you do?

Exhibit:

A. Create a Group Policy Object (GPO) that disables the configuration of connection sharing. Grant Client1, Client2, and Client3 the Read permission and the apply Group Policy permission for the GPO.
B. Create a Group Policy Object (GPO) that disables the configuration of connection sharing. Grant Client4 the Read permission and the apply Group Policy permission for the GPO.
C. Create a Group Policy Object that creates a high-security zone for Microsoft Internet Explorer.
D. Create a Group Policy Object that deletes existing connection settings for Microsoft Internet Explorer.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: In this scenario we want the GPO to apply to client 4 so that the internet connection on client4 cannot be shared. Therefore we must create a Group Policy Object (GPO) that disables the configuration of connection sharing and grant Client4 the Read permission and the Apply Group Policy permission for the GPO. This will allow the GPO to be applied to Client4.

Incorrect Answers:
A: In this scenario we want the GPO to apply to client 4 so that the internet connection on client4 cannot be shared. Therefore we should assign the Read permission and the apply Group Policy permission for the GPO

to Client4 and not to Client1, Client2, and Client3.
C: Microsoft Internet Explorer cannot be used for setting up and configuring connection sharing. This solution is thus not appropriate to the problem.
D: We do not want to delete the existing connections because this would result in Client4 having no connection to the Internet.

QUESTION 62
Your company's network consists of two domains: contoso.com and sales.contoso.com. The contoso.com domain contains one Domain Controller and one member server. You are a member of the Domain Admins group in sales.contoso.com

The sales.contoso.com domain contains two Windows 2000 Domain Controllers, one Windows NT BDC, 50 Windows NT Workstation computers and 50 Windows 2000 Professional computers.

A Windows 2000 Domain Controller in sales.contoso.com fails and cannot be recovered from backup tape. Users who are running Windows NT Workstation report that they cannot change their passwords.

You want to enable all users to change their passwords. What should you do?

To Answer click the select and place button, and then drag the appropriate object to the appropriate destination.

Action	Role	
Transfer	The infrastructure master	By using A
Seize	The RID master	By using
Query	The PDC emulator	By using A
	The domain naming master	By using
	The schema master	

Answer:

Action	Role	
Seize	The PDC emulator	
Transfer	The infrastructure master	By using A
	The RID master	By using
		By using A
Query	The domain naming master	By using
	The schema master	

Section: (none)

Explanation/Reference:
Explanation: If the domain contains computers operating without Windows 2000 client software or if it contains Windows NT backup Domain Controllers (BDCs), the PDC emulator acts as a Windows NT primary Domain Controller. It processes password changes from clients and replicates updates to the BDCs.

When the PDC emulator is not available, we may need to immediately seize the role. We must therefore seize the PDC emulator. We cannot transfer it because the original PDC emulator is offline. Furthermore we must use the Ntdsutil utility, not the Active Directory Sites and Services to seize the PDC emulator role.

Note:
To seize the PDC emulator role

1. Click **Start**, click **Run**, and then type **cmd**.
2. At the command prompt, type **ntdsutil**.
3. At the **ntdsutil** prompt, type **roles**.
4. At the **fsmo maintenance** prompt, type **connections**.
5. At the **server connections** prompt, type **connect to server**, followed by the fully qualified domain name.
6. At the **server connections** prompt, type **quit**.
7. At the **fsmo maintenance** prompt, type **seize PDC**.
8. At the **fsmo maintenance** prompt, type **quit**.
9. At the **ntdsutil** prompt, type **quit**.

Reference:

Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller (Q255504)
Windows 2000 Server Resource kit, Active Directory Diagnostic Tool (Ntdsutil.exe), Managing Operations Master Roles
Microsoft Windows 2000 Server documentation

QUESTION 63
You are the administrator of your company's Windows 2000 network. The network consists of a single Windows 2000 domain, which operates in native mode. The domain contains four Domain Controllers. Many users report that their accounts receive the following error message: “Your account has been disabled. Please see your system administrator”.

You want to discover how the accounts are being locked out. You implement an audit policy that records an event whenever an account is locked out. After several hours, a user reports that she is still receiving the error message.

Where should you examine the security logs?

A. On the Domain Controller that holds the RID master role.
B. On the Domain Controller that holds the infrastructure master role.
C. On the Domain Controller that holds the PDC emulator role.
D. On the first Domain Controller installed in the domain.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: The PDC emulator gets preference for logons therefore the events would be recorded there.

Incorrect Answers:
A: The Domain Controller that holds the RID master role gives objects the RID. This is not related to user events and is thus not relevant to this problem.
B: The Domain Controller that holds the infrastructure master role controls group membership. This is not related to user events and is thus not relevant to this problem.
D: The PDC emulator may have been moved from the first Domain Controller installed and thus might not be located on this Domain Controller any longer. There this is not the best Answer:

QUESTION 64
You are the administrator of your company's Windows 2000 network. The network contains three DNS servers that are configured as shown in the following table.

Server name	Operating system	Server role	DNS zone type
Server 1	Windows NT Server 4.0	BDC	Primary DNS zone
Server 2	Windows 2000 Server	Domain Controller	Secondary DNS zone
Server 3	Windows 2000 Server	Member Server	Secondary DNS zone

You want to configure the DNS servers to support secure dynamic updates. You must reconfigure the DNS zones appropriately to permit the implementation of secure dynamic updates.

What should you do?

To Answer: click the Select and Place button, and then drag the appropriate DNS zone type to the appropriate server. (Note: Each DNS zone type can be used more than once)

Answer:

Section: (none)

Explanation/Reference:
Explanation:
Only Windows 2000 Active Integrated DNS zones supports secure dynamic updates. The Active Integrated DNS zone must be put on a Domain Controller Server 2. The other DNS servers, both the Windows 2000 member server and the Windows NT 4.0 server can be used as secondary DNS servers.

QUESTION 65
You are the administrator of your company's Windows 2000 network. The network consists of downlevel client computers and Windows 2000 Professional computers. You use DHCP to assign IP addresses for all client computers. You enable secure dynamic updates in DNS and configure DHCP servers to update the A (host) records for the down-level client computers.

You upgrade several down-level client computers to Windows 2000 Professional. You discover that the upgraded computers cannot dynamically update their A (host) records in DNS. You must enable these computers and all client computers that will be upgraded to upgrade their own A (host) records in DNS.

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

A. Add the DHCP servers to the DNSUpdateProxy group in Active Directory.
B. Add all upgraded and down-level client computers to the DNSUpdateProxy group in Active Directory.
C. Delete all existing A (host) records in DNS for the upgraded and down-level client computers.
D. Delete all existing PTR (pointer) records in DNS for the upgraded and down-level client computers.
E. On all upgraded and down-level client computers, manually specify the DNS servers to use DHCP for IP address assignment.
F. On all upgraded and down-level client computers, manually force a release and renewal of their IP addresses.

Answer: AF
Section: (none)

Explanation/Reference:
Explanation: The problem in this scenario is that some upgraded clients cannot dynamically update their A (host) records in DNS. The problem is that before the update a DHCP server registered A (host) records for the down-level clients. In effect the DHCP server that registered the client's A (Host) record now owns that A (Host) record, and the record cannot be released.

By putting the DHCP server in the DNSUpdateProxy group, it will not own the DNS records. When the downlevel clients are upgraded to Windows 2000, they will be able to update their DNS records.

By forcing a renewal of the IP address on all client computers the old A (host) records will be released and a new A (Host) record will be added instead.

Incorrect Answers:
B: The DHCP servers, not the down-level clients, should be added to the DNSUpdateProxy group.
C: Deleting all A (host) records would be a daunting administrative task.
D: Deleting all PTR (pointer) records would be a daunting administrative task
E: The DNS servers use static IP addresses. DNS server and DHCP servers integrate but DNS servers are not DHCP clients.

QUESTION 66
Your company's network consists of a single Windows 2000 domain named contoso.com. You are a member of the Domain Admins group

Your company is acquiring Fabrikam, Inc. The Fabrikam, Inc., company network consists of a single Windows 2000 domain named fabrikam.com

You want to give the Fabrikam Inc. employees user accounts in contoso.com. What should you do?

A. Use the Ntbackup utility to back up the fabrikam.com accounts and then to restore the fabrikam.com accounts to contoso.com.
B. Use the MoveTree utility to move accounts from fabrikam.com to contoso.com.
C. Use a script to re-create the fabrikam.com accounts in the contoso.com domain.
D. Create an external trust between fabrikam.com and contoso.com.
Use the Active Directory Users and Computers snap-in to move the accounts from fabrikam.com to contoso.com.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: With Windows 2000 we can use scripts to copy user accounts from one domain to another domain.

Incorrect Answers:
A: Using the Ntbackup utility to back up the fabrikam.com accounts and then to restore the fabrikam.com accounts to contoso.com would result in the accounts having the same SID. We however need new SIDs from the Contoso domain.
B: Movetree can only be used between 2 domains in the same forest.
D: Creating an external trust between fabrikam.com and contoso.com will enable the users to access the other domain but it will not create the accounts.

QUESTION 67
Your company's network consists of two domains: contoso.com and sales.contoso.com. You are a member of the Enterprise Admins group.

The contoso.com domain contains one Domain Controller named ContosoDC1. The sales.contoso.com domain contains one Domain Controller named SalesDC1. No operations master roles have been moved from their default locations.

A database administrator in sales.contoso.com wants to extend the Active Directory schema by using a custom application. However, you need to temporarily take the computer that owns the schema master role offline for service.

You need to ensure that schema modifications can occur when the server is unavailable. What should you do before you take the server offline?

To Answer: click the select and place button, and then drag the appropriate object to the appropriate destination.

Action	Schema Owner	Targeted Schema Owner
Transfer Schema master	From ContosoDC1	To ContosoDC1
Seize Schema master	From SalesDC1	To SalesDC1

Answer:

Action	Schema Owner	Targeted Schema Owner
Transfer Schema master	From ContosoDC1	To SalesDC1
		To ContosoDC1
Seize Schema master	From SalesDC1	

Section: (none)

Explanation/Reference:
Explanation: We can transfer because the schema master is online. ContosoDC1 has the schema master role because it is the first machine installed in the forest. This must be transferred to the other machine. To accomplish this we can use two methods. The preferred method is to use the Active Directory Schema GUI. This option is not listed here however, so instead we must use the command-line utility ntdsutil.

Note: Transferring the Schema Master Role with ntdsutil.

1. Use an account that is a member of the Schema Administrators group to log on to a domain controller.
2. At a command prompt, type the following command:
   ntdsutil
3. When prompted, type
   roles

4. Next, type
   connections
5. Type
   connect to server <name of domain controller to which the role will be transferred>
6. After server connections: type
   quit
7. Type
   transfer schema master

Reference:
Windows 2000 Server Resource kit, Active Directory Diagnostic Tool (Ntdsutil.exe), Managing Operations Master Roles
HOW TO: View and Transfer FSMO Roles in the Graphical User Interface (Q255690)

QUESTION 68
You are a member of the Enterprise Admins group in your company's Windows 2000 network. The network consists of one domain and two Active Directory sites: Paris and Stockholm. Paris and Stockholm are connected by 56-KB WAN link.

Your company opens a new office in New York. You configure a 56-KB WAN link to connect New York with Paris. The network is now configured as shown in the exhibit.

You want to install a Domain Controller in the New York subnet. You need to minimize the directory replication traffic that is generated by the Domain Controller installation.

What should you do before you install the Domain Controller?

Exhibit:

A. Create an Active Directory subnet and site for New York.
B. Create an Active Directory subnet for New York and associate it with the Paris site.
C. Enable slow link detection in the Default Domain Group Policy Object (GPO).
D. Enable slow link detection in the default Domain Controllers Group Policy Object (GPO).

Answer: A
Section: (none)

Explanation/Reference:
Explanation: In this scenario we should first create a subnet and a site for New York. Then place the subnet in the site. This will allow us to schedule replication to occur over the site links during times that the network is less busy.

Incorrect Answers:
B: We should place the NY subnet in the NY site and not in the Paris site.
C: Slow link detection is used for the application of group policy, not Active Directory replication. This solution is thus not appropriate to this scenario.
D: Slow link detection is used for the application of group policy, not Active Directory replication. This solution is thus not appropriate to this scenario.

QUESTION 69
You are a member of the Enterprise Admins group in your company's Windows 2000 network. Your company consists of 2 offices. Each office has a T1 connection to the internet and uses a virtual private network to establish a direct, secure connection with every other office.

Currently, only two offices, Melbourne and Sydney, contain Domain Controllers. A site link connects these two offices. Your company wants all offices to contain at least one Windows 2000 Domain Controller.

You install a new Domain Controller in the Auckland office. A portion of the network is now configured as shown in the exhibit.

You want to configure Active Directory to minimize site replication delays between all offices. You also want to be able to reschedule replication traffic between all offices with the least amount of administrative effort.

You need to configure directory replication with Auckland. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

Exhibit:

A. Create a new site link between Auckland and Melbourne.
B. Create a new site link between Auckland and Sydney.
C. Add the Auckland site to the existing link between Melbourne and Sydney.
D. Set the replication cost for all site links to a value of 1.
E. Set the replication frequency for all site links to every 15 minutes.

Answer: AB
Section: (none)

Explanation/Reference:
Explanation: In this scenario we are required to create site links between all sites so that we can schedule replication.

Incorrect Answers:
A: We cannot add a site to a link as a link joins two sites.
B: By default, the replication cost for all site links has a value of 1. We would therefore not be altering the site link configurations by setting the replication cost for all site links to a value of 1.
C: Setting the replication frequency for all site links to every 15 minutes will increase replication traffic, as the default replication frequency is 180 minutes.

QUESTION 70
Your company's network consists of two Windows 2000 domains: contoso.com and sports.contoso.com. Both domains operate in mixed mode.

The sports.contoso.com domain contains two Windows 2000 Domain Controllers and one Windows NT 4.0 member server. You and another employee named Sophie are members of the Domain Admins group in the sports.contoso.com domain.

You and Sophie need to create several global groups that will be used to grant permissions for shared folders. Sophie creates a global group named Teams. You create three global groups: Basketball, Baseball, and Hockey.

You want to add the Basketball, Baseball, and Hockey global groups to the Teams global group by using the least amount of administrative effort. What should you do?

A. Convert only sports.contoso.com to native mode.
B. Convert contoso.com to native mode, and then convert sports.contoso.com to native mode.
C. Convert sports.contoso.com to native mode, and then convert contoso.com to native mode.
D. Convert only contoso.com to native mode.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: In this scenario we want to add the Basketball, Baseball, and Hockey groups to the Teams global group in the sports.contoso.com domain therefore we only need to convert this domain to native mode so that we can nest global groups.

Incorrect Answers:
B: We do not need to convert contoso.com to native mode, as all the groups we want to nest are located in the sports.contoso.com domain.
C: We do not need to convert contoso.com to native mode, as all the groups we want to nest are located in the sports.contoso.com domain.

D: We do not need to convert contoso.com to native mode, as all the groups we want to nest are located in the sports.contoso.com domain.

QUESTION 71
You are the administrator of your company's Windows 2000 domain. The domain contains an Organizational Unit (OU) named Marketing. Users in the Marketing OU frequently work on different Windows 2000 Professional computers in the domain. The domain also contains a Windows 2000 Server computer named Server1.

You want to accomplish the following goals:

- Users in the Marketing OU will have their own desktop settings available on all computers.
- All users in the Marketing OU will be able to access their My Documents folder from any Windows 2000 computer in the domain.
- Contents of the My Documents folders will not be automatically copied to or from the server when users log on to or log off of the domain.

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

A. For each user in the Marketing OU, configure a roaming profile. Use \\Server1\Profiles\%username% as the profile path.
B. For each user in the Marketing OU, configure a Home folder. Use \\Server1\Homedrives\%username% as the home drive path.
C. Create a Group Policy Object (GPO) that is linked to the Marketing OU to redirect the My Documents folder for users in the Marketing OU. Use \\Server1\Docs\%username% as the redirected path.
D. Create a Group Policy Object (GPO) that is linked to the Marketing OU to redirect the Desktop folder for each user in the Marketing OU. Use \\Server1\Profiles\%username% as the redirected path.
E. Create a Group Policy Object (GPO) that is linked to the Marketing OU to create roaming profiles for users in the Marketing OU. Use \\Server1\profiles\%username% as the roaming profile path.

Answer: AC
Section: (none)

Explanation/Reference:
Explanation:
A: We must create roaming profiles, as they are required by users who logon to the network from different locations or computers but who require the same desktop setting regardless of where they logon.
C: We must then redirect the My Documents folders so that the files in the My Documents can be accessed by users regardless of where and from which computers they use to logon to the network. By redirecting the My Documents folder, the roaming profile will access the folder on the network location rather than down loading it onto the logon computer. This will reduce network traffic.

Incorrect Answers:
B: Home folders are not appropriate to this scenario. We need to redirect My Documents.
D: The desktop folder is already part of the roaming profile therefore we do not have to redirect the desktop folder
E: Roaming profiles are not defined by Group Policy objects.

QUESTION 72
You are the administrator of your company's Windows 2000 domain. The domain contains one Domain Controller.

The Domain Controller is running out of disk space on the volume that contains the Active Directory database.

You decide to move the database to an empty volume on a different disk. You want to complete this task with the least possible interruption to this server.

What should you do?

A. Restart the server in directory services restore mode. Use the Ntdsutil utility to move the database file to the empty volume.
B. Create a backup of the system state data. Restart the server in directory services restore mode. Restore the system state data to the empty volume.
C. Restart the server in directory services restore mode. Use Windows Explorer to move the database file to the empty volume.
D. Create a backup of the system state data. Restart the server in Recovery Console mode. Restore the system state data to the empty volume.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: The Ntdsutil command-line utility in Directory Services Restore mode is used to move the Active Directory database. This utility automatically updates the registry keys so that Active Directory will start from the location it was moved to. We can enter this Directory Services Restore mode by pressing F8 to display the Windows 2000 Advanced options menu. We must then logon using the Administrators account and type NTDSUTIL at the command prompt, specify files, then type 'MOVE DATABASE TO [drive letter:\directory name]'. Finally, we must reboot the Domain Controller for the changes to take effect.

Incorrect Answers:
B: We cannot restore the Active Directory database to a different location, as the registry keys will still point to the old location. Therefore Active Directory will not start properly as it would not be able to access the database.
C: We cannot move the Active Directory database to a different location, as the registry keys will still point to the old location. Therefore Active Directory will not start properly as it would not be able to access the database.
D: We cannot restore the Active Directory database to a different location, as the registry keys will still point to the old location. Therefore Active Directory will not start properly as it would not be able to access the database.

QUESTION 73
Your company's network consists of a single Windows 2000 domain. You are a member of the Domain Admins group. You install a Windows 2000 member server, and then install Remote Installation Services on the member server.

You enable the RIS server to respond to client computers. You successfully load a CD-based image on the server. You attempt to initiate a RIS session on your first PXE-compliant client computer, but your RIS server does not respond to the request.

You want to ensure that the RIS server responds to client computers. What should you do?

A. Install DNS on the RIS server.
B. Install WINS on the RIS server.
C. Authorize the RIS server.
D. Assign the RIS server an address by means of DHCP.
E. Add a reservation for each client computer on the DHCP server.

Answer: C

Section: (none)

Explanation/Reference:
Explanation: By default, a RIS server is not configured to begin servicing client computers immediately after the installation of the RIS server is completed. To configure RIS we must authorize RIS servers, set RIS server properties, set RIS client installation options, and set RIPrep image permissions. In this scenario the RIS server must still be authorized.

Incorrect Answers:

A: All Windows 2000 domains require DNS for Active Directory therefore we already have a DNS server, which was set up when the domain was created.
B: RIS requires a DHCP server and a DNS sever with Active Directory. The DHCP server is required for IP address leasing and the DNS server with Active Directory is required for name resolution. A WINS server is required for compatibility purposes when non-Windows 2000 computers are part of the domain. In this scenario however, the RIS server has not been authorized.
D: The RIS server does not need a dynamic IP address. It must be authorized instead.
E: The RIS server does not require IP reservations for each client. It must be authorized instead.

QUESTION 74
You are a member of the Enterprise Admins group in your company's Windows 2000 network. The network exists in one building and consists of a single Active Directory site. The site contains one subnet.

Users in the sales department are moving to a new building named Building B. You configure a 56-KB WAN link to connect both buildings. You create a new Active Directory subnet for Building B. The network is now configured as shown in the exhibit.

You want to add a Domain Controller to Subnet B. You also want to minimize directory replication traffic over the WAN.

What should you do before you install the Domain Controller?

Exhibit:

A. Associate the existing site with both subnets.
B. Create a new Active Directory site and associate it only with Subnet B.
C. Create a new Active Directory site and associate it with both subnets.
D. Associate the existing site only with Subnet B.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: To enable scheduled replication, we must create sites that we can schedule replication to occur across the site link. In this scenario we need a site for subnet B so that we can schedule replication.

Incorrect Answers:
A: We can only schedule replication between two sites. We therefore cannot associate both subnets with one site.
C: The procedure suggested in this solution is incorrect. We must associate the subnet a site, not an Active Directory site with a subnet.
D: We can only schedule replication between two sites. We therefore cannot only associate Subnet B with the existing site; we require the creation of a second site as well.

QUESTION 75
Your company's network consists of two Windows 2000 domains: contoso.com and newyork.contoso.com. The newyork.contoso.com domain contains three organizational units: Sales, Marketing, and Finance. You are a member of the Domain Admins group in newyork.contoso.com

An employee named Stephan is the administrator for the Finance OU. Stephan reports that he cannot edit any Group Policy Object. Administrators for the Sales and Marketing OUs report no problems editing GPOs.

You want Stephan to be able to edit GPOs. What should you do?

A. Delegate to Stephan the ability to manage Group Policy Links for the Finance OU.
B. Grant Stephan the read permission and the create group objects permissions for the Finance OU.
C. Grant Stephan the read permission and the apply group policy objects permission for the GPOs he wants to edit.
D. Add Stephan to the group policy creator group in newyork.contoso.com.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Active Directory supports security settings on individual properties. Thus, a non-administrator can be given Read and Write access to specific properties. If non-administrators have Read and Write access to the gPLink and gPOptions properties, they can manage the list of Group Policy objects linked to that site, domain, or organizational unit. To give a user Read and Write access to these properties, use the Delegation of Control Wizard and select the Manage Group Policy links predefined task. Thus, by delegating the task to manage Group Policy Links for the Finance OU to Stephan, he will be able to manage and edit the already existing GPOs that are linked to the Finance OU.

Incorrect Answers:
B: In this scenario Stephan must be able to edit GPOs, not to create them.
C: This will just apply the GPOs to himself
D: Adding Stephan to the group policy creator group in newyork.contoso.com would enable him to create GPOs anywhere in the domain.

QUESTION 76
You are a member of the Enterprise Admins group in your company's Windows 2000 domain. Users in the Finance department keep losing their membership in an Active Directory group. You turn on auditing to monitor changes to Active Directory.

The next day, you discover that the Finance users have been removed from the group again. You open the security event log and find several thousand events. You want to reduce the number of security events you must analyze in order to discover who is removing the Finance users from the group.

You open the Event Viewer snap-in. You need to filter the security log to include only the events located in the appropriate category. Which categories should you choose? (Choose Two)

A. Directory service access.
B. Account management.
C. Privilege use.
D. Policy change.

Answer: AB
Section: (none)

Explanation/Reference:
Explanation: In this scenario we should analyze the directory service access as this provides information on when a user gained access to an Active Directory object. We should also analyze account management as group membership changes are logged by auditing account management. This includes: when an administrator created, changed, or deleted a user account or group, a user account was renamed, disabled, or enabled, or a password was set or changed.

Incorrect Answers:
C: Auditing Privilege use logs events when a user exercised a right, such as changing the system time (this does not include rights that are related to logging on and logging off).
D: Auditing Policy change logs changes that were made to the user security options, user rights, or audit policies.

QUESTION 77
You are the administrator of your company's Windows 2000 network. The company has one office in New York and one in Boston. The offices are connected by a WAN link. An Active Directory site and an organizational unit (OU) are configured for each office.

Users in the Boston Sales department are moving to New York. You want to move one of the two Domain Controllers in Boston to New York.

After you transport the Domain Controller to New York and connect it to the New York subnet, users report that all network activity between New York and Boston is slow.

You want to improve network performance between New York and Boston. What should you do?

A. Using the Active Directory sites and services snap-in, configure the site link between Boston and New York for less frequent replication.
B. Using the Active Directory users and computers snap-in, change the location file of the Boston server object from Boston to New York.
C. Using the Active Directory users and computers snap-in, move the Domain Controller from the Boston OU to the New York OU.
D. Using the Active Directory sites and services snap-in, move the Domain Controller from the Boston site to the New York site.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: Sites define sets of domain controllers that are well-connected in terms of speed and cost. It is important for Active Directory replication to create a site for each well-connected subnet, associate subnets with the correct site, and add the domain controllers to the appropriate sites.

In this scenario we have physically moved a domain controller from the Boston subnet to the New York subnet. To improve network performance we should also move the domain controller Active Directory object from the

Boston site to the New York site. This is accomplished by using the Active Directory sites and services snap-in.

Note: Sites contain only computer objects and connection objects used to configure replication between sites.

Incorrect Answers:
A: In this scenario we want to eliminate the cause of the extra replication as this is reducing network performance. Less frequent replication will reduce replication traffic, but it will not address the problem at hand: one domain controller has been moved from one subnet to another subnet without being moved to the appropriate site.
B: The location file of the Boston server object displays a description of the Boston server in the Active Directory. Updating the location file would not improve network performance.
C: We should first move the domain controller to the appropriate site to improve network performance. Then we could move it to the appropriate OU for administrative purposes.

QUESTION 78
Your company's network consists of two divisions: Contoso Ltd, and Fabrikam Inc. Each division has two domains. All domains are contained in the same forest.

Contoso Ltd. contains two domains: contoso.com and sales.contoso.com, Fabrikam Inc. contains two domains: fabrikam.com and sales.fabrikam.com. The sales.contoso.com domain and the sales.fabrikam.com domain each contain an OU named Marketing.

Fabrikam, Inc. is changing its name to Litware, Inc. You need to create a user principle name (UPN) of litware.com. Users in both Marketing OUs will use the UPN to be authenticated by Active Directory.

At which level in Active Directory should you create the UPN?

A. The Marketing OU in sales.contoso.com and the Marketing OU in sales.fabrikam.com.
B. The contoso.com domain tree and the fabrikam.com domain tree.
C. The root domain.
D. The forest.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: The UPN, which stands for User Principal Name, is “user friendly” and a UPN is composed of a shorthand name for the user account and the DNS name of the tree where the user account object resides. For example, user Firstname Lastname (substitute the first and last names of an actual user) in the microsoft.com tree might have a UPN of FirstnameL@microsoft.com (using the full first name and the first letter of the last name). Hence the UPN is made up of the complete domain name therefore changes must be made at the top of the domain tree.

Reference: Users Can Log in Using User Name or User Principal Name (Q243280)
HOW TO: Add UPN Suffixes to a Forest (Q243629)

Incorrect Answers:
A: The UPN is made up of the complete domain name therefore changes must be made at the top of the domain tree and not at the OU level.
C: The root domain is the first domain created. It might not be the top of the Fabrikam tree. Therefore this is not the best Answer:
D: The UPN is made up of the complete domain name. It is therefore related to the domain tree and not the forest.

QUESTION 79
You are the administrator of your company's Windows 2000 network. In the Payroll folder of a file server, you configure auditing to track all file activity. One week later, you are asked to discover if any files in the Payroll folder have been accessed by a user account named CSeeley.

You verify that the audit log contains data for all payroll transactions during the past week. This data includes thousands of transaction events about files accessed by everyone in the company. You want to review only transaction event data for the CSeeley user account.

What should you do?

A. View the Audit tab of the properties page for the CSeeley user account.
B. Reconfigure auditing of the files in the Payroll folder for only the CSeeley user account, and then refresh the Event Viewer.
C. Export the audit log to CSV format, and then use Microsoft WordPad to display log entries that contain the text “CSeeley”
D. Apply an Event Viewer filter that displays only events containing the text “CSeeley” in the User field.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: To analyze the transaction event data for a particular user account we must use Event Viewer to create a filter to display records containing the user name.

Incorrect Answers:
A: In Windows 2000 the properties page for user accounts do not have an audit tab.
B: By refreshing the Event Viewer we will start a new audit. In this scenario we need to analyze the existing logs.
C: It is possible to export an audit log file to a comma-delimited file that can then be viewed in a spreadsheet programme such as Microsoft Excel. However, Windows 2000 has a built-in Event Viewer that can be used to filter and view audit log files. It is thus not necessary to export the audit log.

QUESTION 80
You are the administrator of your company’s network. The network consists of one Windows 2000 domain that spans multiple subnets. You are configuring DNS for host name resolution throughout the network.

You want to accomplish the following goals:

- DNS zone transfer traffic will be minimized on the network.
- Administrative overhead for maintaining DNS zone files will be minimized.
- Unauthorized host computers will not have records created in the zone.
- All zone updates will come only from authorized DNS servers.
- All zone transfer information will be secured as it crosses the network.

You take the following actions:

- Create an Active Directory integrated zone.
- In the Zone Properties dialog box, set the Allow Dynamic Updates option to "Only Secure Updates".
- On the Name Servers tab of the Zone Properties dialog box, enter the names and addresses of all DNS servers on the network.
- On the Zone Transfers tab on the Zone Properties dialog box, select the Allow zone transfer only to
- servers listed on the Name Servers tab option.

Which result or results do these actions produce? (Choose all that apply)

A. DNS zone transfer traffic is minimized on the network.
B. Administrative overhead for maintaining DNS zone files is minimized.
C. Unauthorized host computers do not have records created in the zone.
D. All zone updates come only from authorized DNS servers
E. All zone transfer information is secured as it crosses the network.

Answer: ABCDE
Section: (none)

Explanation/Reference:
Explanation:
A: Active Directory integrated zones use incremental transfers; therefore zone transfer traffic is minimized on the network.
B: Dynamic updates negate the need for manually updating the zone file by manually adding records and thus minimizes administrative overhead for maintaining DNS zone files.
C: We have selected the "Only Secure Updates" option. This will ensure that no unauthorized host computers have records created in the zone.
D: To ensure that all zone updates come only from authorized DNS servers we have selected the Allow Zone transfers only to the servers listed on the Name servers tab option on the zone transfers tab of the zone properties dialog box.
E: Active Directory integrated zone transfers are included in the Active Directory replication, which uses a secure RPC channel therefore all zone transfer information is secured as it crosses the network.

QUESTION 81
You are the administrator of the Contoso Ltd. company network. You are designing a Windows 2000 domain. Contoso Ltd. has an Internet presence and owns contoso.com, a registered domain name. The existing DNS zone is hosted on Windows NT Server 4.0 computers.

You want to accomplish the following goals:

- Internal host names will not be exposed to the Internet.
- Internal host users will be able to resolve external names for access to Internet-based resources.
- Complexity and depth of domain names for Active Directory will be minimized.
- To comply with management requirements, the existing DNS servers that host the zone for contoso.com will not be upgraded.

You implement a DNS design as shown in the exhibit.

Which result or results does your implementation produce? (Choose all that apply)

x081 (exhibit):

x081_2 (exhibit):

A. Internal host names will not be exposed to the Internet.
B. Internal users will be able to resolve external names for access to Internet based resources.
C. Complexity and depth of a domain names for Active Directory will be minimized.
D. To comply with management requires the existing DNS server's host the zone for contoso.com will not be upgraded.

Answer: ABCD
Section: (none)

Explanation/Reference:
Explanation: With a private network name and primary DNS, internal names will not be exposed to the Internet.

The internal DNS has a secondary zone for the external DNS and we are not using a child domain of the external domain. Furthermore, it is not necessary to upgrade the external DNS.

QUESTION 82
You are the network administrator for Litware Inc. You are implementing Windows 2000 on your network. Part of your network configuration is shown in the exhibit.

You have installed Server2 and Server4 as Domain Controllers for litware.com. You have installed Server1 and Server3 as DNS servers for the litware.com domain.

Each server has a standard primary zone named litware.com. You configure the domain to run in native mode.

When Server2 attempts to contact Server4 by name, it cannot establish a connection. However, you can ping both Server2 and Server4 from any computer in either site. You need to be able to resolve names of servers in both sites. You want the information to be updated regularly.

What should you do?

Exhibit:

A. Configure Server1 and Server3 to allow dynamic updates in DNS.
B. Configure Server1 and Server3 to allow zone transfers to any server. Then configure the DNS notification options to notify each server of updates.
C. Reinstall Server4 as a member server in the same domain as Server2. Create a new site, and promote Server4 to a Domain Controller within the new site.
D. Re-create the litware.com zone on Server3 as a secondary zone. Configure Server3 to replicate DNS data from Server1.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: To replicate the zones we must create a primary and a secondary DNS server. Windows 2000 does not allow for replication between two primary DNS Servers for the same zone on different DNS servers. Furthermore, there can only be one primary DNS zone, but there can be several secondary DNS zones.

Incorrect Answers:
A: Dynamic updates in DNS will not affect zone replication.
B: Windows 2000 does not allow for replication between two primary DNS Servers.
C: Sites are required for scheduling Domain Controller replication and are not related to DNS replication. Therefore this solution is inappropriate.

QUESTION 83
You add a new Domain Controller named GC01 to your network to take the place of the existing Global Catalog server. You also enable GC01 as a Global Catalog. You want to use GC00, the original server, as a Domain Controller, but not as a Global Catalog server for the domain. You want to increase disk space on GC00. What should you do? (Choose all that apply)

A. Open the Active Directory Sites and Services snap-in. Select the NTDS settings object for the GC00 Server to clear the **Global Catalog** check box.

B. On the GC00 server, run the Ntdsutil utility to defragment Active Directory.
C. On the GC00 server, reinstall Windows 2000.
D. On the GC01 server, run the Ntdsutil utility to enable the Global Catalog server option.

Answer: AB
Section: (none)

Explanation/Reference:
Explanation:
A: To stop GC00 from serving as a Global Catalog we must select the NTDS settings object for the GC00 Server to clear the Global Catalog check box in Active Directory Sites and Services.
B: We must then run the Ntdsutil utility to defragment Active Directory on the GC00 server. This will clear Global Catalog data from the Active Directory database of GC00 and recover the disk space used by the Global Catalog data.

Incorrect Answers:
C: In is not necessary to reinstall Windows 2000 as we could use Active Directory Sites and Services to stop the server from serving as a Global Catalog.
D: The Ntdsutil utility is not used to enable the Global Catalog server option.

QUESTION 84
You are the LAN administrator for Arbor Shoes. You hire Sophia to be a LAN administrator for the Dublin office. Arbor Shoes has one domain named arborshoes.com. Each office has its own OU. Sophia needs to be able to create child OUs under only ou=Dublin, dc=arborshoes, dc=com and verify the existence of the created OUs.

Which permissions should you assign to Sophia on the Dublin OU? (Choose three)

A. Full Control.
B. List Contents.
C. Create Organizational Unit objects.
D. Create All Child Objects.
E. Write.
F. Read.

Answer: BCF
Section: (none)

Explanation/Reference:
Explanation: To be able to verify the existence of the created OUs Sophia would require Read and List contents permission on the Dublin OU. She would also require Create OU objects permission to create OUs to be able to create child OUs.

Incorrect Answers:

A: Sophia does not require Full Control permissions. She only requires Create OU objects permission to create OUs and Read and List contents permission to be able to verify the existence of the created OUs. Providing Sophia with Full control permissions would grant her too much privilege.
D: The create All Child Objects permissions would enable Sophia to create any object in the Dublin OU.
E: The Write permissions would enable Sophia to modify existing objects in the Dublin OU.

QUESTION 85
You are the enterprise administrator in your company's Windows 2000 network. The network consists of a

domain tree that contains five domains. All domains are in native mode. Each domain has one or more users who are help desk staff. Each domain has a global group named Members that contains the help desk staff from each domain.

There is an Organizational Unit (OU) named Interns in the root domain. You want all help desk staff to be able to reset passwords of the users in the Inters OU.

What should you do?

A. Create a new global security group named Staff in the root domain.
   Place the five Members groups in Staff group.
   Create a new local security group named Reset Interns in the root domain.
   Place the Staff group in the Reset Interns group.
   On the reset Interns group, grant the Reset Password permission to the Staff group.
B. Create a new global security group named Staff in the root domain.
   Place the five Members group in the Staff group.
   Create a new local security group named Reset Interns in the root domain.
   Place all users from the Interns OU in the Reset Inters group.
   On the Interns OU, grant the Reset Password permission to the Reset Interns group.
C. Create a new universal security group named Staff in the root domain.
   Place the five Members groups in Staff group.
   Create a new local security group named Reset Interns in the root domain. Place the Staff group in the Reset Interns group.
   On the Interns OU, grant the Reset Password permission to the Reset Interns group.
D. Create a new universal security group named Staff in the root domain.
   Place the five Members groups in Staff group.
   Create a new local security group named Reset Interns in the root domain.
   Place all users from the Interns OU in the Reset Interns group.
   On the Reset Interns group, grant the Reset Password permission to the Staff group.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: The correct procedure to assign permissions is to use universal groups to group global groups, then place the universal group in a local group and assign permission to the local group.

Incorrect Answers:
A: We cannot group global groups from multiple domains in one global group. We must use universal groups to group global groups.
B: It is not necessary to place all users in the interns group.
D: It is not necessary to place all users in the interns group.

QUESTION 86
You add three new SCSI hard disk drives to your company's Domain Controller. The SCSI disks are configured in a hardware RAID-5 array. You have two other physical disks in this Domain Controller. You want to optimize the speed of the Active Directory database.

What can you do? (Choose two)

A. Move the Ntds.dit file to the RAID-5 array.
B. Move the log files to a separate physical disk from the operating system.
C. Move the log files and the Ntds.dit file to the RAID-5 array.
D. Move the Netlogon share to the RAID-5 array.

E. Create a mirror volume and place the log files on the mirror.

Answer: AB
Section: (none)

Explanation/Reference:
Explanation: To optimize the speed of the Active Directory database we should move the Active Directory database file to the RAID-5 array as this provides faster read and write speeds than a single disk. Furthermore, we should place the log files on a separate disk to the Active Directory database.

Incorrect Answers:
C: To improve performance we should place the log files and the ntds.dit file on separate disks.
D: Moving the Netlogon share to the RAID-5 array will not improve the performance of the Active Directory database, as the Netlogon is not related to the Active Directory database.
E: Mirrored disks will not improve performance, as the changes to the system must be written to both hard drives. This will in fact degrade performance.

QUESTION 87
You are the administrator of Trey Research and ADatum Corporation. You manage a multi-domain Windows 2000 network of 5,000 users for the two companies. The network is configured as shown in the exhibit.

The two companies have a total of six departments. Each department is an organizational unit in Active Directory.

Each domain and OU has specific group policy settings that must be applied to all of its members. Your company is reorganizing all six departments. Some, but not all, of the users in each OU have moved. Many users have changed departments, and some have changed domains.

You want to accomplish the following goals in the least possible amount of time:

- Place the user accounts in the appropriate domains.
- Apply the existing policies for each domain or OU to the moved account.
- Do not disrupt user access to shared resources.

What should you do?

Exhibit:

A. For all users, create a new user account in the appropriate OU. Assign permissions to the accounts to apply group policy settings, and then delete the old accounts.
B. For the users moving between domains, create new user accounts in the appropriate OUs. Assign permissions to the account to apply the group policy settings, and then delete the old accounts. For the users moving between OUs in the same domain select the accounts then choose move from the action menu, targeting the new OU.
C. For the users moving between domains, use the Movetree utility, specifying the source and target domains and the OUs. For the users moving between OUs in the same domain, select the accounts. Then choose **move** from the **action** menu, targeting the new OU.
D. For the users moving between domains, create new user accounts in the appropriate OUs. Assign permissions to the account to apply group policy settings, and then delete the old accounts. For the users moving between OUs in the same domain, select the accounts. Then choose copy from the action menu, entering the appropriate account information for the new user accounts. Then delete the old accounts.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: The movetree utility can be used to move users between domains in the same forest, while the move command is used to move users between OUs.

Incorrect Answers:
A: It is not necessary to recreate the user accounts on the new domain as we can use the movetree utility to move users between domains in the same forest.
B: It is not necessary to recreate the user accounts on the new domain as we can use the movetree utility to move users between domains in the same forest.
D: It is not necessary to recreate the user accounts on the new domain as we can use the movetree utility to

move users between domains in the same forest.

QUESTION 88
You are the administrator of the company network for Arbor Shoes. Arbor Shoes has three domains: arborshoes.com, na.arborshoes.com, and sa.arborshoes.com. All the domains are in native mode. You are going to remove the na.arborshoes.com domain in an effort to consolidate domains. There are 300 users in na. arborshoes.com. You want to move all 300 users at the same time to arborshoes.com.

What should you do?

A. At the command prompt, type the following command: Cscript sidhist.vbs/srcdc:dc1/srcdom:na.arborshoes. com /dstdc:dc1 /dstdom:arborshoes.com.
B. At the command prompt, type the following command: Movetree /start /s dc1.na.arborshoes.com/ddc1 arborshoes.com/sdncn=users,dc=na,dc=arborshoes,dc=com /ddn cn=users, dc=arborshoes, dc=com.
C. In MMC, use the **copy** command in Active Directory Users and Computers.
D. In MMC, use the **move** command in Active Directory Users and Computers.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: The movetree utility can be used to move users between domains in the same forest. However the move tree utility cannot be used to move Local and Global groups that contain members between domains. To move Local and Global groups that contain members between domains we must make use of scripts or the netdom command.

Incorrect Answers:
A: sidhist.vbs keeps a copy of the old user account SID. This is used if we are moving users that would still require access to resources on the old domain.
C: We cannot copy users to a new domain; we must use the movetree utility to move users between domains in the same forest.
D: The **move** command in Active Directory Users and Computers can only be used to move users between OUs in the same domain. It cannot be used to move users between domains in the same forest. The movetree utility can be used to move users between domains in the same forest.

QUESTION 89
You are the administrator of a Windows 2000 Network. Your network's organizational unit (OU) structure is shown in the exhibit.

You grant Create Users Objects permission to Anita for the Executive OU, but she is unable to create users objects in the Users OU. Anita is able to create users objects in the Workstation OU.

What should you do to enable Anita to create users objects in the Users OU?

Exhibit:

A. Clear the Allow inheritable permissions from parent to propagate to this object check box in the Executive OU properties.
B. Select the Allow inheritable permissions from parent to propagate to this object check box in the Users OU properties.
C. Add Anita to the Server Operators group.
D. Move the Users OU to the same level as the Executive OU.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: Selecting the Allow inheritable permissions from parent to propagate to this object check box in the Users OU properties will allow the permissions to be inherited by the users OU.

Incorrect Answers:
A: Clearing the Allow inheritable permissions from parent to propagate to this object check box in the Executive OU properties will block permissions set at the domain level.
C: Adding Anita to the Server Operators group would provide her with too much permission.
D: We cannot propagate permissions to OUs on the same level therefore moving the Users OU to the same level as the Executive OU would not affect the propagation of permissions. We would instead have to set the permissions on each OU.

QUESTION 90
You are hired by Fabrikam Inc. to secure its Windows 2000 network. You use Security Templates to create a custom template and save it as Securefab.inf.

You need to use this template on 5 Domain Controllers in fabrikam.com domain. What should you do? (Choose two)

A. Copy the Securefab.inf file to Sysvol shared folder on one Domain Controller.
B. Create a new security database.
C. Import the Securefab.inf file.
D. Rename Securefab.inf to NTconfig.pol.
E. Create a Group Policy Object (GPO) on Domain Controllers organizational unit (OU).
F. Configure the File Replication service to replicate the template file to all Domain Controllers.

Answer: CE
Section: (none)

Explanation/Reference:
Explanation: To use this template on 5 Domain Controllers in fabrikam.com domain we should create a GPO for the Domain Controllers and import the security template to the GPO.

Incorrect Answers:
A: Coping the Securefab.inf file to Sysvol shared folder on one Domain Controller will result in the security template being replicated to the 5 Domain Controllers but will not result in the application of the template.
B: It is not necessary to create a new security database as the security template has already been created.
D: The Ntconfig.pol is used for Windows NT system policies. It is not used in Windows 2000.
F: Configuring the file replication service to replicate the template file to all Domain Controllers will result in the security template being replicated to the 5 Domain Controllers but will not result in the application of the template.

QUESTION 91
You are the security analyst for Duluth Mutual Life. You are assessing the security weaknesses of the company's Windows 2000 network. The network consists of three sites in one domain. The domain contains three OUs and 11,000 users. There are five Domain Controllers in the domain. You configure one of the Domain Controllers to meet the security requirements of the company. You need to duplicate those settings on the other four Domain Controllers. You want to use the least possible amount of administrative effort. What should you do?

A. Create a GPO for the Domain Controllers OU. Configure the GPO settings to match the settings of the secured Domain Controller.
B. Open Security Configuration and Analysis on the secured Domain Controller. Export the secured Domain Controller's security configuration to a template file. Copy the template file to the Sysvol folder on each Domain Controller.
C. Create a GPO for the domain. Assign Domain Users Read and Apply Group Policy permissions. Configure the GPO settings to match the settings of the secured Domain Controller.
D. Open Security Configuration and Analysis on the secured Domain Controller. Export the secured Domain Controller's security configuration information to a template file. Open Security Configuration and Analysis on the other Domain Controllers, import the template file, and then select **Analyze Computer Now**.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: To duplicate the security settings of one Domain Controller to the other four Domain Controllers in the domain, we must create a GPO for the Domain Controllers OU and configure the GPO settings to match the settings of the secured Domain Controller or we must open Security Configuration and Analysis on the secured Domain Controller, export the secured Domain Controller's security configuration information to a template file, then open Security Configuration and Analysis on the other Domain Controllers, import the template file, and select the Configure Computer Now option.

Incorrect Answers:
B: Exporting the secured Domain Controller's security configuration to a template file and coping this template file to the Sysvol folder on each Domain Controller would result in the security template being replicated on the other Domain Controllers but will not result in the template being applied on the other Domain Controllers.
C: Assigning Domain Users Read and Apply Group Policy permissions would result in the policy being applied to all objects in the domain and not just the Domain Controllers.
E: To duplicate the security settings of one Domain Controller to the other four Domain Controllers in the domain, we must open Security Configuration and Analysis on the secured Domain Controller, export the secured Domain Controller's security configuration information to a template file, then open Security Configuration and Analysis on the other Domain Controllers, import the template file, and select the Configure Computer Now option and not the Analyze Computer Now option.

QUESTION 92
You edit the Default Domain Controllers Group Policy on the arborshoes.com domain to require passwords to be at least eight characters long. However, users are able to create passwords that do not comply with the implemented policy. What should you do?

A. Initiate replication to make sure the Group Policy containers and the Group Policy template (GPT) are replicated.
B. Configure each client computer to have a local Group Policy that requires password to be at least eight characters long.
C. Edit the Default Domain Group Policy to require passwords to be at least eight characters long.
D. Edit the Default Domain Controllers Group Policy to force the password to meet complexity requirements.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: As users are able to create passwords that do not comply with the Group Policy, the wrong GPO has been edited, instead of configuring the Default Domain Controllers Group Policy we should have configured the Default Domain Group Policy. As password policies must always be applied at domain level.

Incorrect Answers:
A: Initiating replication to make sure the Group Policy containers and the Group Policy template (GPT) are replicated will not ensure that the policy is applied as the policy has been applied to the wrong container.
B: Configuring each client computer to have a local Group Policy that requires password to be at least eight characters long would increase administrative overhead. The same function can be accomplished through the use of Group Policies.
E: Password policies must be applied at domain level.

QUESTION 93
You are the administrator of your company's network. The network consists of one Windows 2000 domain. The domain contains four organizational units as shown in the following exhibit.

You want to centralize security policy in your domain. You create the following three security templates and Group Policy Objects.

- SecPol1 defines Password, Audit, and User Rights Policies.
- SecPol2 defines User Desktop policy, File System security, and registry security.
- SecPol3 defines a High Security User Desktop policy for network administrators.

You want the GPOs to apply your security policies to users and computers in the domain. You want to use the fewest assignments possible. Where possible, you want Group Policy to apply at the OU level for more

granular administrative control.

How should you apply security policies?

To Answer: click the Select and Place button, and drag A, B, C, and D to the correct locations. (Note: Letters can be used more than once.)

Answer:

Section: (none)

Explanation/Reference:
Explanation:
Drag Secpol1 to the top (domain level).
Password policies must be applied at domain level.
Drag Secpol 2 to the Corp OU level.
The policy will filter down to the other OUs.
Drag Secpol3 to the IT OU.
Only Admins should receive this policy.
Drag No GPO applied to the Sales OU and to the Mktg OU.
These OU inherits the settings applied at the domain level and at the Corp OU level.

QUESTION 94

You are the administrator of your company's Windows 2000 domain. You want to deploy a custom Microsoft Windows installer application named Payroll.

You want to deploy the Payroll application in two Phases. For Phase I, you want only users in the Payroll Pilot security group to install the application by using a Start menu shortcut.

For Phase II, you want all users in the domain to install the application by using Add/remove Programs in Control Panel.

You need to deploy the Payroll application. Which two courses of action should you take? (Each correct answer presents part of the solution. choose two)

A. For Phase I, create an Organizational unit (OU) for only the Payroll application users. Use the Security Configuration and Analysis snap-in to create a custom .inf template that runs the setup routine for the Payroll application. Create a Group Policy Object and link the GPO to the OU. Import the custom .inf template to the GPO.
B. For Phase I, create a Group Policy Object that assigns the Payroll application to the domain. For the Group Policy Object, remove the apply group policy permissions from the Authenticated Users group. Grant the Payroll pilot group the apply Group Policy Permission.
C. For phase I, create a Group Policy Object that publishes the Payroll application to the domain. For the Group Policy Object, remove the apply group policy permissions from the Authenticated Users group. Grant the Payroll pilot group the apply Group Policy Permission.
D. For Phase II, remove the Group Policy Object that you created in Phase I. Use the Security Configuration and Analysis snap-in to create a custom .inf template that runs the setup routine for the Payroll application. Create a GPO and link the GPO to the domain. Import the custom .inf template to the GPO.
E. For Phase II, modify the Group Policy Object to assign the Payroll application to the domain. For the Group Policy Object, grant the Authenticated Users group the Apply Group Policy permission. Remove the Apply Group Policy Permission from the Payroll Pilot group.
F. For Phase II, modify the Group Policy Object to publish the Payroll application to the domain. For the Group Policy Object, grant the Authenticated Users group the Apply Group Policy permission. Remove the Apply Group Policy Permission from the Payroll Pilot group.

Answer: BF
Section: (none)

Explanation/Reference:
Explanation:
B: For Phase I we assign the application to the domain through a GPO, but we only grant the Payroll Pilot group the apply Group Policy permission to the GPO. The application could then be installed through a Start menu short-cut for the Payroll Pilot users.

F: For Phase II we publish the application instead of assigning it. We also change the permission so that all authenticated domain users are granted Apply Group Policy permission to the GPO.

Note: In Windows 2000 we can manage the installation of software on a client computer centrally by assigning applications to users or computers or by publishing applications for users. When we assign an application to a user, the application is advertised to the user the next time the user logs on to the network regardless of which computer the user actually uses to log on. The application is installed the first time the user activates the application on the computer, either by selecting the short cut to application on the start menu or by activating a document associated with the application. When we assign an application to a computer, the application is advertised and is installed when there are no other applications running on the computer. This usually occurs when the computer next starts up. When we publish an application to a user, the application does not appear installed on the users' computers and no shortcut to it is visible on the desktop or the start menu. Instead, the application is available for the user to install using Add/Remove Programs in Control Panel or by clicking a file associated with the application. We cannot publish an application to a computer.

Incorrect Answers:
A: We cannot use an .inf template to install an application.
C: We should assign, not publish the application for Phase 1.
D: We cannot use a .inf template to install an application.
E: For Phase II we must change the way the application is deployed. For Phase 1 it should be assigned but for Phase II it should be published.

QUESTION 95
You are the administrator of your company's network. The company has two native-mode domains in six sites as shown in the exhibit.

Each site has one or more Domain Controllers. Users report that at times of high network usage authentication and directory searches are extremely slow.

You want to improve network performance. What should you do?

Exhibit:

A. Move all Domain Controllers into one site.
B. Promote more Windows 2000 server computers in each site to be Domain Controllers.
C. Install a DNS server in each site and configure it to use Active Directory integration.
D. Designate a Domain Controller in only one site as a Global Catalog server.
E. Designate a Domain Controller in each site as a Global Catalog server.

Answer: E
Section: (none)

Explanation/Reference:
Explanation: With Windows 2000, we require a Global Catalog for logon purposes on a domain that runs in native mode. One Global Catalog should be placed in each site for improved logon time. The Global Catalog server answers Active Directory Search queries and must be present to allow clients to successfully logon as it holds a copy of all Objects of the whole Forest although it only holds only a subset of the Attributes.

There should be at least one Global Catalog server in a large Site.

Incorrect Answers:
A: Moving all Domain Controllers into one site would result in all logon traffic having to pass over the links. This would increase network traffic and reduce logon performance.
B: A Global Catalog is required for logon purposes on a domain that runs in native mode, not just a Domain Controller.
C: DNS will not improve logon times; therefore it is not necessary to install a DNS server in each site and configure it to use Active Directory integration.
D: One Global Catalog should be placed in each site for improved logon time.

QUESTION 96
Your company's network consists of a single Windows 2000 domain. You are the administrator for an organizational unit named Sales. Four Group Policy Objects are linked to the Sales OU. Each GPO is shown in the exhibit.

The East Remove Run GPO contains a policy that removes the Run command from the Start menu. This GPO affects only the users in the Eastern region.

The All Users: Enable Display & Distribute Software GPO contains a policy that enables Display in Control Panel. This GPO affects all users in the Sales department.

The West Disable Display & Remove Run Group Policy Object contains a policy that removes the Run command from the Start menu and a policy that disables Display in Control Panel. This GPO affects only the users in the Western region.

You discover that users in the Western region are making unauthorized changes to their desktop settings by using Display in Control Panel. You need to ensure that users in the Sales OU cannot access Display in Control Panel.

What should you do?

Exhibit:

A. Set the West Disable Display & Remove Run GPO to **No override.**
B. Set the All Users Enable Display & Distribute Software GPO to **Block Inheritance.**
C. Raise the priority of the All Users Enable Display & Distribute Software GPO
D. Lower the priority of the All Users Enable Display & Distribute Software GPO

Answer: D
Section: (none)

Explanation/Reference:
Explanation: In this scenario the Enable Display GPO is overwriting the Disable Display GPO. We need to lower the priority of the Enable Display GPO so that the Disable Display GPO can overwrite it for the west users.

Incorrect Answers:
A: Setting the West Disable Display & Remove Run GPO to **No override** will remove the run command for all users.
B: Setting the All Users Enable Display & Distribute Software GPO to **Block Inheritance** will not prevent the Disable Display GPO being overwritten for West users and would allow them to change their display settings.
C: Raising the priority of the All Users Enable Display & Distribute Software GPO will not prevent the Disable Display GPO being overwritten for West users and would allow them to change their display settings.

QUESTION 97
You are the administrator of your company's network. A vendor provides you with an application and four transform files. You need to deploy the application to employees in the Sales department.

You deploy the application and the transform files. After the deployment is complete, you test the application and discover that the second transform file is unnecessary.

You want to deploy the application so that it includes only the first, third, and fourth transform files. You need to complete this task by using the least amount of administrative effort. What should you do?

A. In the application properties, remove all transform files, and then add the required transform files in order.
B. In the application properties, remove the second transform file.
   Use the Move Up and Move Down buttons to order the files.
C. Remove the package definition from Group Policy.
   Create a new definition for the package.
   Add the required transform files in order.
D. Remove the package definition from Group Policy.
   Copy the required transform files to the package source in order.
   Create a new definition for the package.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: Modifications are associated with the Windows Installer package at deployment time rather than when the Windows Installer is actually using the package to install or modify the application. Modifications (. mst files) are applied to Windows Installer packages (which have the .msi extension) in an order specified by the administrator. This order must be determined before the application is assigned or published.

If the modifications are not properly configured we will have to uninstall the package or upgrade the package with a correctly configured version. Furthermore, the transformation, or modifications of deployment packages cannot be undone. We have to remove the package and create a new package definition and then apply the transformations in the correct order.

Incorrect Answers:
A: The whole package, not only the transform files, has to be removed.
B: We cannot remove the transform files and the order of transform files cannot be changed. We have to remove the package and create a new package definition and then apply the transformations in the correct order.
D: The proper order for undoing the changes is to remove old package, create new definition of package, and add transforms in the correct order. After removing the old package we cannot start copying the transform files. The transform files should be applied not copied.

QUESTION 98
You are a member of the Enterprise Admins group in your company's Windows 2000 network. The network consists of a single domain. The organizational unit (OU) structure of the domain is configured as shown in the exhibit.

To improve security, only members of the Finance Admins and Audit Admins groups should have permission to log on to servers in the Audit OU. Similarly, only members of the Corp Admins and Finance Admins groups should have permission to log on to servers in the Finance OU. Only members of the Corp Admins group should be able to log on to servers in the Servers OU. Some members of the Corp Admins group are also members of the Audit Admins and Finance Admins groups.

You create a new Group Policy Object for the Servers OU, and assign the Corp Admins group the Log on locally user right in the GPO. You create a new GPO for the Finance OU named Financeservers. You create a new GPO for the Audit OU named AuditServers

You need to complete the implementation of the security policy. What should you do?

Exhibit:

A. In the FinanceServers GPO, assign Finance Admins the Log on locally user right.
In the AuditServers GPO, assign Audit Admins the Log on locally user right.

B. In the FinanceServers GPO, assign Finance Admins the Log on locally user right.
In the AuditServers GPO, assign Audit Admins the Log on locally user right and assign Corp Admins the Deny logon locally user right.

C. In the FinanceServers GPO, assign Corp Admins and Finance Admins the Log on locally user right.
In the AuditServers GPO, assign Finance Admins and Audit Admins the Log on locally user right.

D. In the FinanceServers GPO, assign Corp Admins and Audit Admins the Log on locally user right.
In the AuditServersGPO, assign Corp Finance Admins and Audit Admins the Log on locally user right and assign Corp Admins the Deny logon locally user right.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: In this scenario there are three OUs that must be configured so that different groups have to

right to log on locally on the servers on this domain. On the Server OU the Corp Admins should have the right to log on locally. However, a new GPO, where the Corp Admins group has been assigned to right to log on locally, has already been created for the Server OU. Therefore this requirement is already fulfilled. On the Finance OU both the Corp Admins and Finance Admins group should be able to log on locally. Therefore the FinanceServers GPO must assign both the Corp Admins and the Finance Admins groups the right to log on locally. Finally, on the Audit OU the Finance Admins and the Audit Admins should have the right to log on locally. Therefore the AuditServers GPO must assign the Audit Admins and the Finance Admins the rights to log on locally.

Incorrect Answers:
A: The Corp Admins group must have the right to log on locally on the servers in the Finance OU.
B: The Corp Admins group must have the right to log on locally on the servers in the Finance OU. Corp Admins that are members of the Audit Admins must be allowed access to servers in the audit OU. But they are denied access to them.
D: The Audit Admins should not have access to the servers in the Finance OU. Corp Admins which are members of the Finance Admins group must be able to access servers in the Finance OU, but they are denied access.

QUESTION 99
You are the administrator of your company's Windows 2000 network. The network consists of a single Active Directory site named Default-First-Site-Name. The site contains one domain controller named DC1.

On a Windows 2000 computer named Server1, you install an application that uses Active Directory frequently. After the installation, users report that network performance is slow when they try to access shared folders on DC1.

You use a high-performance router to separate the network into two segments. Then, you add a domain controller named DC2 to the new segment. The network is now configured as shown in the exhibit.

Users report that network performance between the segments is still occasionally slow. You need to improve network performance.

What should you do?

Exhibit:

A. Configure both domain controllers to be global catalog servers.
B. Configure the router to block LDAP traffic between the segments.
C. Create a new Active Directory site for each segment.
D. Create a new Active Directory subnet for Segment B, and associate the subnet with the existing Active Directory site.

Answer: A

Section: (none)

Explanation/Reference:
Explanation: The application on Server1 uses the Active Directory frequently. In order the reduce the network traffic between Segment A and Segment B we should therefore configure both domain controllers as global catalog servers. The application on Server1 could use the global catalog server in segment B to access resources in the Active Directory without any, or at least very little, communication between the segments.

Incorrect Answers:
B: Blocking all LDAP traffic at the router would reduce network traffic, but it would also prevent Active Directory traffic between the segments. In particular the application on Server1 would not be able to run.
C: It might seem like a good idea to create a site for each network segment, and it would probably be the next thing to be done after configuring the domain controllers as global catalog servers. In this scenario, however, the application on Server1 uses Active Directory frequently. The application would have to access DC1 in the other segment. This traffic would not be reduced by creating sites.
D: Creating a new subnet for segment B and associating it with a new site for segment B could be a good idea. However, associating the new subnet with the existing site would not improve performance, since it would not change the current configuration.

QUESTION 100
You are the administrator of your company's Windows 2000 network. The network consists of a four Active Directory sites. The option to bridge all site links is enabled and has not been changed from the default installation setting. The site link configuration is shown in the exhibit.

Directory replication traffic from London to Los Angeles must take place through Atlanta. Directory replication from New York to Los Angeles must take place directly with Los Angeles. You want to reconfigure site link costs to support these requirements.

Which costs should you reassign to site links A and E?

Exhibit:

A. A=76, E=68
B. A=32, E=36
C. A=26, E=25

D. A=22, E=27

Answer: C
Section: (none)

Explanation/Reference:
Explanation: This solution gives B + E =75 and A + D =76. B-E will the preferred path and replication will go through Atlanta.

Note: In replication we can configure which site links to use by specifying site link costs. Replication would then occur across the site links with the lowest cost. In this scenario the sum of the cost of site link E and site link B must be lower than the sum of the cost of site link D and site link E and the cost of site link A must be lower than the sum of the cost of site link C and site link B. This would result in replication between Los Angeles and London passing through the site link that joins these two sites to Atlanta. Hence replication between Los Angeles and London would pass through Atlanta rather than New York.

Incorrect Answers:
A: The site link costs specified in this solution would cause the replication between New York and Los Angeles to pass through Atlanta. B+E=118 and A+D=116. A-D will be the preferred path for replication.
B: The site link costs specified in this solution would cause the London to Los Angeles replication to pass through New York. B+E=86 and A+D=82. A-D will be the preferred path for replication.
D: The site link costs specified in this solution would cause the London to Los Angeles replication to pass through either New York or Los Angeles. B+E=77 and A+D=77. Both paths will be used for replications.

QUESTION 101
You install a Windows 2000 Server computer on your network. You promote the computer to be a Domain Controller. This computer also functions as the DNS server for the domain. All client computers are running Windows 2000 Professional.

When users attempt to logon, they receive an error message stating that a Domain Controller cannot be located. You verify that Active Directory is installed and functional on the server.

You want to ensure that the Domain Controller is available for user logons. What should you do next?

A. Check DNS for the addition of an appropriate SRV (service) record in the zone.
B. Check DNS for the addition of an appropriate A (host) record in the zone.
C. Check for the presence of an NTDS folder on the Domain Controller.
D. Check for the presence of a Sysvol folder on the Domain Controller.
E. On the client computers, create a Hosts file that contains the SRV (service) records for the Domain Controller.
F. On the client computers, create a Hosts file that contains the A (host) record for the Domain Controller.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: The DNS requires SRV records so that the clients can find the Active Directory Servers, specifically to find Domain Controllers during the logon process.

Incorrect Answers:
B: This would enable clients to resolve host names but we need SRV records so that the clients know which machines are Domain Controllers.
C: Ensuring that the DNS has the addition of an appropriate A (host) record in the zone would result in the DNS holding records for the Active Directory. It would not enable clients to find the Domain Controllers.

D: The sysvol folder is used for replication. It would not enable clients to find Domain Controllers.
E: Hosts files cannot contain SRV records.
F: Creating a Hosts file that contains the A (host) record for the Domain Controller on the client computers would enable clients to resolve host names. However, we require SRV records so that the clients know which machines are Domain Controllers.

QUESTION 102
You are the enterprise administrator of a Windows 2000 domain named fabrikam.com. The domain contains three Domain Controllers named DCA, DCB, and DCC. DCA does not hold any operations master roles. You backed up the System state data of DCA two weeks ago.

Without warning, the DCA hard disk fails. You decide to replace DCA with a new computer. You install a new Windows 2000 computer.

What should you do next?

A. Add the server to the domain.
   Do an authoritative restore of the original backup of the original DCA System State data that you made two weeks ago.
B. Add the server to the domain.
   Use Windows Backup to create a backup of the DCB System State data, and restore this backup on the new DCA.
C. Use the Active Directory installation wizard to make the new computer a replica in the domain.
D. Use the Ntdsutil utility to copy the Active Directory database from DCB to the new DCA.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: When a Domain Controller that has no Operation Master roles fails, it can be restored to a new computer by using the Active Directory installation wizard to make the new computer a replica in the domain. No further action is required, as the Domain Controller had no Operation Master roles.

Incorrect Answers:
A: The original Domain Controller had no Operation Master roles therefore we do not need to perform any restore from the previous backup. We could simply set the Domain Controller to be a replica in the domain.
B: We cannot restore system state data to different computer.
D: It is not necessary to manually copy the Active Directory database from another Domain Controller to the new computer, as this will occur automatically during the installation of Active Directory.

QUESTION 103
You are the administrator of your company's network. Your company has its main office in Seattle and branch offices in London, Paris, and Rio de Janeiro. The local administrator at each branch office must be able to control users and local resources. You want to prevent the local administrators from controlling resources in branch offices other than their own.

You want to create an Active Directory structure to accomplish these goals. What should you do?

A. Create a top-level organizational unit (OU). Delegate control of this OU to administrators at the main office.
B. Create child OUs for each office. Delegate control of these OUs to administrators at the main office.
C. Create child OUs for each office. Delegate control of each OU to the local administrators at each office.
D. Add the local administrators to the Domain Admins group.

E. Create users groups for each office. Grant the local administrators the appropriate permissions to administer these user groups.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: One of the main purposes of OUs in Windows 2000 is the delegation of control.

Incorrect Answers:
A: Creating a top-level organizational unit (OU) and delegating control of this OU to administrators at the main office will not give local Admins control of their resources.
B: Creating child OUs for each office and delegating control of these OUs to administrators at the main office will not give local Admins control of their resources but will give control to Admins at the main office.
D: Adding the local administrators to the Domain Admins group will give the Domain Admins group control over the whole domain.
E: Creating users groups for each office and granting the local administrators the appropriate permissions to administer these user groups would only allow the local administrators to manage users and user accounts.

QUESTION 104
Your company's Windows 2000 network consists of a single domain. You are the enterprise administrator of the domain. Two administrators named Ann and Bill make changes to Active directory at approximately the same time at two different Domain Controllers named ServerA and ServerB.

Ann deletes an empty OU named Branch1 from ServerA. Before this deletion is replicated to ServerB, Bill move five existing users from the Branch2 OU to the Branch1 OU at ServerB. Ten minutes later, Bill discovers that the Branch1 OU is deleted from Active Directory.

You want to reinstate the configuration that Bill attempted to accomplish. What should you do?

A. Perform an authoritative restore of the Branch1 OU at ServerA.
B. Perform a nonauthoritative restore of the Branch1 OU at ServerA.
C. Perform an authoritative restore of the five users at ServerB.
D. At ServerB, move the Branch1 OU from the LostAndFound container to its original location.
E. At ServerA, create a new Branch1 OU. Move the five users from the Branch2 OU to the new Branch1 OU.
F. At ServerB, create a new Branch1 OU. Move the five users from the LostAndFound container to the new Branch1 OU.

Answer: F
Section: (none)

Explanation/Reference:
Explanation: During a move process, objects that are not moved are classified as orphaned objects and are placed in an "orphan" container in the LostAndFound container in the source domain. In this scenario the users are in the lost and found container. They need to be moved to the new OU.

Incorrect Answers:
A: During a move process, objects that are not moved are classified as orphaned objects and are placed in an "orphan" container in the LostAndFound container in the source domain.
B: During a move process, objects that are not moved are classified as orphaned objects and are placed in an "orphan" container in the LostAndFound container in the source domain.
C: During a move process, objects that are not moved are classified as orphaned objects and are placed in an "orphan" container in the LostAndFound container in the source domain. These users should be put back in the lostandfound container because there is no OU for them.

D: During a move process, objects that are not moved are classified as orphaned objects and are placed in an "orphan" container in the LostAndFound container in the source domain. The OU has been deleted and would therefore not be in the lostandfound container.
E: The users are not in the branch2 OU. They have been moved to the lostandfound container.

QUESTION 105
You are the administrator for Arbor Shoes. Part of your network configuration is shown in the exhibit.

All the computers are running Windows 2000 Professional and are members of the arborshoes.com domain in the company LAN. All the users are members of the Power Users group on their computers. Andrew has dial-up access to the Internet for a special project he is working on. You do not want other users to share Andrew's Internet connection and to have unrestricted Internet Access.

What should you do?

Exhibit:

A. Create a high security zone in MICROSOFT Internet Explorer.
B. Create a Group Policy Object that disables the configuration of connection sharing. Grant Andrew Read and Apply Group Policy permissions to the GPO.
C. Create a Group Policy Object that disables the configuration of connection sharing. Grant Michel, Laura, and Anita Read and Apply Group Policy permissions to the GPO.

D. Remove the Internet connection from the All Users profile on Andrew's computer, and then re-create the connection in Andrew's personal profile.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: To prevent Andrew from sharing his Internet connection we should create a Group Policy Object that disables the configuration of connection sharing and grant Andrew Read and Apply Group Policy permissions to this GPO. This will prevent Andrew from sharing his internet connection.

Incorrect Answers:
A: The security zone settings in Microsoft Internet Explorer are not related to internet connection sharing and are thus not relevant to this problem.
C: To prevent Andrew from sharing his Internet connection we should create a Group Policy Object that disables the configuration of connection sharing and grant Andrew Read and Apply group Policy permissions to this GPO. We do not have to grant Michel, Laura, and Anita Read and Apply group Policy permissions to the GPO as only Andrew has an internet connection.
D: Removing the Internet connection from the All Users profile on Andrew's computer, and then recreating the connection in Andrew's personal Profile will not stop Andrew sharing his connection.

QUESTION 106
You are using RIS to deploy Windows 2000 Professional on 1,500 computers. Your network configuration is shown in the exhibit:

You have four RIS servers. You have deployed 100 computers. RIS server1 and RIS server3 are overworked and respond too slowly for the timely deployment of you are computers. You need more consistent performance results before you deploy the remaining computers.

What should you do?

Exhibit:

A. Create computer accounts for all the computers. Complete the **Managed by** property for each account.
B. Create one OU for each segment. Add user accounts for all the users to the appropriate OUs. Specify the appropriate RIS server in the **Log on to** property for each user's account.
C. Create prestaged computer accounts for all the computers. Specify which RIS server will control each computer.
D. Create one site for each segment. Move two RIS servers to each site.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: When using multiple RIS servers we can create load balancing by creating prestaged computer accounts for all the computers that the software must be deployed on and specify which RIS server will control each computer.

Incorrect Answers:
A: In Windows 2000 the computer accounts do not have a **Managed by** property.
B: When using a RIS server to deploy software we do not require users to logon to the RIS server.
D: By creating one site for each segment and moving two RIS servers to each site we will not ensure load balancing between the two RIS servers.

QUESTION 107
You are the network administrator for Just Togs. Your Windows 2000 network consists of 15,000 users. Users have recently reported that documents are missing from the servers. You need to track the actions of the users to find out who has been deleting the files. You create a GPO on the justtogs.com domain and assign the appropriate permissions to the GPO.

What actions should you audit? (Choose two)

A. Object access.
B. Process tracking.
C. Privilege use.
D. Delete and Delete subfolders and files.
E. Directory Services access.

Answer: AD
Section: (none)

Explanation/Reference:
Explanation: Object access refers to the accessing of network resources such as files and printers. Thus, by auditing object access we could track who is accessing which network resources. In this scenario we should audit the deletion of files or folders.

Incorrect Answers:
B: Object access refers to the accessing of network resources such as files and printers. Thus, by auditing object access we could track who is accessing which network resources. We cannot use process auditing to track network resource access.
C: Object access refers to the accessing of network resources such as files and printers. Thus, by auditing object access we could track who is accessing which network resources. We cannot use Privilege use to track network resource access.
E: Directory Services access is for the auditing of Active Directory objects, not files or folders. Object access refers to the accessing of network resources such as files and printers. Thus, by auditing object access we could track who is accessing which network resources.

QUESTION 108
You are administrator of a Windows 2000 domain. The domain has an OU named Trading. You define a logon script for all the users in the Trading OU. The logon script is located at \\server2\docs\tradescript.vbs.

You want to use a Group Policy Object to assign the logon script to the users in the Trading OU. What should you do? (Choose three)

A. Create a new GPO named script and assign the script GPO to the Trading OU.
B. Create a new GPO named script and assign the script GPO to the domain. Configure the permissions on the script GPO to grant Read permissions to all users in the Trading OU.
C. Copy the tradescript.vbs file to the appropriate folder in the Group Policy Template (GPT) of the script GPO.
D. Copy the tradescript.vbs file to the folder that is shared as Netlogon on the PDC emulator.
E. For each user in the Trading OU, set the logon script in the user Profile to tradescript.vbs.
F. Add tradescript.vbs as a logon script to the script GPO.

Answer: ACF
Section: (none)

Explanation/Reference:
Explanation: The Group Policy Template is a folder structure in the %systemroot%\SYSVOL\sysvol\<domain_name>\Policies folder of Domain Controllers. The GPT is the container where policy settings for administrative templates, security settings, script files, and software settings are stored. In this scenario we need to create a GPO and add the script to the GPO. When we add a script to a GPO, a folder will open for us to put the script in. We must then assign the GPO to the OU.

Incorrect Answers:
B: The GPO should be assigned to the OU and not to the domain.
D: The folder that is shared as Netlogon is not the correct folder to place the Group Policy Template in. We should place the Group Policy Template in the %systemroot%\SYSVOL\sysvol\ <domain_name>\Policies folder of Domain Controllers.
E: It is not necessary to set the logon script in the user profile to tradescript.vbs for each user in the Trading OU as we could perform the same function through the use of a GPO.

QUESTION 109
You are the administrator of a Windows 2000 network. You are deploying Windows 2000 Professional to 200 client computers. A custom configuration is required for each one of 50 of the client computers.

You are using Microsoft Systems Management Server to install various applications on all of the client computers. You want to use RIS to install Windows 2000 on all of the client computers.

What should you do?

A. Create a CD-based RIS image with different answer files for each custom configuration.
B. Create a RIPrep image for each configuration. Grant Read & Execute permission to users for the image folder.
C. Install a test client computer for each custom configuration. Use the Setup Manager wizard to create an answer file for each configuration.
D. Use the Setup Manager wizard to create a Sysprep answer file. Use third-party imaging software to create a separate image for each configuration.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: We only need the Windows 2000 source files because we are using Microsoft Systems Management Server to deploy the applications. We can also create different answer files for each configuration.

Incorrect Answers:
B: We do not need a RIS image as we are using Microsoft Systems Management Server to deploy the applications, we only need the Windows 2000 source files.
C: Installing a test client computer for each custom configuration would increase administrative overhead, as it would involve manually installing the computers.
D: We are not using Sysprep therefore we should not create a Sysprep answer file. We're using RIS.

QUESTION 110
You are the administrator of a Windows 2000 domain named arborshoes.com. You install RIS on the server. You are using RIS to install 35 new client computers.

When you start a test client computer, the Client Installation wizard does not appear. You are using network adapter cards that are not PXE compliant. You want to connect to the RIS server.

What should you do next?

A. From a command prompt, run Rbfg.exe to create RIS a boot disk.
B. Identify the GUID of each client computer.
C. Set up a DHCP Relay Agent.

D. Install Windows 2000 on the test client computer. Run RIPrep.exe from a network share on the RIS server.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: When deploying software to clients with Non-PXE compliant network cards, the clients must be provided with a RIS boot disk to be able to connect to the RIS server, as clients with Non-PXE compliant network cards cannot be booted over the network. A boot disk can be created by using the RBFG.EXE utility.

Incorrect Answers:
B: Identifying the GUID of each client computer would not solve the problem in this scenario, as the clients with the Non-PXE compliant network cards cannot connect to the RIS server.
C: A DHCP Relay Agent not needed in this scenario. A DHCP Relay Agent is required for routed networks. Clients with Non-PXE compliant network cards are not be able to connect to the RIS server.
D: Installing Windows 2000 on the test client computer and running RIPrep.exe from a network share on the RIS server would result in the creation of a RIS image. The problem in this scenario is that the clients with Non-PXE compliant network cards are not be able to connect to the RIS server.

QUESTION 111
You are the administrator of a Windows 2000 domain. To control the desktop environment of users in the domain, you use a script file named Desktop.vbs to change settings in the current user profiles. This script file is deployed as a login script for all users in the domain.

The Desktop.vbs script usually takes 15 seconds to complete its work. You want to ensure that each user's desktop appears only after the Desktop.vbs script is completed.

What should you do?

A. For all users in the domain, set the logon script in the user profile to Desktop.vbs.
B. Create a new Group Policy Object. Assign the GPO to the domain. Add Desktop.vbs to the GPO as a logon script. Configure the GPO to run logon scripts synchronously.
C. Create a new Group Policy Object. Assign the GPO to the domain. Add Desktop.vbs to the GPO as a logon script. Configure the GPO to set a maximum wait time of 15 seconds for Group Policy scripts.
D. Create a new Group Policy Object. Assign the GPO to the domain. Add Desktop.vbs to the GPO as a logon script. Configure the GPO to set a timeout of 15 seconds for logon dialog boxes.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: To ensure that each user's desktop appears only after the Desktop.vbs script is completed we must create new GPO, add the Desktop.vbs file to the GPO as a login script and assign the GPO to the domain. This will ensure that the policy is applied to all users. We must then configure the GPO to run scripts synchronously to specify that all scripts must be finished before Windows Explorer starts and the Desktop appears.

Incorrect Answers:
A: Setting the logon script in the user profile to Desktop.vbs for all users in the domain would be a daunting administrative task. Furthermore, if the logon script is not run synchronously the Desktop could be shown before the script has finished.
C: By setting maximum wait time of 15 seconds for Group Policy scripts, if a logon script takes longer than 15 seconds the Desktop will be shown, even though the logon script has finished running. We must however ensure that the Desktop only appears after the Desktop.vbs script is complete.
D: Timeout settings are used for logoff and shutdown scripts not for logon scripts.

QUESTION 112
You are the administrator of a Windows 2000 domain. The domain has 20 users and a Windows 2000 Server computer named Glasgow. Users in the domain frequently work on different Windows 2000 Professional computers. All Windows 2000 Professional computers are in the domain.

You want to accomplish the following goals:

- All users in the domain will be able to work on all Windows 2000 Professional Computers and have their own predefined desktop settings available on all computers.
- Users will be allowed to make changes to the desktop settings while they are logged on.
- Changes that users make to the desktop settings will not be saved when they log off.

What should you do?

A. One each Windows 2000 Professional Computer, delete the Systemdrive\Documents and Settings\Default User folder.
B. On each Windows 2000 Professional Computer, rename the Systemroot\System32\Config\System file to System.man.
C. Configure a roaming profile for each user in the domain. Use \\Glasgow\Profiles\%username% as the profile path. On the Glasgow server, rename the Ntuser.dat file to Ntuser.man for each user.
D. Create a Group Policy Object named DelProfile. Assign the DelProfile GPO to the domain. Configure the DelProfile GPO to delete the local copy of a user's profile when the user logs off.
E. Create a Group Policy Object named GetProfile. Assign the GetProfile GPO to the domain. Configure the GetProfile GPO to wait for the remote copy of a user profile to load.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: With roaming profiles the users' settings can be used wherever they log on. With mandatory profiles, which are created by renaming the Ntuser.dat file to Ntuser.man, users can change settings while they are logged on to the network; however, the changes are not saved when the user logs off.

Incorrect Answers:
A: By deleting the Systemdrive\Documents and Settings\Default User folder we would delete all profiles.
B: Mandatory profiles are created by renaming the Ntuser.dat file to Ntuser.man. They are not created by renaming the system file.
D: The roaming profiles are stored on a network server and not on the local computer. Therefore configuring a GPO to delete the local copy of a user's profile when the user logs off would not affect the roaming profile. It is however not necessary to delete the local copy of the roaming profile when the user logs off as we can set the profile to a mandatory profile, meaning that the changes made by a user to their desktop settings are not saved when the user logs off.
E: We must create roaming profiles, as they are required by users who logon to the network from different locations or computers but who require the same desktop setting regardless of where they logon. In this scenario the roaming profiles have not been configured.

QUESTION 113
You are installing a new Windows 2000 Server computer on your existing Windows NT network. You run DCPromo.exe to promote the server to a Domain Controller in a domain named domain.local. You receive the following error message: "The domain name specified is already in use on the network". There are no other Windows 2000 domains on your network.

What should you do?

A. Place an entry in your DNS server host table for the domain.local domain name.
B. Place an entry in your WINS database for the domain.local domain name.
C. Change the domain name to domain.com.
D. Change the down level domain name to domain1.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: The default NetBIOS domain name is DOMAIN. The Windows NT domain is using this domain name therefore we need to change the NetBIOS domain name during the DCPromo process.

QUESTION 114
You are the enterprise administrator of a Windows 2000 domain. The domain is in native mode. You want to implement a policy to disable the ShutDown command for all users in the domain except for the members of the Domain Admins security group.

You create a new Group Policy object (GPO) named Shutdown. You configure the Shutdown GPO to disable the Shutdown option. You assign the Shutdown GPO to the domain.

You want to ensure that the policy does not apply to the members of the Domain Admins group. What should you do?

A. On the Shutdown GPO, deny the Apply Group Policy permission to the Domain Admins group.
B. On the Shutdown GPO, remove the Apply Group Policy permission from the Authenticated Users group. Grant the Apply Group Policy permission to the Users group.
C. Add the Domain Admins group to the Group Policy Creator Owners group.
D. Create a new OU named No Shutdown.
Move the Domain Admins group to the No Shutdown OU.
Configure the No Shutdown OU to block policy inheritance.
E. On the computers that the members of the Domain Admins group use to log on, configure the local GPO to enable the Shutdown option.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Users and groups must be granted the Read and Apply Group Policy permissions for a policy configured in a GPO to be implemented. Therefore, to ensure that a policy configured in a GPO is not applied to a particular user or group, we can deny the user or group the Apply Group Policy (or Read) permission. The deny permission would override all other permissions the user or members of a group might have been granted in other contexts, i.e. as members of other groups. In this scenario

Incorrect Answers:
B: The members of the Domain Admins group are also members of the users group; therefore the policy would be applied to them as well.
C: The application of the policy is independent of the owner of the policy but is dependent on the user being granted Read and Apply Group Policy permissions.
D: We can ensure that that a policy configured in a GPO is not applied to the Domain Admins group by placing them in an OU and configuring the OU to block policy inheritance. It would however require less administrative effort to deny the Domain Admins group the Apply Group Policy permissions.
E: The domain GPOs are processed after the local GPO has been processed; therefore the domain GPOs would override the local GPO.

QUESTION 115
You are deploying Windows 2000 Professional on your network of 1,000 users. Part of your network is shown in the exhibit.

You have recently installed an RIS server to assist in the deployment process. You confirm that the client computers meet the requirements for RIS deployment. However, you still cannot connect the RIS client computers to the RIS server. Existing client computers are able to connect to all servers for network resources.

What can be causing the problem? (Choose all that apply.)

Exhibit:

A. The RIS server has no client-side tools installed.
B. The RIS server is not trusted for delegation.
C. The RIS server is not authorized in Active Directory.
D. The client computers are not configured to use DHCP.
E. The RIS server is not configured to respond to client computers requesting service.

Answer: CE
Section: (none)

Explanation/Reference:
Explanation: To connect the RIS client computers to the RIS server, the RIS server must be authorized in Active Directory and must be configured to respond to client computers. This will enable the RIS server to respond to client requests.

Incorrect Answers:
A: Windows 2000 does not support client-side tools on the RIS server. For the RIS server to respond to client requests it must be configured to do so and must be authorized in Active Directory.
B: In Windows 2000 a RIS server does not need to be trusted for delegation.
D: It is possible that the client computers are not configured to use DHCP and therefore are not receiving IP addresses from the DHCP. Should this be the case the clients would be use Auto Private IP Addressing, which would enable them to communicate within the subnet that they are on. The clients would then not be able to communicate across the default gateway. As no clients have complained about lack of connectivity across the default gateway, we can assume that the problem lies elsewhere.

QUESTION 116
You are the administrator of your company's network. The network consists of two Windows 2000 domains named contoso.com and mktg.contoso.com. You create separate zones for each domain on your DNS server. Later, you add a second DNS server to the network. This server also functions as a Domain Controller. You convert the contoso.com zone to an Active Directory integrated zone and set the zone to allow only secure updates to the zone database.

You discover that unauthorized computers are registering themselves in the mktg.contoso.com domain. You check the zone's properties and discover that the zone is allowing unsecured dynamic updates. You also discover that the option to select secure dynamic updates is not available.

What should you do to correct this problem?

A. Initiate a zone transfer between the mktg.contoso.com zone and the contoso.com zone.
B. Reinstall mktg.contoso.com as a standard secondary zone.
C. Reinstall contoso.com as a standard primary zone.
D. Convert mktg.contoso.com to an Active Directory integrated zone.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: Windows 2000 only supports secure dynamic updates on Active Directory integrated zones. Therefore we must ensure that all the zones are Active Directory integrated zones.

Incorrect Answers:
A: Initiating a zone transfer between the mktg.contoso.com zone and the contoso.com zone will not ensure that only secure updates are made to the zone database.
B: A Windows 2000 domain requires a primary zone we should therefore not reinstall mktg.contoso.com as a standard secondary zone.
C: Contoso.com is a standard primary zone therefore it is not necessary to reinstall it as a primary zone.

QUESTION 117
You are the network administrator for Enchantment Lakes Corporation. Enchantment Lakes Corporation and Five Lakes Publishing are planning a merger.

The planned Windows 2000 network configuration is shown in the exhibit.

You want to host the fivelakespublishing.com domain on the enchantmentlakes.com DNS server. The fivelakespublishing.com domain uses an Active Directory integrated zone on its DNS server. FiveLakesPublishing will retain its domain structure after the merger is complete.

You want to set up the enchantmentlakes.com DNS server to host the fivelakespublishing.com domain.

What should you do?

Exhibit:

A. On Server1, create an Active Directory integrated zone named fivelakespublishing.com.
Enable WINS lookup, and specify Server7 as the IP address for the WINS server.
B. On Server5, create a secondary zone named fivelakespublishing.com.
Configure DNS zone transfers to allow Server1 to replicate data.
C. On Server5, configure DNS zone transfers to allow Server1 to replicate data.
On Server1, create a secondary zone named fivelakespublishing.com.
D. On Server1, create an Active Directory integrated zone named fivelakespublishing.com.
Configure DNS zone transfers to allow Server5 to replicate data.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: In this scenario we need to create a secondary zone on server1 so that it can pull zone files from server5. Server5 has to be configured to allow server1 to pull the zone files from it.

Incorrect Answers:
A: Windows 2000 does not support replication between two primary zones as Active Directory integrated zones are primary zones. This would result in the replication between two Active Directory integrated zones.
B: We need the data to be copied from server5 to server1. In Windows 2000 replication occurs from the primary zone to the secondary zone therefore server5 must be configured as the primary zone and server1 as the secondary zone.
D: Windows 2000 does not support replication between two primary zones as Active Directory integrated zones are primary zones. This would result in the replication between two Active Directory integrated zones.

QUESTION 118
You create a new Windows 2000 Active Directory network. Five months after deployment of the network, you receive a report that the Active Directory database file takes too much disk space on the ServerA Domain Controller. You want to reduce the size of the Active Directory database file.

What should you do? (Choose three.)

A. Restart ServerA in directory services restore mode.
B. Stop the Net Logon service on ServerA.
C. Run Windows Backup to back up the System State data.
Immediately run Windows Backup again to restore the System State data from the backup file.
D. Use the Ntdsutil utility to compact the database to a folder.
Move the compacted database file to the original location.
E. Restart ServerA and boot normally.
F. Start the Net Logon service on ServerA.

Answer: ADE
Section: (none)

Explanation/Reference:
Explanation: To reduce the size of the Active Directory database file we must use the Ntdsutil command-line utility, which is run in Directory Services Restore mode. This utility can be used to compress the Active Directory database. We can enter Directory Services Restore mode by pressing F8 to display the Windows 2000 Advanced options menu. We must the logon using the Administrators account and type NTDSUTIL at the command prompt, specify files, then type 'COMPACT TO C:\TEMP'. We must then move the compressed Active Directory database file, the NTDS.DIT file, from the C:\temp folder to the location of the original NTDS.DIT file and allow the new file to overwrite the existing file. The existing NTDS.DIT file is usually located in the

C:\WINNT\system32 folder. Finally, we must restart the computer and boot normally for the changes to take effect.

Incorrect Answers:
B: To reduce the size of the Active Directory database file we must use the Ntdsutil command-line utility, which is run in Directory Services Restore mode. Stopping the netlogon service will not reduce the size of the Active Directory database file.
C: Backing up and restoring the System State Data will not reduce the size of the Active Directory database file.
F: The NetLogon service will start automatically when we boot the computer normally.

QUESTION 119
You are the administrator of a Windows 2000 network. The network is composed of four domains named arborshoes.com, na.arborshoes.com, sa.arborshoes.com, and fabrikam.com. The root of the forest is arborshoes.com. There are two Windows NT BDCs in each domain.

Graphic artists place finished artwork for Fabrikam, Inc. in a shared folder located on a Domain Controller named bna01.fabrikam.com. Read and Write permissions are granted to the Artists Domain Local group in the fabrikam.com domain.

Sharon is a member of the Graphic Artists global distribution group in the na.arborshoes.com domain. She is unable to gain access to the shared folder.

You want to allow Sharon access to the shared folder. What should you do?

A. Change the Graphic Artists group type to Security and add it to the Artists Domain Local group.
B. Change the Artists Domain Local group to a universal group and add it to the Graphic Artists group.
C. Change the Graphic Artists group to a Domain Local group and add it to the Artists Domain Local group.
D. Change the mode of the Domain Controller in na.arborshoes.com to native mode.
   Add the Graphic Artists group to the Artists Domain Local group.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Applications use distribution groups as lists for nonsecurity-related functions. We should use distribution groups when the only function of the group is nonsecurity-related, such as sending e-mail messages to a group of users at the same time. We cannot use distribution groups to assign permissions. Windows 2000 uses only security groups, which we can use to assign permissions to gain access to resources. Therefore the global group needs to be a security group to inherit permissions.

Incorrect Answers:
B: Windows 2000 uses only security groups, which we can use to assign permissions to gain access to resources. Therefore the global group needs to be a security group to inherit permissions. Furthermore, universal groups are not supported in mixed mode domains. A mixed mode domain comprises Windows 2000 and Windows NT 4.0 computers. As universal groups are a new feature in Windows 2000 Windows NT 4.0 cannot support them.
C: Windows 2000 uses only security groups, which we can use to assign permissions to gain access to resources. Therefore the global group needs to be a security group to inherit permissions.
D: We cannot change the domain mode to native mode as the domain has two Windows NT BDCs. Native mode can only be specified for domain that only uses Windows 2000 Domain Controllers. Furthermore, we can use security groups to assign permissions to gain access to resources. Therefore the global group needs to be a security group to inherit permissions.

QUESTION 120
When you run DCPromo.exe to install the new domain, you receive an error message stating that the existing domain cannot be contacted. Installation of the new child domain will not proceed.

What should you do to correct this problem?

A. Create an Active Directory integrated zone for the child domain on the new Domain Controller.
B. Install WINS on the new Domain Controller.
C. Configure the new Domain Controller with the address of an authoritative DNS server for the existing domain.
D. Configure the new Domain Controller with the address of an existing WINS server.
E. Add SRV (service) records for the domain naming master to a Hosts file on the new Domain Controller.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: When we promote a member server to a Domain Controller, the Domain Controller must be able to connect to a DNS server. Therefore the address of the DNS sever should be configured in the TCP/IP properties of the Domain Controller.

Incorrect Answers:
A: When we promote a member server to a Domain Controller, the Domain Controller must be able to connect to a DNS server. Therefore the address of the DNS sever should be configured in the TCP/IP properties of the Domain Controller. It is not necessary and not possible to create an Active Directory integrated zone for the child domain on the new Domain Controller as we are unable to upgrade the machine to a Domain Controller.
B: A WINS server is not required for the promotion of a member server to a Domain Controller.
D: A WINS server is not required for the promotion of a member server to a Domain Controller.
E: We cannot add SRV records to a hosts file.

QUESTION 121
You are the administrator of your company's network. Your company's main office is in Seattle. Large regional offices are located in Chicago, Los Angeles, and New York, as shown in the exhibit.

Three smaller branch offices are located within each region. The regional offices are connected to the main office by T1 lines. The branch offices are connected to the regional offices by ISDN lines. Branch offices in Boston, Dallas, and San Diego also have direct ISDN connections with Seattle. The network consists of one Windows 2000 domain. For fault-tolerance and load-balancing purposes, each office has its own Windows 2000 Domain Controller. Each office is configured as its own site. All site links have been created. You want to create a replication topology that allows only the regional offices to communicate with the main office. You want to ensure that each branch office communicates only with the closest regional office.

What should you do?

A. Manually create connection objects between the Domain Controllers in the main office and the regional offices Use SMTP as the transport protocol.
B. Manually create connection objects between each branch office and the closest regional office. Use SMTP as the transport protocol.
C. Allow the Knowledge Consistency Checker (KCC) to automatically create the connection objects between the main office and all other offices.
D. Allow the Knowledge Consistency Checker (KCC) to automatically create the connection objects between the branch offices and the regional offices.

Answer: C

Section: (none)

Explanation/Reference:
Explanation: The Knowledge Consistency Checker (KCC) is a built-in service that runs on all Domain Controllers and automatically establishes connections between individual machines in the same site. These are known as Windows 2000 Directory Service connection objects. In this scenario a replication topology must be created that allows only regional offices to communicate with the main office. The regional offices should not be included. Since this is a single domain SMTP cannot be used for replication. The KCC will automatically create connection objects.

Note 1: The Knowledge Consistency Checker (KCC) is a Windows 2000 component that automatically generates and maintains the intra-site and inter-site replication topology.

Note 2: SMTP replication is used only for replication between sites. You also cannot use SMTP replication to replicate between domain controllers in the same domain—only inter-domain replication is supported over SMTP (that is, SMTP can be used only for inter-site, inter-domain replication).

Reference:
HOW TO: Disable the Knowledge Consistency Checker Inter-Site Topology Generation for All Sites (Q245610)
Microsoft Techinfo, Step-by-Step Guide to Setting up ISM-SMTP Replication

Incorrect Answers:
A: The SMTP protocol can only be used for intersite replication between different domains.
B: Connection objects must be made between the main office and the regional office, not between branch and regional offices. Furthermore, the SMTP protocol can only be used for intersite replication between different domains.
D: The KCC should be set up to automatically create the connection objects between the main office and all other offices, not between the branch offices and the regional offices.

QUESTION 122
You are the administrator of your company's network. Your company's main office is in Chicago. Company operations are divided into two regions East and West. The East region has an office in Miami and an office in New York. The West region has an office in Denver and an office in Seattle. The offices in the East region contain the human resources (HR) and marketing (Mktg) departments. The offices in the West region contain the sales and finance departments. Company IT policy states that Group Policy must be applied only at the organizational unit (OU) level, and that user groups must correspond to departments.

You want to accomplish the following goals:

- Control of users and resources can be delegated to local and departmental administrators.
- The IT department can control Group Policy for the entire enterprise.
- A single Group Policy object (GPO) can be applied to the sales and marketing departments.
- User environments can be customized by city.

You implement an OU structure as shown in the exhibit.

Which result or results does your implementation produce? (Choose all that apply.)

Exhibit:

A. Control of users and resources can be delegated to local and departmental administrators.
B. The IT department can control Group Policy for the entire enterprise.
C. A single GPO can be applied to the sales and marketing departments.
D. User environments can be customized by city.

Answer: ABC
Section: (none)

Explanation/Reference:
Explanation:
A: Local and Departmental administrators can be delegated control since there are departmental OUs.
B: The IT department can configure one single OU and apply it to Corp OU.
C: A single GPO can be applied to several OUs. There is an OU for Sales department and one OU for the Finance Department.

Incorrect Answers:
D: There are no OUs for the cities so user environments cannot be customized by city.

QUESTION 123
You are the administrator of your company's network. The network consists of one Windows 2000 domain. Your company has two locations, which are connected by a dedicated T1 line. Users frequently report that logons to the network, file transfers, and directory searches are extremely slow. When you monitor the network, you discover that replication between Domain Controllers is generating excessive network traffic between the locations.

You want to accomplish the following goals:

- Replication traffic between locations will be reduced.
- Logon response time for users will be improved.
- Average file transfer rates for users will be improved.
- Directory search response times will be improved.
- All Domain Controllers will have up-to-date replicas of the directory.
- Fault tolerance for domain logons and directory searches will be maintained.

You take the following actions:

- Configure a Domain Controller in each location to be a Global Catalog server.
- Create a new subnet in Active Directory for each location.
- Modify the location attribute of each Domain Controller's server object.

Which result or results do these actions produce? (Choose all that apply.)

A. Replication traffic between locations is reduced.
B. Logon response time for users is improved.
C. Average file transfer rates for users are improved.
D. Directory search response times are improved.
E. All Domain Controllers have up-to-date replicas of the directory.
F. Fault tolerance for domain logons and directory searches is maintained.

Answer: ABDEF
Section: (none)

Explanation/Reference:
Explanation:
A: Global Catalog Servers store a large part of the Active Directory. So less Active Directory data will have to be replicated.
B: By adding a site (with the subnet) at each location the local Domain Controller will be used for logon.
D: The Global Catalog server holds a copy of all objects of the whole forest and can be used for Active Directory searches.
E: The default replication time is 180 minutes. This keeps the Domain Controllers with up-to-date replicas of the directory.
F: Global Catalog servers in each location provide fault tolerance for both domain logons and directory searches.

Incorrect Answers:
C: In this scenario we have not improved file transfer speed.

QUESTION 124
You are the administrator of a DNS server that runs on a Windows 2000 Server computer. You receive a report that the Windows 2000 Server computer constantly uses more than 80 percent of the CPU. You want to monitor the number of DNS queries that are handled by the DNS server. What should you do?

A. Run the Nslookup command-line utility.
B. Use the Event Viewer and monitor the DNS server log.
C. Use the monitoring function of the server properties in the DNS console.
D. Use the DNS counters in System Monitor.
E. Check the contents of the Netlogondns file.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: With System Monitor we can monitor the DNS counters over a period of time and see the results in real-time. These counters include Total Query Received, Total Query Received/Sec, Failed DNS, Pending DNS Resolutions, and Successful DNS Resolutions.

Incorrect Answers:

A: The Nslookup command-line utility is used to send a resolution request to a DNS server.
B: The Event Viewer can be used to view the data contained in the DNS server log however only errors are logged to the DNS server log. This will therefore not provide us with any statistics about the number of queries.
C: The monitoring function of the server properties in the DNS console will only provide us with total statistics, it will not provide us with figures for concurrent queries.
E: Windows 2000 does not have a Netlogondns file.

QUESTION 125
You are the administrator of your company's Windows 2000 network. You have been auditing security events on the network since it was installed. A user on your network named John Thorson recently reported that he was no longer able to change his password.

Because there have been no recent changes to account policies, you suspect that someone has been modifying the properties of user accounts in Active Directory. There are thousands of entries in the event logs, and you need to isolate and review the events pertaining to this problem in the least possible amount of time.

What should you do?

A. In the security log, create a filter for events matching the following criteria:
   Event source: Security
   Category: Account Management
   User: JTHORSON.
B. In the directory service log, create a filter for events matching the following criteria:
   Event source: NTDS Security
   Category: Security.
   Search the remaining items for events referencing John Thorson's account.
C. In the directory service log, create a filter for events matching the following criteria:
   Event source: NTDS Security
   Category: Global Catalog
   User: JTHORSON.
D. In the security log, create a filter for events matching the following criteria:
   Event source: Security
   Category: Account Management.
   Search the remaining items for events referencing John Thorson's account.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: User accounts are related to security events and the creation or deletion of accounts is related to account management. In this scenario we must therefore create a filter based on security events and must specify the account management category. We however cannot filter events by username. We must thus manually search for events referencing John Thorson's account after the account management filter has been applied.

Incorrect Answers:
A: In Event Viewer we cannot filter events by username.
B: User accounts are related to security events and the creation or deletion of accounts is related to account management. In this scenario we must therefore create a filter based on security events and must specify the account management category.
C: User accounts are related to security events and the creation or deletion of accounts is related to account management. In this scenario we must therefore create a filter based on security events and must specify the account management category.

QUESTION 126
You are the administrator of your company's network. The network is configured as a Windows 2000 domain.

You want to strengthen the security of communications between client computers and servers in the Reps organizational unit (OU). You do not want to decrease overall productivity of the domain.

What should you do?

A. Create one Group Policy object (GPO) in the Sales OU. Increase maximum service ticket lifetime in the GPO, and decrease maximum lifetime that a user ticket can be renewed in the GPO.
B. Create one Group Policy object (GPO) in the Sales OU. Decrease maximum service ticket lifetime in the GPO, and decrease maximum lifetime that a user ticket can be renewed in the GPO.
C. Create one Group Policy object (GPO) in the Reps OU. Decrease maximum service ticket lifetime in the GPO, and increase maximum lifetime that a user ticket can be renewed in the GPO.
D. Create one Group Policy object (GPO) in the Reps OU. Decrease maximum service ticket lifetime in the GPO, and decrease maximum lifetime that a user ticket can be renewed in the GPO.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: We need to strengthen the security of communications between client computers and servers in the Reps OU. We create a GPO and link it to Reps OU. The policy will be used to increase security of the Kerberos Authentication protocol.

Maximum service ticket lifetime
A "service ticket" is a session ticket. Default value: 10 hours.
By decreasing the **Maximum service ticket lifetime,** session keys will change more often and would be harder to expose.

Maximum lifetime that a user ticket can be renewed
This is the maximum lifetime of a user ticket. No ticket can be renewed after this time. Default value: 7 days.
By increasing the **Maximum lifetime that a user ticket can be renewed**, the user tickets would be refreshed periodically without having to issue completely new tickets.

Incorrect Answers:
A: The GPO must be applied to Reps OU, not the Sales OU, since the security of the computers in the Reps OU need to be strengthened.
B: The GPO must be applied to Reps OU, not the Sales OU, since the security of the computers in the Reps OU need to be strengthened.
D: The **Maximum lifetime that a user ticket can be renewed** should be increased, not decreased, since this would allow refreshing periodically without having to issue completely new tickets.

QUESTION 127
You are the administrator for Arbor Shoes. Administrative control of Active Directory has been delegated to several people in the company. You need to track changes made to the arborshoes.com domain. To ensure accountability of the other administrators' actions, you want to monitor user and computer account creation and deletion.

What should you do?

A. Modify the default Group Policy object (GPO) on the arborshoes.com domain. Configure the local audit policy to audit account management and directory services access for success and failure. Monitor the security logs for activity on the Domain Controllers.

B. Modify the default Group Policy object (GPO) on the Domain Controllers organizational unit (OU). Configure the local audit policy to audit account management and directory services access for success and failure. Monitor the security logs for activity on the Domain Controllers.
C. Modify the default Group Policy object (GPO) on the Domain Controllers organizational unit (OU). Configure the local audit policy to audit account logon events and object access for success and failure. Monitor the security logs for activity on the Domain Controllers.
D. Modify the default Group Policy object (GPO) on the arborshoes.com domain. Configure the local audit policy to audit account logon events and object access for success and failure. Monitor the security logs for activity on the Domain Controllers.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: We need to audit directory services access for computer accounts and account management for user accounts. These accounts will be created on Domain Controllers so we only need to audit the Domain Controllers OU.

Incorrect Answers:
A: No need to audit the whole domain.
C, D: Wrong things being audited.

QUESTION 128
You want to implement a password policy for all users in an organizational unit (OU) named Sales in a Windows 2000 network. All the users in the Sales OU are in a group named Sales Users. You create a Group Policy object (GPO) named PassB to enforce a minimum password length of six characters. You assign the PassB GPO to the Sales OU. There are no other GPOs assigned that specify a minimum password length. However, the week after you assign the PassB GPO to the Sales OU, users from the Sales OU report that they can still change their passwords to consist of fewer than six characters.

How should you correct this problem?

A. Ensure that the Sales Users group has Read and Apply Group Policy permissions on the PassB GPO.
B. Apply the PassB GPO to the domain instead of to the Sales OU. Filter the policy for the Sales Users group.
C. For the Sales OU, block policy inheritance.
D. For the Sales OU, enforce policy inheritance on the PassB GPO.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: Password policies can only, and must always, be applied at domain level as Windows 2000 ignores password policies set at lower levels.

Incorrect Answers:
A: Password policies must be applied at domain level.
C: Blocking or enforcing policy inheritance will not ensure that the policy is implemented. Password policies set at OU level are ignored by Windows 2000.
D: Blocking or enforcing policy inheritance will not ensure that the policy is implemented. Password policies set at OU level are ignored by Windows 2000.

QUESTION 129
You are the administrator of a Windows 2000 network. Your network has one domain named parnellaerospace.

com. The parnellaerospace.com domain supports 8,000 users at three locations. The network has three sites connected by T1 lines, as shown in the exhibit.

The West site has 2,500 users; the East site has 3,000 users; and the Central site has 2,500 users. Each site contains a Global Catalog server. The Global Catalog server in the West site is named LAX01-Global Catalog. The Global Catalog server in the Central site is named TUL01-Global Catalog. The Global Catalog server in the East site is named NYC01-Global Catalog.

You want users located in the West site to query TUL01-Global Catalog if the West site Global Catalog server is offline. What should you do?

Exhibit:

A. Create a new subnet, assign it to the West site, and move TULO 1-Global Catalog to the West site.

B. Configure the site link between the Central site and the West site to have a lower cost than the site link between the West site and the East site.
C. Add a Global Catalog server to the Central site that has an IP address in the West site subnet.
D. Configure TUL01-Global Catalog as a preferred bridgehead server.
E. Set the query policy on LAXO 1-Global Catalog to the default query policy.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: By default, network traffic will pass across the route that has the lowest cost in Windows 2000. We can therefore configure which routes network traffic should pass through by specifying the cost of each site link; network traffic would then pass across the route with the lowest cost.

Incorrect Answers:
A: It is not necessary assign a new subnet to the West site and move TULO 1-Global Catalog to the West site as we can ensure that network traffic passes across a particular route by specifying route costs for all the routes in the network. Network traffic will then pass across the route with the lowest cost.
C: Adding a Global Catalog server to the Central site that has an IP address in the West site subnet would render the Global Catalog server unable to communicate with any other computers, as it must be configured with the subnet mask of the subnet it s located on. In this solution that subnet mask should be the subnet of the Central site. This however would not ensure that network traffic passes across a particular route.
D: Bridgehead servers are the Domain Controllers in each site that replication goes between.
E: Windows 2000 does not support a query policy.

QUESTION 130
You are the administrator of a large Windows 2000 network. You have three domains named adatum.com, us. adatum.com, and eur.adatum.com. Eric has recently been hired to assist you with network administration. You want him to be able to manage user accounts, back up servers, and configure services on all workstations and servers only in the eur.adatum.com domain.

What should you do?

A. Add Eric to the Enterprise Admins group and delegate control only at the adatum.com domain.
B. Move Eric's user account to the Domain Controllers organizational unit (OU) in eur.adatum.com.
C. Add Eric's user account to the Domain Admins group in eur.adatum.com
D. Add Eric's user account to the Server operators and Account operators group in eur.adatum.com.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: To configure services on workstations, Eric needs to be a member of the Domain Admins group.

Incorrect Answers:
A: In Windows 2000 we cannot delegate control only at the adatum.com domain.
B: The Domain Controllers organizational unit is an OU for Domain Controllers, not users. We therefore cannot add users to the Domain Controllers organizational unit.
D: To configure services on workstations, Eric needs to be a member of the Domain Admins group. Furthermore, the Server Operators group does not exist on the Windows 2000 Professional workstation computers.

QUESTION 131

You create an organizational unit (OU) structure for the blueskyairlines.com domain. You want to delegate administrative control of user objects on your Windows 2000 network. The User OU is a child of the Research OU.

You create a group named Research User Administrator that includes users who have permissions to create and manage the workstations in the Workstation OU.

The Research User Administrator group has Full Control permission on the Research OU. You want user accounts to be created only in the User OU.

Which three actions should you take?

A. Grant Full Control permission to the Research User Administrator group on the User OU for computer objects.
B. Remove the Research User Administrator group from the Research OU ACL.
C. Grant Create Contact objects permission on the User OU.
D. Disable inheritance of permissions from the Research OU to the User OU.
E. Deny Create User objects permission on the Research OU.
F. Grant Read and Write permissions to the blueskyairlines.com domain

Answer: ADE
Section: (none)

Explanation/Reference:
Explanation: In this scenario the Research User Admin Group already has Full Control permissions on the Research OU. The User OU is a child of the Research OU and user accounts should only be created in the User OU. Therefore we should give the Research User Admin group Full Control permissions for computer objects of the User OU. This would allow them to create User accounts in the User OU. We should deny Create User objects permission on the Research OU. This will prevent user accounts being created in the Research OU. We must then disable inheritance from the Research OU to the User OU so that the User OU does not inherit the “Deny Create User Objects” Permission from the Research OU.

Incorrect Answers:
B: Removing the Research User Administrator group from the Research OU ACL is not required. By removing them, they would have no permission on the Research OU, but the only requirement on the Research OU is that user accounts must not be created.
C: A contact object is not a user account. A contact object is an account that does not have any security permissions. You cannot log on to the network as a contact. Contacts are typically used to represent external users for the purpose of e-mail.
F: Granting read and write permissions to the domain would allow user accounts to be created throughout the domain, but they should only be created only in the User OU.

QUESTION 132
You are the administrator of a Windows 2000 domain. The domain has an OU named NORTH. You want to standardize the Start menu for the users in the NORTH OU. Some members of the Domain Admins group are in the NORTH OU. Folders and shortcuts that form the standardized Start menu are on the network at \\server2 \menu. The Everyone group has change permission on the menu share.

You want to accomplish the following goals:

- Each member of the Domain Admins group will have a separate Start menu that the member can change.
- All users in the NORTH OU, except members of the Domain Admins group, will use the \\server2\menu Start menu.
- Users who use the \\server2\menu Start menu will not be able to change the contents of the Start menu.
- Each user who is not a member in the NORTH OU will have a separate Start menu that the user can

change.

You take the following actions:

- Create a new GPO named Menu.
- Assign the Menu GPO to the NORTH OU.
- Configure the Menu GPO to redirect the Start menu folder for the Domain Users group to \\server2\menu
- Change the permissions on the Menu GPO to deny the Apply Group policy permission to the Domain Admins group.

Which result or results do these actions produce? Choose all that apply.

A. Each member of the Domain Admins group will have a separate Start menu that the member can change.
B. All users in the NORTH OU, except members of the Domain Admins group, will use the \\server2\menu Start menu.
C. Users who use the \\server2\menu Start menu will not be able to change the contents of the start menu.
D. Each user who is not a member in the NORTH OU will have a separate Start menu that the user can change.

Answer: ABD
Section: (none)

Explanation/Reference:
Explanation:

A: Each member of the Domain Administrators Group will have a separate start menu that the member can change as we have changed the permissions on the Menu GPO to deny the Apply Group policy permission to the Domain Admins Group. This would result in the Menu GPO not being applied to the Domain Admins Group.
B: We have configured the Menu GPO to redirect the Start menu folder for the Domain Users group to \ \server2\menu. Therefore all users in the NORTH OU, except members of the Domain Admins group, will use the \\server2\menu Start menu.
D: We have assigned the Menu GPO to the NORTH OU. Therefore the policy will only be applied to the NORTH OU. Each user who is not a member in the NORTH OU will thus have a separate start menu that the user can change.

Incorrect Answers:
C: The Everyone group has permission to change the menu folder.

QUESTION 133
You are the network administrator of a Windows 2000 network. The network consists of 500 Windows 2000 Professional computers. You recently discovered that users of these computers have been using the same passwords since their accounts were created. You need to correct this problem to maintain security in the network.

You create a Group Policy object (GPO) and filter it to the users. You want to configure the GPO to require users to create a different password periodically.

Which two settings should you enable? (Choose Two)

A. Minimum password length.
B. User must log on to change the password.
C. Enforcement of password history.
D. Minimum password age.

E. Maximum password age.

Answer: CE
Section: (none)

Explanation/Reference:
Explanation: To ensure that users create a different password periodically we should enable the Enforcement of password history and the Maximum password age options. This will force the users to change their passwords once the password reaches a particular age. Furthermore, the password history will prevent them from using the same passwords again.

Incorrect Answers:
A: The Minimum password length option will force users to specify passwords of a particular character length.
B: The User must log on to change the password option will ensure that the users must log on first before they can change their password. It does not force them to change their passwords.
D: The Minimum password age option will force users to keep their passwords for a set minimum amount of time. It will not force them to change their passwords once that time has expired but will prevent them from changing it until the set time has expired.

QUESTION 134
You are the administrator of a Windows 2000 network that has only one domain. You are configuring the network security settings for the domain's Windows 2000 Professional users.

Your Sales team uses portable computers and Routing and Remote Access to connect to the company's network. Sales users need local Administrator rights to their computers so that they can run a third party application. You want to configure the computers to prevent the users from modifying their existing network connections.

What should you do?

A. On each portable computer, create only the permitted LAN and Remote and Routing Access connection. At the server, configure the Sales user accounts to permit connections to only the specific computers.
B. Create a System Policy to hide Network Neighborhood and disable registry-editing tools. Apply this policy to all the Sales users.
C. Create a Group Policy object (GPO) for the domain.
Filter the GPO for the Sales users.
Configure the GPO to deny the Sales users access to the properties of the LAN or Remote and Routing Access connection.
D. Create a Group Policy object (GPO) for the Domain Controllers.
Filter the GPO for the Sales users.
Configure the GPO to deny the Sales users access to the Network Connection Wizard.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: We can use GPOs to implement computer configuration. In this scenario we must create a Group Policy object (GPO) for the domain and filter the GPO for the Sales users. Configure the GPO to deny the Sales users access to the properties of the LAN or Remote and Routing Access connection. This will prevent the Sales users from changing any settings on the LAN or RRAS connections.

Incorrect Answers:
A: Configuring the Sales user accounts at the server to permit connections to only the specific computers will not prevent the Sales user from modifying the network connections on their computers.
B: System policy was used on Windows NT 4.0 computers. It has been superceded by Group Policy in

Windows 2000.
D: The Group Policy object (GPO) must be applied to the domain, not the Domain Controllers.

QUESTION 135
You are the administrator of a Windows 2000 network. Users in an Organizational Unit (OU) named Procs need to have a drive mapped to a network location. These users log on from Windows 2000 Professional computers. You want to use a logon script named Userlog.cmd to implement this drivemapping for all current and future users in the Procs OU.

What should you do?

A. Copy Userlogon.cmd to the Netlogon share on each Domain Controller in the domain.
   Select each user in the Procs OU and set the logon script to Userlog.cmd.
B. Copy Userlog.cmd to the Sysvol share on each Domain Controller.
   Assign Read permission to the file for all users in the Procs OU.
C. Create a Group Policy object (GPO) that enforces Userlog.cmd as a logon script.
   Assign the GPO to the Procs OU.
D. Create a Group Policy object (GPO) that enforces Userlog.cmd as a startup script.
   Assign the GPO to the Procs OU.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: By creating a Group Policy object (GPO) that enforces Userlog.cmd as a logon script and assigning this GPO to the Procs OU we will ensure that the GPO will affect all current users and any future users in the Procs OU.

Incorrect Answers:
A: Setting the logon script each user in the Procs OU would require considerable administrative effort and will have to be performed for all future users of the Procs OU as well. Creating a Group Policy object (GPO) that enforces Userlog.cmd as a logon script and assigning this GPO to the Procs OU would require less administrative effort and will ensure that the policy is automatically applied to all future members of the Procs OU as well.
B: In this scenario we have assigned read permission to the Userlog.cmd file for all users in the Procs OU. This will give the users in the Procs OU permission to read the file and will not ensure the implementation of the logon script.
D: In this scenario we require a logon script, not a startup script. A logon script is executed every time a user logs on to the network while a startup script is only executed when the computer starts.

QUESTION 136
You are the backup operator of a Windows 2000 domain. The domain has two Domain Controllers. You want the Active Directory database files of both Domain Controllers to be automatically backed up once a week.

What should you do?

A. Schedule a backup job that will backup the System State Data once a week.
B. Schedule a backup job and select Schema.ini file in the System32 folder and all files in the NTDS folder to be backed up once a week.
C. Schedule a task that will run the Ntdsutil once a week.
D. Schedule a task that will copy the Ntds.dit file and the Sysvol folder once a week.

Answer: A

Section: (none)

Explanation/Reference:
Explanation: The System State data includes the registry, the COM+ Class Registration database, system boot files, the SYSVOL directory, the Active Directory, and the Certificate Services database if the server is a certificate server. Therefore, the Active Directory database files will be backed up when we perform a backup of the System State data. We however cannot choose to restore only individual components, such as the Active Directory database files, of the System State data.

Incorrect Answers:
B: Scheduling a backup job and selecting the Schema.ini file in the System32 folder and all files in the NTDS folder to be backed up once a week might work, but the System state data option was designed specifically for this purpose.
C: Although it is possible to use Ntdsutil to backup the data, an automated solution such as a System State Data backup would be a better solution.
D: Scheduling a task that will copy the Ntds.dit file and the Sysvol folder once a week might work, but the System state data option was designed specifically for this purpose.

QUESTION 137
You are the administrator of your company's network. The network consists of one Windows 2000 domain that is connected to the Internet. You want to prevent Internet users from using the LS command of the nslookup utility against your DNS server to view the computers on your network.

However you want to allow the use of utility internally on your network for diagnostic purposes. You also want your DNS server to be able to respond to legitimate name resolution requests from the Internet.

What should you do?

A. In the DNS server properties restrict the interfaces on which DNS will respond to requests.
B. In the DNS server properties select the disable recursion advanced option.
C. In the zone properties set the permission on the zone to allow only the administrators group to access the zone.
D. In the zone properties set the option to allow zone transfers only to specified IP addresses.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: By disabling recursion our name servers will be in passive mode and would not send queries on behalf of other name servers or resolvers. The server will also not conduct recursive searches on behalf of DNS clients. If they receive an external nslookup -ls request, the request will be discarded.

Incorrect Answers:
A: In this scenario the DNS server is going to be used both internally and externally. Restricting the interfaces on which the DNS server will respond to requests is thus not an option.
C: It is not possible in the zone properties to set permission on the zone to allow or restrict user or groups to access the zone, in particular it is not possible to only allow the administrator group to access the zone.
D: We are interested in restricting Internet users from using the nslookup -ls, not restricting zone transfers.

QUESTION 138
You are the administrator of a Windows 2000 domain. The domain is in native mode. The domain contains 15 Windows 2000 Server computers that are functioning as Domain Controllers and 1500 Windows NT client computers.

During a power outage the first Domain Controller that you install suffers a catastrophic hardware failure and will not restart. After the power outage users report that password changes do not take the effect for several hours. In addition users are not able to logon or connect to resources by using their new passwords.

What should you do to correct this problem?

A. Using the NTDSUTIL utility connect to another Domain Controller and transfer the PDC emulator role.
B. Using the NTDSUTIL utility connect to another Domain Controller and seize the PDC emulator role.
C. Using the NTDSUTIL utility connect to another Domain Controller and transfer the domain naming master role.
D. Using the NTDSUTIL utility connect to another Domain Controller and cease the domain naming master role.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: The PDC emulator is needed for password changes etc for the Windows NT computers. In this scenario the PDC emulator is offline therefore we need to seize the role. If it was online we could transfer the role.

Incorrect Answers:
A: If the PDC emulator was online we could transfer the role. However the PDC emulator is offline and we therefore have to seize the role.
C: The domain naming master is not related to passwords changes. The PDC emulator is needed for password changes
D: The domain naming master is not related to passwords changes. The PDC emulator is needed for password changes.

QUESTION 139
You are the network administrator for Contoso Ltd. Marc is moving from the IT department to the Sales department and will be the technical sales manager for the eastern United States.

The current OU structure is shown in the exhibit.

You move Marc's user account from the IT OU to the Technical Sales OU. You want Marc to be able to create user accounts in ou=sales, ou=eastern, dc=contoso, dc=com. What should you do?

Exhibit:

A. Move Marc's user account to the Sales OU.
B. Add Marc's user account to the Account Operators group.
C. Grant Marc's user account Create User Object Permission for the Sales OU.
D. Grant Marc's user account Write permission for the Sales OU.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: Through the use of the delegation of control wizard we can grant users permissions to perform specific tasks. We could thus grant users permissions to create user objects such as user accounts. In this way we can delegate administration.

Incorrect Answers:
A: Moving Marc's user account to the Sales OU will not give him any permissions for the OU.
B: Adding Marc's user account to the Account Operators group will grant Marc too much permission. He could then create user accounts anywhere in the domain.
D: Granting Marc's user account Write permission for the Sales OU will allow him to create any objects in the Sales OU.

QUESTION 140
You are the administrator of your company's network. The network consists of two Windows 2000 domains. There are 10 Windows 2000 Server computers and 1100 Windows 2000 Professional client computers on the network. Two of the servers in each domain function as Domain Controllers. Both domains are in native mode. When the initial Domain Controller is taken off line for maintenance users receive an error message stating

that the Domain Controller cannot be located. Users are not able to logon to the network, although the other Domain Controllers are still operating.

What should you do to correct this problem?

A. Create a primary DNS zone.
B. Create a secondary DNS zone.
C. Configure at least one other Domain Controller as the Global Catalog server.
D. Configure at least one other Domain Controller as a PDC emulator.
E. Configure at least one other Domain Controller as a WINS server.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: In a native mode domain we require a Global Catalog for logon purposes. By default the first Domain Controller in the domain serves as a Global Catalog. The other Domain Controllers do not serve as a Global Catalog unless we configure them to serve as a Global Catalog.

Incorrect Answers:

A: All Windows 2000 domains require a DNS server. If there were no DNS the domain would not be functional. However, the DNS server is required for name resolution, not for logon purposes. In a native mode domain we require a Global Catalog for logon purposes.
B: All Windows 2000 domains require a DNS server. If there were no DNS the domain would not be functional. However, the DNS server is required for name resolution, not for logon purposes. In a native mode domain we require a Global Catalog for logon purposes.
D: PDC emulators are only required for down-level clients, although without one, we would not be able change our passwords.
E: A WINS server is required by downlevel computers for name resolution, not for logon purposes. However, in a native mode domain we require a Global Catalog for logon purposes.

QUESTION 141
You are the administrator of Trey Research. Trey Research has two Windows 2000 domains named treyresearch.com and na.treyresearch.com. Blake has a user account in the trey research.com domain and needs to use support documents in the na.treyresearch.com domain.

You create a global group name NA support in na.treyresearch.com. NA support is a member of the Domain Local group named Support. Support has read permission to the Support shared folder in the na.treyresearch. com domain. Your network contains only Windows 2000 Domain Controllers. The domains are in native mode.

You want to grant Blake Read permissions to the Support shared folder. What should you do?

A. Create a universal group in treyresearch.com and make Blake a member.
   Add the universal group to the NA support group.
B. Create a new user account in the na.treyresearch.com.
   Use the same user name and password that Blake uses for his user account in the treyresearch.com.
C. Create a global group in treyresearch.com and make Blake a member.
   Add the global group to the NA Support group.
D. Create a universal group in treyresearch.com and make Blake a member. Add the universal group to the Support group.
E. Create a new global group name Global Support in treyresearch.com.
   Add Blake to new global group.
   Add the Global Support group to the Support group.

Answer: E
Section: (none)

Explanation/Reference:
Explanation: In this scenario we are only talking about one user in one domain therefore we need only a global group that must be added to the domain local group. Therefore we should create a new global group, add Blake to new global group and add the Global group to the Support group.

Incorrect Answers:
A: In this scenario we are only talking about one user in one domain therefore we need only a global group and not a universal group. Microsoft recommends that we add the Universal Group to a Global Group in another Domain. But global groups can only contain user accounts and global groups from the same domain.
B: We cannot create two user accounts with the same name and password. Each user account must have its own SID. Furthermore, Blake's user account has not been given any permissions on the shared folder.
C: We cannot add a global group to another global group in a different domain.
D: In this scenario we are only talking about one user in one domain therefore we need only a global group and not a universal group. Microsoft recommends that we add the Universal Group to a Global Group in another Domain. But global groups can only contain user accounts and global groups from the same domain.

QUESTION 142
You are the enterprise administrator of a network. The network has eight domains in the domain tree. You add a domain to the domain tree. One of the Domain Controllers in the root domain becomes unavailable because of a hardware failure. After the hardware failure you are unable to add an additional domain to the domain tree. How should you correct this problem?

A. On one of the other Domain Controllers seize the domain naming master role.
B. Promote a Windows 2000 server computer to be able to be a replica controller in the root domain.
C. On one of the other Domain Controllers seize the infrastructure master role.
D. Open the Active Directory sites and services console on a Domain Controller from the root domain and force replication.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: We require a domain naming master to add domain trees to the forest. As the Domain Controller that acts as the domain naming master role is offline we have to seize the role.

Incorrect Answers:
B: Promoting a Windows 2000 server computer to be able to be a replica controller in the root domain won't solve the problem, as the replica will not have the domain naming master role. The Domain Controller that acts as the domain naming master role is offline
C: The Infrastructure Master role keeps track of group membership, not domain names.
D: We cannot replicate the domain naming master role, as the Domain Controller that acts as the domain naming master role is offline

QUESTION 143
You are the network administrator for Blue Sky Airlines. You are implementing a Windows 2000 network consisting of five sites in the blueskyairlines.com domain.

There are 15,000 users in Chicago, 5,000 users in Los Angeles, 2,000 users in Miami, 10,000 users in New York and 2,000 users in Seattle. You are designing the structure of your DNS service. You want to allow secure dynamic updates to DNS in Chicago, Los Angeles and New York. You want full DNS replication to occur in all

the three sites. You do not want Miami site have an editable copy of DNS zone.

How should you configure the DNS server to accomplish this goal?

To Answer: click the Select and Place button and then drag the letter indicating the appropriate server type to each site. Next drag the number indicating the appropriate zone type to each site. Two sites have been partially contained for you. (Note zone types and server types can be used more than one)

Answer:

Section: (none)

Explanation/Reference:
Chicago, LA, New York.
Active Directory integrated zones for secure updates. Need Domain Controllers for Active Directory integrated zones.
Seattle, Miami.
Secondary zones for full zone replication. Secondary zones are non editable. Use member servers for secondary zones.

QUESTION 144
You are the administrator of a Windows 2000 domain. The domain has a Windows 2000 Server computer named MainApps. The MainApps server is not a domain controller.

Members of the Domain Users group have the right to logon locally at the MainApps server. When one of these members logs on locally you want a script named Setperms.vbs to be executed. This script defines environment variables in the settings in the current user's profile that are needed for the MainApps server.

What should you do?

A. Copy the Setperms.vbs script to the Netlogon share on the MainApps server.
B. Place the Setperms.vbs script in the Sysvol share on the MainApps server.
C. Add the Setperms.vbs script to the local Group Policy Object (GPO) as a logon script.
D. Add the Setperms.vbs script to the local Group Policy Object (GPO) as a startup script.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: By adding the Setperms.vbs script to the local Group Policy object (GPO) as a logon script we will ensure that when a user logs on to the local computer the logon script will be processed.

Incorrect Answers:
A: Copying the Setperms.vbs script to the Netlogon share on the MainApps server will make the file available to all users who have the required permissions to the shared folder. We however require the script on the local computer and not the network share. Furthermore, this will not ensure that the script is executed when a user logs on to the local computer.
B: Placing the Setperms.vbs script in the Sysvol share on the MainApps server will make the file available to all users who have the required permissions to the shared folder. We however require the script on the local computer and not the network share. Furthermore, this will not ensure that the script is executed when a user logs on to the local computer.
D: In this scenario we require a logon script, not a startup script. A logon script is executed every time a user logs on to the network while a startup script is only executed when the computer starts.

QUESTION 145
You are the administrator of a Windows 2000 domain. The domain has an Organizational Unit (OU) names Sales. All users in the Sales OU use an application named Planning. The Planning application is deployed by using a Group Policy Object (GPO) named Plan App on the Sales OU.

The Plan App GPO is configured to assign the Planning application to users by using a Microsoft Windows installer package for the application. The Planning application will be replaced by another application in the next month.

You want to accomplish the following goals:

- Users who have not yet installed the Planning application will be prevented from installing the application.
- Users who have already installed the Planning application will be able to continue to use it.
- If key application files are missing when the Planning application starts, the missing files will be reinstalled automatically.
- If the vendor of the Planning application releases a software patch by using a Windows Installer package you will be able to assign the patch to only users who have already installed the application.

You take the following actions:

- Create a new software category named Optional Apps.
- Configure the Plan App GPO to add the Planning application to the Optional Apps software category.
- Configure the Plan App GPO to remove the Planning application, but select the option to allow users to continue to use this software.

Which result or results do these actions produce? (Choose all that apply)

A. Users you have not yet installed the Planning application are prevented from installing the application.
B. Users who have already installed the Planning application can continue to use it.

C. If key application files are missing when the Planning application starts, the missing files are reinstalled automatically.
D. If the vendor of the Planning application releases a software patch by using a Windows installer package, you can assign (you are able to assign) the patch to only the users who have already installed the application.

Answer: ABCD
Section: (none)

Explanation/Reference:
Explanation:
A: We have configured the Plan App GPO to remove the Planning application therefore no one will be able to install it.
B: The option to allow people to continue to use the app was set.
C: Software deployed in .msi packages can be repaired automatically when key application files are missing or become corrupted. We have not removed the application from the GPO, therefore it can still be repaired.
D: The patch will look for the program on the PCs. If the program exists then the patch will install. If the program does not exist, the patch will not install.

QUESTION 146
You are the administrator of a network that consists of 500 computers. Your network configured as shown in the exhibit.

You are deploying Windows 2000 Professional on the computers in the Tech and Sales Organizational Units (OUs). There is one Windows 2000 Server computer that is running RIS. You create a group named RIS Installer that consists of users from the Tech OU. Only members of RIS installer user group will use RIS to deploy Windows 2000.

You want to accomplish the following goals:

- Members of the RIS installer group will be able to choose client computer names during client computer installation.
- New computer accounts will be organized into the corresponding OUs.
- The company naming convention will be applied to all new computer accounts.
- The computers that are not in either the Tech OU or Sales OU will not be able to download images during RIS deployment.

You take the following actions:

- Create an OU, and then specify the client account location in the RIS properties sheet.
- Enter a custom Client computer naming format in RIS properties sheet.
- Place Mktg computers in a different IP subnet from the Tech and Sales users.

Which result or results do these actions produce? (Choose all that apply)

Exhibit:

A. Members of the RIS installer group can choose client computer names during client computer installation.
B. New computer accounts are organized into their corresponding OUs.
C. The company naming convention will be applied to all new computer accounts.
D. Computers that are not in either the Tech OU or Sales OU cannot download images during RIS deployment.

Answer: BC
Section: (none)

Explanation/Reference:
Explanation:
B: Because we created an OU, and then specified the client account location in the RIS properties sheet, the new computer accounts will be organized into their corresponding OUs.
C: We have entered a custom Client computer naming format in the RIS properties sheet therefore the company naming convention will be applied to all new computer accounts.

Incorrect Answers:
A: Members of the RIS installer group cannot choose client computer names during client computer installation because the naming will be automatic as the naming format was entered into the RIS properties sheet.
D: We have not set any permission on the RIS folder.

QUESTION 147
You are the administrator of your company's Windows 2000 Domain. Your company wants to deploy a custom application named Drawing. To configure the Drawing application, you need to set the custom policy setting in the HKCU\software\policies location in the registry for every user in the domain.

What should you do?

A. Create a Group Policy Object (GPO) named Draw Setting.
Assign the Draw Setting GPO to the domain.
Configure the Draw Settings GPO to run a startup script that changes the appropriate **HKCU\Software\Policies** location in the registry.

B. Create a Group Policy Object named Draw Setting.
Assign the Draw Setting GPO to the domain.
Configure the Draw Settings GPO to run a logon script that changes the appropriate **HKCU\Software\Policies** location in the registry.

C. Create a Group Policy Object named Draw Setting.
Assign the Draw Setting GPO to the domain.
Create a new administrative template that defines the custom policy settings.
Add the new administrative templates to the Draw Setting Group Policy Object.
Configure the Draw Setting GPO to set the appropriate policy.

D. Create a registry file that has the .reg file name extension.
Edit the registry file to change the appropriate **HKCU\Software\Policies** location in the registry.
Place the registry file in the All Users Startup folders of all computers in your domain.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: We can use administrative templates to modify registry settings by adding the template to a GPO and assigning it to the domain. This will change all the registry settings so that we can deploy the application.

Incorrect Answers:
A: We cannot use a startup script to change the registry settings.
B: We cannot use a logon script to change the registry settings.
D: Creating a registry file would require administrative effort. It would be easier to use a GPO.

QUESTION 148
You are deploying Windows 2000 Professional on your network. You recently installed a RIS server to expedite the deployment process. Your network is now configured as shown in the exhibit.

When you attempt to use the RIS server to deploy Windows 2000 on Julia's and Carlos's computer you cannot establish the initial connection. Anita and Peter install Windows 2000 from a CD-ROM and did not have any problems with installation.

What should you do to correct the problem?

A. Integrate the DNS into Active Directory.
B. Install a DHCP server and authorize it in Active Directory.
C. Install a WINS server and configure the DNS server to use it for name resolution.
D. Create computer accounts in Active Directory for Julia and Carlos, and specify the name of the RIS server on the **Remote Install** tab of the **Computer Accounts** property sheet.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: RIS requires a DHCP server and either a DNS server with Active Directory. The DNS server is required for name resolution while RIS requires DHCP as the RIS clients will initially connect at the protocol level. The RIS clients broadcast for a DHCP to provide them with IP configurations. In the exhibit there is both a DNS server and Active Directory but no DHCP.

Incorrect Answers:
A: In the exhibit there is both a DNS server and Active Directory but no DHCP.
C: RIS requires a DHCP server and either a DNS server with Active Directory. The DNS server is required for name resolution. In the exhibit there is both a DNS server and Active Directory but no DHCP
D: RIS requires a DHCP server and either a DNS server with Active Directory. In the exhibit there is both a DNS server and Active Directory but no DHCP.

QUESTION 149
You are the administrator of a Windows 2000 network. Users in the Organizational Unit named Procx need to have a drive mapped to a network location. These users logon from Windows 2000 Professional computers. You want to use a log on script named userlog.cmd to implement this drive mapping for all current and future users in the Procx Organizational Unit. What should you do?

A. Copy user log.cmd to the net logon share on each Domain Controller in the domain. Select the user in the Procx Organizational Unit and set the logon script to the userlog.cmd.
B. Copy user log.cmd to the sysvol share on each Domain Controller in the domain. Assign read permissions to the file for all users in the Procx Organizational Unit.
C. Create a Group Policy Object that enforces userlog.cmd as a logon script. Assign the Group Policy Object to the Procx Organizational Unit.
D. Create a Group Policy Object that enforces userlog.cmd as a start up script. Assign the Group Policy Object to the Procx Organizational Unit.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: By creating a Group Policy object (GPO) that enforces Userlog.cmd as a logon script and assigning this GPO to the Procx OU we will ensure that the GPO will affect all current users and any future users in the Procx OU.

Incorrect Answers:
A: Setting the logon script for each user in the Procx OU would require considerable administrative effort and will have to be performed for all future users of the Procx OU as well. Creating a Group Policy object (GPO) that enforces Userlog.cmd as a logon script and assign this GPO to the Procx OU would require less administrative effort and will ensure that the policy is automatically applied to all future members of the Procx OU as well.
B: In this scenario we have assigned read permission to the Userlog.cmd file for all users in the Procx OU. This will give the users in the Procx OU permission to read the file but will not ensure the implementation of the logon script.
D: In this scenario we require a logon script, not a startup script. A logon script is executed every time a user logs on to the network while a startup script is only executed when the computer starts.

QUESTION 150
You are the administrator of a Windows 2000 network. The domain is named litware.com.

The distinguished name for the Sales organizational unit (OU) is ou=Sales, ou=NorthAmerica, dc=litware, dc=com. You want to assign Andrew the ability to manage all the objects in only the Sales OU.

What should you do?

A. Add Andrew to the Domain Administrators group.
B. Grant Andrew Full Control permission to the North America OU and disable inheritance at the Sales OU.

C. Grant Andrew Read and Write permissions to the Sales OU.
D. Grant Andrew Full Control permission to the Sales OU.
E. Move Andrew's user account to the Sales OU.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: In this scenario we want to assign Andrew the ability to manage all the objects in only the Sales OU. We should thus grant Andrew Full Control permission to the Sales OU. This will allow him to add, modify and remove objects in the Sales OU.

Incorrect Answers:
A: Adding Andrew to the Domain Administrators group would provide Andrew with too much permission.
B: We should grant Andrew the appropriate permission to the Sales OU, not the North America OU.
C: Granting Andrew Read and Write permissions to the Sales OU will allow him to add or modify objects but will not allow him delete objects.
E: Moving Andrew's user account to the Sales OU will not provide with him any rights on the OU. Rights must be granted to users or user groups.

QUESTION 151
Your company's network consists of two domains contoso.com and sports.contoso.com. You are a member of the Domain Admins group in sports.contoso.com

The network contains three Active Directory sites: Site A, site B, and site C. Each site is connected to the other sites by means of a WAN link. Site A contains three Domain Controllers. Site B contains one Domain Controller. Site C contains two Domain Controllers.

The Domain Controller in site B fails. Users in sites A, B, and C report that they cannot log on to the network.

You need to allow users to log on to the network. What should you do?

A. Seize the infrastructure master role from the failed Domain Controller.
B. Seize the RID master ole from the failed Domain Controller.
C. Move a Domain Controller from site C to site B.
D. Create another Domain Controller in site B.
E. Create a Global Catalog server in site A.

Answer: E
Section: (none)

Explanation/Reference:
Explanation: A Global Catalog is required for logon purposes. When the Global Catalog is not available, users will not be able to logon to the network. The only Answer: that could possibly stop people from all sites from logging on is the loss of the Global Catalog server.

Incorrect Answers:
A: The infrastructure master role holds the database of group memberships. It does not affect logons.
B: Seizing the RID master ole from the failed Domain Controller would not affect logons.
C: As users in all sites cannot logon the Global Catalog must be unavailable.
D: Creating another Domain Controller in site B will not solve the problem as the Domain Controllers in other sites are available for use.

QUESTION 152
You are the administrator of your company's Windows 2000 network. The password security on a Domain Controller name DC1 has been compromised.

You create a new security policy to improve password security. You will deploy the policy by using a Group Policy Object. You must force DC1 to apply the new security settings as quickly as possible.

What should you do?

A. Restart DC1 and force Active Directory replication from another Domain Controller.
B. Run Secedit.exe on DC1.
C. Export the configuration of another Domain Controller, and then import the configuration to DC1 by means of the Security Configuration and Analysis snap-in.
D. Perform a nonauthoritative restore the system state data on DC1.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: We can use secedit.exe with the /refresh machine_policy switch to process the GPO with immediate effect.

Incorrect Answers:
A: The GPO would be processed when the computer restarts and a user logs on however the secedit command can be used to apply the policy without the requirement to restart the computer or to logon to the network.
C: We need to refresh a GPO, to change the security settings. The other Domain Controller may not have the GPO applied yet therefore importing the configuration of another Domain Controller will not result in the policy being applied immediately.
D: A nonauthoritative restore will restore an old security configuration.

QUESTION 153
You are the administrator of your company's Windows 2000 domain. Your company wants to deploy a custom application. To configure the application, you need to configure a registry value in the HKEY Current User (HKCU) hive of the registry.

You create a Group Policy Object, and then link the GPO to the domain. You need to complete the configuration.

What should you do?

A. Configure the GPO to run a startup script that changes the appropriate HKCU\Software\Policies location and value in the registry.
B. Configure the GPO to run a logon script that modifies the NTuser.dat file.
C. Create a new administrative template that defines the custom policy setting.
Add the template to the GPO, and then configure the GPO to set the appropriate policy.
D. Use the Security Configuration and Analysis snap-in to create a custom template.
Configure the GPO to import the custom template.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: We can use administrative templates to modify registry settings by adding the template to a

GPO and assigning it to the domain. We can then distribute these templates with a GPO.

Incorrect Answers:
A: We cannot use a startup script to modify registry settings.
B: We cannot use a logon script to modify registry settings.
D: Creating a custom template would require considerable administrative effort and have to be done on each computer. The process can however be automated through the use a GPO.

QUESTION 154
Your company's network consists of a single Windows 2000 Domain. The domain is located in an Active Directory site named New York. You are a member of the Domain Admins group.

Two Group Policy Objects (GPOs) are linked to sales.contoso.com. One GPO removes the Run command from the Start menu. The other GPO removes the Search command from the Start menu.

Two GPOs are linked to the New York site. One GPO disables Control Panel. The other GPO hides all icons that are on the desktop.

After the users log on and begin working with an application, they report that their desktop icons disappear, Control Panel is disabled, and the Run and Search commands are not visible.

You want to ensure that Control Panel is disabled and that desktop icons are removed when users log on but before they start working. What should you do?

A. Disable asynchronous policy processing
B. Disable background refresh policy processing
C. Enable Group Policy Loopback processing in merge mode.
D. Enable Group Policy Loopback processing in replace mode.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Apparently the GPO that removes the desktop icons is not processed until after the desktop is visible. This behavior can occur when asynchronous policy processing has been enabled. If we disable asynchronous policy processing we assure that all GPOs will be processed before the desktop becomes visible and the users will not see disappearing desktop icons.

Note: Synchronous and Asynchronous Processing

Asynchronous refers to processes that do not depend on each other's outcome, and can therefore occur on different threads simultaneously. The opposite is synchronous. Synchronous processes wait for one to complete before the next begins. For those Group Policy settings for which both types of processes are available as options, you choose between the faster asynchronous or the safer, more predictable synchronous processing.

By default, the processing of Group Policy is synchronous. Computer policy is completed before the CTRL +ALT+DEL dialog box is presented, and user policy is completed before the shell is active and available for the user to interact with it.

Reference: Windows 2000 Resource Kit, Group Policy, Group Policy Processing Loopback Processing of Group Policy (Q231287)

Incorrect Answers:
B: If we disable background refresh policy processing we prevent Group Policies from being updated while the

computer is in use. This would not make an impact how GPOs are applied though.

C, D: You can use the Group Policy loopback feature to apply Group Policy Objects (GPOs) that depend only on which computer the user logs on to. This would not help in this scenario though. We have a problem with the asynchronous processing of GPOs.

QUESTION 155
You are the administrator of your company's Windows 2000 network. The network contains 350 computers running Windows 95 and 700 computers running Windows 2000 Professional. You need to upgrade all Windows 95 computers to Windows 2000 Professional in the next six months.

You configure the DNS servers in the network to allow secure dynamic updates. You use DHCP to configure network settings for all client computers. You configure the DHCP servers to update the A (host) records for the Windows 95 computers in DNS.

After the upgrade is complete, you need to ensure that client computers can update their own A (host) records in DNS. What should you do?

A. Install the Active Directory client on the Windows 95 computers before the upgrade
B. Reconfigure the TCP/IP settings on the Windows 95 computers so that the DNS settings must be set manually and so that the IP addresses are set by DHCP
C. Add all the users of the Windows 95 computers to the DNSUpdateProxy group in Active Directory
D. Add all DHCP servers to the DNSUpdateProxy group in Active Directory

Answer: D
Section: (none)

Explanation/Reference:
The DHCP server that registered a specific Windows 95 client computer will own that record. In order to allow the Windows 95 clients to register their records in DNS we must add the DHCP servers to the DNSUpdateProxy group.

Note: Installation of DNS will extend the Active Directory schema to include the DNSUpdateProxy group. This is a very powerful group that allows objects to be created that has no security. When this occurs, any authenticated user can take ownership of those objects created in this manner.

Client records A and PTR are updated in DNS during the DHCP process in Windows2000. When both clients and servers are Windows2000, then secure dynamic updates can be completed using a default installation. When other clients need to be supported, then secure dynamic updates cannot be used unless the DHCP Server is added to the DNSUpdateProxy group. This allows the DHCP server to perform dynamic updates for these legacy clients.

Incorrect Answers:
A: Installing the Active Directory client on the Windows 95 clients before the upgrade to Windows 2000 will not help with this DNS registration problem.
Note: The Active Directory features supported in the Active Directory client for Windows 95/98 are:
- Site awareness.
- Active Directory Service Interfaces (ADSI).
- DFS fault tolerance client.
- Active Directory Windows Address Book (WAB) property pages
- NTLM version 2 authentication.

B: Setting the DNS setting on the clients to manual will do more harm than good.
C: DHCP servers, not client computers, should be added to the DNSUpdateProxy group.

QUESTION 156
You are the administrator of your company's Windows 2000 network. The network consists of a main office and three branch offices. Each office contains a Windows 2000 DNS server.

Users in a branch office report slow response times when they log on to the network. You want to discover why network response times are slow. You must configure the Windows 2000 DNS server to collect the necessary data for this analysis.

What should you do?

A. On the DNS server in the branch office, configure System Monitor to log the data on the **Total Query Received** counter and the **Total Response Sent** counter.
B. On the DNS server in the branch office, configure System Monitor to log the data on the **IXFR Success Sent and Received** counter and the **AXFR Success Sent and Received** counter.
C. In the DNS server snap-in, configure the DNS server in the branch office to log only notification and update messages
D. In the DNS server snap-in, configure the DNS server in the branch office to log only the question packets and the answer packets

Answer: B
Section: (none)

Explanation/Reference:
Explanation: The remote users report slow response time when they log on the network. This might be an indication that they use the central DNS server and not the branch DNS servers. The reason for this could a problem with zone transfers. We should therefore configure the system monitor to log data on the **IXFR Success Sent and Received** counter and the **AXFR Success Sent and Received** counter. These counters will measure zone transfer traffic.

Note: IXFR (RFC 1995), Incremental zone transfer, sends only the changes in the zone. AXFR zone transfers sends the whole zone. IXFR are more effective than AXFR.

Reference: IXFR RFC 1995

Incorrect Answers:
A, C, D: We should measure the zone transfer traffic.

QUESTION 157
You are the administrator of your company's Windows 2000 network. The network consists of a single domain. The domain contains three Active Directory sites. Each site contains one domain controller. You install an additional domain controller in each site. You want only the new domain controllers to perform intersite directory replication.

What should you do?

A. Configure each existing domain controller to be the preferred bridgehead server for its site.
B. Create a connection object from the existing domain controller in each site to the new domain controller in the other sites.
C. Create a connection object from the new domain controller in each site to the existing domain controller in each site.
D. Configure each new domain controller to be the preferred bridgehead server for its site.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: We configure the new domain controllers to be preferred bridgehead servers. All intersite replication will go through these servers.

Note: In Windows 2000 Server, bridgehead servers are the contact point for the exchange of directory information between sites. A bridgehead server is a domain controller that has been either administratively assigned or automatically chosen to replicate changes collected from other domain controllers in the site to bridgehead servers in other sites.

Reference: Description of Bridgehead Servers in Windows 2000 (Q271997)

Incorrect Answers:
A: The new domain controllers, not the old existing domain controllers, should be configured as preferred bridgehead servers.
B, C: A connection object would not enforce communication between specific servers. It would only define a possible communication path.

QUESTION 158
You are the administrator of your company's Windows 2000 network. The network contains 500 computers running Windows 2000 Professional. Each computer uses DHCP to acquire its network settings.

You discover that outdated DNS records are accumulating in the DNS zone. You need to ensure that these records are removed from DNS on a regular basis.

What should you do?

A. Configure DHCP to enable updates for DNS client computers that do not support dynamic updates
B. Reconfigure the DNS zone to allow only secure dynamic updates
C. Configure record scavenging to poll the DNS zone
D. Add all client computers to the DNSUpdateProxy group

Answer: C
Section: (none)

Explanation/Reference:
Explanation: Scavenging is the process that removes stale records from a DNS zone. The idea behind aging and scavenging is to remove records that haven't been refreshed within a certain interval. If we schedule regular scavenging of the DNS zone the outdated DNS records will be removed.

Incorrect Answers:
A: All clients are Windows 2000 computers. Windows 2000 clients support dynamic updates so there is no need to configure DHCP to enable updates for clients that don’t support dynamic updates.
B: This is a DNS record problem, not a security problem.
D: It is not necessary to add client computers to the DNSUpdateProxy group. Only DHCP servers should be added to the DNSUpdateProxy group.

QUESTION 159
You are the administrator of your company's Windows 2000 network. The network consists of a single domain, which contains all company user and computer accounts.

A new corporate policy states that no employee can have access to the network by means of dial-up connections. You discover that some employees have configured their Windows 2000 Server computers as remote access servers.

You want to ensure that employees cannot configure their computers to user Routing and Remote Access.

What should you do first?

A. Configure the Default Domain Group Policy Object (GPO) to disable the Routing and Remote service.
B. Create a remote access policy that allows only approved Routing and Remote access servers to establish connections.
C. Configure the Default Domain Group Policy Object (GPO) to prohibit the configuration of connection sharing.
D. Configure the Default Domain Group Policy Object (GPO) to prohibit the connecting and disconnecting of a remote access connection.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: We should configure the Default Domain GPO to disable the RAS service. This would prevent the RAS service starting anywhere throughout the domain.

Reference: Microsoft: Step-by-Step Guide to Configuring Enterprise Security Policies

Incorrect Answers:
B: Remote access policies only decide which connections are allowed to be established to a particular RAS server. It would not prevent the RAS service from being installed on other computers.
C: Internet connection sharing is not the same thing as the Remote Access Service.
D: There is no such GPO setting that can prohibit connecting and disconnection of a remote access connection.

QUESTION 160
Your company's network consists of a single Windows 2000 Domain. You are a member of the Domain Admins group. All user and computer accounts belong to a group named SalesGroup and to an Organizational unit (OU) named SalesOU.

A vendor provides you with an application that contains a Setup.exe file. You need to deploy the application to the sales department by using the least amount of administrative effort.

What should you do?

To answer, click the select and place button, and then drag the appropriate object to the appropriate destination.

Answer:

Section: (none)

Explanation/Reference:
References:
How to Publish non-MSI Programs with .zap Files (Q231747)
How to Deploy Software to a Specific Group By Using a Group Policy (Q302430)

Incorrect Answers:
We cannot assign a non-msi file.
We cannot transform or use an .exe setup file as an MSI package.
We cannot deploy the application to a group. We must use a GPO and link it to an OU, a domain, or a site.
A non-msi file cannot be deployed to computers.

QUESTION 161
You are the administrator of your company's Windows 2000 network. The network consists of four domains and five Active Directory sites. The network is configured as shown in the exhibit.

Each domain contains 500 Windows 2000 Professional computers. Five users in each domain are authorized to access data on the Human Resources member servers in Alabama. These member servers are located in an organizational unit named HR servers.

You want to protect the information on the Human Resources servers from being read by a network trace. You also want to avoid extra processing loads on computers that do not communicate with the Human Resources servers.

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

Exhibit:

A. In each domain, create an OU for the client computers that require secured access to the servers, and then add the computer accounts to the OU. In Group Policy, set the IP security policy to **Secure server (Require Security).**
B. In each domain, create an OU for the client computers that require secured access to the servers, and then add the computer accounts to the OU. In the Group Policy, set the IP security policy to **Client (Respond only)**
C. In each domain, create an OU for the users who require secured access to the servers, and then add the user accounts to the OU. In the Local Group Policy, set the IP security policy to **Secure Server (Require Security)**
D. For the HR Servers OU, create a Group Policy Object (GPO) that sets IP security to **Client (Respond Only)**
E. For the HR Servers OU, create a Group Policy to set IP security to **Secure Server (Require Security)**

Answer: BE
Section: (none)

Explanation/Reference:
Explanation:
B: The computers that need to communicate with the Servers in the OU HR servers should be configured for the IP security policy of **Client (Respond only)**. If they communicate with computers that require IP security they will respond with IP security. If they communicate with computer that doesn't require IP security no IP security will be applied.

E: All traffic to and from the servers in the HR Servers OU must be secure so no network sniffer (network trace) can compromise security. In order to implement this security we must configure the IP security to **Secure Server (Require Security)** which will enforce encryption on all communication. All non-encrypted access attempts will be denied.

Incorrect Answers:
A: Only traffic to and from the servers in the HR Server OU should require security.
C: The computers, not the users, should be configured for IP security.
D: The computers in the HR Servers OU require security; all communication to and from these computers must be encrypted.

QUESTION 162
You are the administrator of a secured Windows 2000 network. The company has several Windows 2000 member servers located in a high-security area of the office building.

You create a security policy for these servers by using the Security Configuration and Analysis snap-in. You must ensure that the appropriate security settings are applied every four hours.

What should you do?

A. Schedule the **secedit /refreshpolicy** command to run every four hours.
B. Schedule the **secedit /validate** command to run every four hours.
C. Change the Active Directory replication transport to SMTP and schedule replication to run every four hours.
D. Change the Active Directory replication transport to IP and schedule replication to run every four hours.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: GPOs are normally propagated throughout the domain at regular intervals. By using the command **secedit /refreshpolicy** GPOs can be enforced immediately. We schedule a reoccurring job that uses this command to ensure that the servers have the appropriate security settings.

Incorrect Answers:
B: The **secedit /validate** command validates the syntax of a security template you want to import into a database for analysis or application to a system. It does not apply a security policy.

C, D: The servers are located in an office building. Active Directory replication is of no use in this scenario,

Reference: Using Secedit.exe to Force Group Policy to Be Applied Again (Q227448)

QUESTION 163
You are a consultant hired by Fabrikam, Inc. to secure its Windows 2000 network. The network consists of a single domain named fabrikam.com. The domain contains five domain controllers.

You need to secure the domain controllers. You use the security templates snap-in to create a custom template, and you save the template as Securefab.inf. You need to deploy this secured configuration to the five domain controllers.

What should you do? (Choose all that apply.)

A. Copy the Securefab.inf file to the Sysvol shared folder on one domain controller.
B. Configure the File Replication service to replicate the template file to all domain controllers.

C. Create a new Group Policy Object (GPO) on the domain Controllers Organizational unit (OU).
D. Import the Securefab.inf file

Answer: CD
Section: (none)

Explanation/Reference:
Explanation: Security policies can either be applied with the secedit command or through a GPO.
C: First we create a new GPO and link it to the domain Controllers OU since we want the security policy to apply to all domain controllers throughout the domain.
D: Then we import the security template to the GPO.

Incorrect Answers:
A: Sysvol is not used to deploy security templates.
Note: The Windows 2000 System Volume, or SYSVOL, is built during the creation of a domain controller by Dcpromo.exe. It is a tree of folders containing files that need to be available and synchronized between domain controllers in a domain or forest, including:

- SYSVOL share.
- NETLOGON share.
- Windows 95, Windows 98, and Windows NT 4.0 system policies.
- Windows 2000 Group Policy settings.
- User logon and logoff scripts.

B: File replication services (FRS) is used to replicate files. Security templates replicated through FRS would not be applied.

QUESTION 164
You are the administrator of your company's Windows 2000 network. The network consists of a single DNS domain named litware.com. The domain contains one Windows 2000 Domain controller named WinServer1, one UNIX server named UnixServer1, and 750 Windows 2000 Professional computers. UnixServer1 is running BIND DNS and contains the primary zone for the litware.com zone.

You install a new domain controller named Server2 in the network. However, no client computers are logging on to the new domain controller. You run the Nslookup utility from a client computer. You receive the following results:

```
C:\nslookup
Default Server: unixserver1.litware.com
Address: 10.0.0.1
> set type=srv
> _ldap.tcp.dc.msdcs.litware.com
Server: winserver1.litware.com
Address: 10.0.0.2
Idap.tcp.dc.msdcs.litware.com SRV service location:
Priority = 0
Weight = 0
Port =389
Svr hostname =winserver1.litware.com
Winserver1.litware.com internet address = 10.0.0.2
> exit
C:\>
```

You need to enable the client computers to log on to Server2. How should you configure Server2?

A. Change the TCP port for the LDAP service from 389 to 390

B. Copy the Netlogon.dns file to UnixServer1. Import the Netlogon.dns file to the primary zone on Unixserver1
C. Install DNS and create a secondary zone for litware.com. Import the Root.dns file to the secondary zone.
D. Change the Internet Address of the A (host) record to a public IP address

Answer: B
Section: (none)

Explanation/Reference:
Explanation: In this scenario we must use the UNIX BIND DNS server to provide name resolution for the Windows 2000 computers. Every Windows 2000 DC has a Netlogon.dns file located in its %SystemRoot% \System32\Config folder. This file contains a list of DNS records that the DC will attempt to register when the Netlogon service starts. The DNS records in the Netlogon.dns file must be added in the zone of the BIND DNS server.

Reference: Integrating Windows 2000 DNS into an Existing BIND or Windows NT 4.0-Based DNS Namespace (Q255913)

Incorrect Answers:
A: Port 389 can very well be used by the LDAP service.
C: We must export records to the UNIX BIND servers in order to be able to use the netlogon service. Importing the Root.dns file to the secondary server will not accomplish this goal.
D: Winserver1 has a perfectly good IP address of 10.0.0.2. The UNIX BIND DNS server has the address 10.0.0.1 which is in the same subnet.

QUESTION 165
You are the administrator of the Windows 2000 network at Woodgrove Bank. The network has Active Directory installed and contains a DNS server named Server01. The network is configured as shown in the exhibit. Click the exhibit button.

All client computers in the network are configured to use Server01 as their DNS server. The client computers can connect to Internet sites by using IP addresses. However, they cannot use Internet host names or domain names to connect to internet sites.

You need to enable Internet name resolution for the client computers. How should you configure Server01?

Exhibit:

A. Remove the root domain zone and restart the DNS server service. Configure forwarders to point to the DNS servers at the company's Internet service provider.
B. Add the DNS servers at the company's Internet Service Provider (ISP) to the **Name Servers** configuration tab in the root domain.
C. Add the DNS servers at the company's Internet Service Provider to the top of the DNS server order list in the TCP/IP properties on Server01.
D. Clear the DNS cache, and then restart the DNS server service.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Server01 resolves local names. In order for it to resolve internet names it must use a public DNS server as a forwarder. First we must remove the empty root domain zone, and then we must configure Server01 to forward external name resolution to DNS server at the ISP.

Incorrect Answers:
B: The DNS server listed in the **Name Servers** configuration tab in the root domain are secondary name servers of the root domain. But we must configure a forwarder not a secondary DNS server.
C: We must add the external DNS server as a forwarder at the local DNS server. We cannot use the TCP/IP properties on Server01 to configure it as a forwarder.
D: We must configure the DNS server to use a public DNS server as a forwarder. Clearing the local DNS cache will not help.

QUESTION 166
You are the administrator of a Windows 2000 network. Your company has three locations in North America and three locations in Europe. Your network includes six sites as shown in the exhibit.

The England, France, and Italy sites are in the eur.blueskyairlines.com domain. The NorthWestUS, CentralUS, and NorthEastUS sites are in the na.blueskyairlines.com domain. The root of the forest is blueskyairlines.com.

The connection between the NorthEastUS site and the England site is unreliable. You want to configure replication between the NorthEastUS site and the England site.

What should you do?

Exhibit:

A. Create an SMTP site link between the NorthEastUS site and the England site.
B. Create an IP site link between the NorthEastUS site and the England site.
C. Create an SMTP site link bridge between the NorthEastUS site and the England site.
D. Create an IP site like bridge between the NorthEastUS site and the England site.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Simple Mail Transfer Protocol (SMTP) is an Internet standard host-to-host mail transport protocol that and operates over TCP port 25. When the network connection is interrupted, SMTP queues network packets and attempts to send the packets later. SMTP is the best protocol to use across unreliable network links.

Incorrect Answers:

B: IP site links should only be used on reliable connections, as it does not queue up network packets that were not deliverable. Instead these packets are lost and thus replication will not be successful.
C: By default, when more than two sites are linked for replication and use the same transport protocol; the site links are "bridged". This means that all site links within the bridge can route replication traffic only within the bridge. We thus do not require a site link bridge.
D: By default, when more than two sites are linked for replication and use the same transport protocol; the site links are "bridged". This means that all site links within the bridge can route replication traffic only within the bridge. We thus do not require a site link bridge.

QUESTION 167
You are the administrator of your company's Windows 2000 network. The network contains two Active Directory sites: Munich and Singapore. The network also consists of two domains: fabrikam.com and asia.fabrikam.com. The network is configured as shown in the exhibit.

Users from the Singapore office often travel to the Munich office with their portable computers. When these users log on to the network from Munich, their computers display the text "Applying your personal settings" for a long time.

You want to ensure that users from Singapore do not experience these delays when they log on to the network from Munich.

What should you do?

Exhibit:

A. Associate the Munich subnet with the Singapore site.
B. Create a trust relationship so that fabrikam.com trusts asia.fabrikam.com.
C. Install a domain controller for asia.fabrikam.com in the Munich subnet.
D. Use the Active Directory Sites and Services snap-in to move DC3 to the Munich site.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: When the users from Singapore log on at Munich their personal settings are downloaded from Singapore. Due to the slow WAN link, this procedure causes long delays. By adding a domain controller for asia.fabrikam.com in the Munich subnet, these logins could be processed locally at Munich and the logon delays would disappear.

Incorrect Answers:
A: A site should be a well-connected TCP/IP network. Munich is only connected to Singapore with a slow WAN link and should therefore not be included in the Singapore site.
B: Fabrikam.com and asia.fabrikam.com are in the same domain tree and there already exists a two-way implicit trust between the domains by default since this is a Windows 2000 network. There would be no need to create any explicit trusts between the domains.
D: DC3 is physically placed in the Singapore subnet. To logically move it to Munich site would not increase performance, on the contrary it would most likely increase traffic on the WAN link and performance would decrease. Computers should only be added to the site to which their subnet belongs.

QUESTION 168
You are a member of the Enterprise Admins group for your company's Windows 2000 network. The network consists of a single domain. You want to implement a policy that disables the Add Printer icon in Printers in Control Panel. You want to apply the policy to all user accounts in the domain except for members of the Domain Admins security group.

You create a new Group Policy object (GPO) named NoPrinters. You configure the NoPrinters GPO to disable the Add Printer icon. You link the NoPrinters GPO to the domain.

You want to ensure that members of the Domain Admins group have access to the Add Printer icon. You want to do this by using the least amount of administrative effort.

What should you do?

A. For the NoPrinters GPO, deny the Domain Admins group the Apply Group Policy permission.
B. For the NoPrinters GPO, remove the Apply Group Policy permission from the Authenticated Users group. Grant the Users group the Apply Group Policy permission.
C. Use the **Secedit** command to configure the client computers to enable the **Add Printer** icon for the Domain Admins group.
D. Use local Group Policy to configure the client computers to enable the **Add Printer** icon for the Domain Admins group.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Denying the Apply Group Policy permission on a GPO for a group, will prevent the GPO from being applied to that group. The Deny permission will override any other permission granted on the GPO.

In this scenario we deny the Domain Admins groups the Apply Group Policy permission to the NoPrinters GPO.

Incorrect Answers:
B: By removing the Apply Group Policy permission on the NoPrinters GPO from the Authentication Users, this GPO would not be applied to any users (unless they get this permission explicitly or by membership of another group that has this permission). But the GPO must be applied to all users except the Domain Admins.
C: It would take considerable administrative effort to configure the client computers to apply a policy with the **Secedit** command-line utility. . It is better to configure this centrally by configuring a GPO for the domain.
Note: secedit is a command-line tool that allows you to perform security configuration and analysis.
D: It would be a daunting administrative task to configure all client computers with Local Group Policies. It is better to configure this centrally by configuring a GPO for the domain.

QUESTION 169
You are the administrator of your company's Windows 2000 network. The network contains two Windows 2000 domain controllers. You are configuring an audit policy for the company help desk. The help desk has two employees: Carlos and Julia. Carlos is authorized to create and delete computer accounts. Julia is authorized to change user account information.

You want to track the changes that Carlos and Julia are authorized to make in the domain. What should you do?

A. Create a Group Policy Object (GPO) for the domain controllers.
Configure the GPO to audit directory services access and to audit account management.
B. Create a Group Policy Object (GPO) for the domain.
Configure the GPO to audit directory services access and to audit object access.
C. Create a Group Policy object (GPO) for the domain controllers.
Configure the GPO to audit directory services access and to audit object access.
D. Create a Group Policy Object (GPO) for the domain.
Configure the GPO to audit object access and to audit process tracking.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: We want to track the changes Carlos and Julia make in the domain or more specifically what changes they make to the Active Directory. Configuring computer accounts and changing user account

information involves changing the Active Directory. The Active Directory only exists on the Domain Controllers and we should therefore audit the Domain Controllers. By auditing the directory services access and account management we would be able to track the changes Carlos and Julia make to the Active Directory.

Note:
Directory services audits the following events: a user gained access to an Active Directory object. You must configure specific Active Directory objects for auditing to log this type of event Account management audits the following events: an administrator created, changed, or deleted a user account or group. A user account was renamed, disabled, or enabled, or a password was set or changed.

Incorrect Answers:
B: We should audit the domain controllers, not the domain.
There is no need to audit object access. Object access concerns file, folder, and print access, instead we should audit account management.
C: There is no need to audit object access. Object access concerns file, folder, and print access, instead we should audit account management.
D: We should audit the domain controllers, not the domain. There would be no need to audit object access. Object access concerns file, folder, and print access. There is no need to track programs and processes. Instead we should audit directory services access and account management.

QUESTION 170
You are the administrator of your company's Windows 2000 network. The network consists of a single domain. Several DNS servers at the company's main office host the domain name. Each DNS server contains an Active Directory integrated zone for the domain.

You are configuring a new Windows 2000 DNS server at a branch office. The branch office will not have its own domain controller. However, you want the new DNS server to provide name resolution when users at the branch office log on to the domain. You must configure the new DNS server to communicate with the main office for this purpose.

How should you configure the new DNS server?

A. Create a root zone, and then configure the server to allow zone transfers by specifying the DNS servers at the main office.
B. Disable round robin, and then create a standard primary zone for the domain.
C. Disable recursion, and then create a reverse lookup zone. Add PTR (pointer) records for the DNS servers at the main office.
D. Create a secondary zone for the domain, and then configure the DNS servers at the main office as the master servers for the new zone.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: The DNS servers at the branch offices must be configured to exchange zone information with the DNS servers at the main offices which use Active Directory integrated zones. We cannot use Active Directory integrated zones at the branch offices since they have no domain controllers. Instead we create secondary zones at the branch offices and we configure the DNS servers at the main offices as Master Servers. They are authoritative for the zone and the branch office DNS servers will not be able to update the zones. This was not a requirement however.

Furthermore we should configure the clients in the branch offices to use the local DNS server.

Incorrect Answers:
A: Creating a root zone would allow zone transfers between the DNS servers. Instead we should create a

secondary zone.
B: An Active Integrated zone and a primary zone would not be able to exchange zone information. Both must be authoritative for the zone.
C: Disabling recursion and creating a reverse lookup zone would not enable communication of zone information between the DNS servers.

QUESTION 171
Your company's network consists of two Windows 2000 domains: contoso.com and sales.contoso.com. The contoso.com domain contains three domain controllers: dc1.contoso.com, dc2.contoso.com, and dc3.contoso.com. The sales.contoso.com domain contains two domain controllers: salesdc1.contoso.com and salesdc2.contoso.com. You are a member of the Domain Admins group in sales.contoso.com.

You create 100 new user accounts in sales.contoso.com. These new users report they cannot log on to sales.contoso.com.

What is the most likely cause of this problem?

A. All bridgehead servers in the forest are offline.
B. All global catalog servers in the forest are offline.
C. The server in contoso.com that is holding the PDC emulator role is offline.
D. The server in sales.contoso.com that is holding the PDC emulator role is offline.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: We have recently created 100 new user accounts in sales.contoso.com. These users are unable to log on to the sales.contoso.com domain. The PDC emulator is the first domain controller to receive password changes made at other domain controllers in the domain. The PDC emulator acts somewhat like a PDC in an NT 4.0 domain, and is responsible for the authentication of domain users. A likely cause of this problem is that the PDC emulator of the current domain, sales.contoso.com, is offline.

Note 1: The PDC emulator receives preferential replication of password changes performed by other domain controllers in the domain. If a password was recently changed, that change takes time to replicate to every domain controller in the domain. If a logon authentication fails at another domain controller due to a bad password, that domain controller will forward the authentication request to the PDC emulator before rejecting the logon attempt.

Note 2: The PDC emulator role is used both in mixed mode (domain that contains NT 4.0 domain controllers) and in native mode (only Windows 2000 domain controllers).

Reference: Windows 2000 Active Directory FSMO Roles (Q197132)

Incorrect Answers:
A: Bridgehead servers are used to improve the performance of inter-site communication. Offline bridgehead servers would decrease performance, but it would not prevent domain authentication.
B: Global catalog servers are not used for authentication.
C: The user accounts belong to the sales.contoso.com domain, not the contoso.com. The PDC emulator of the contoso.com domain is not used to authenticate users in the sales.contoso.com domain.

QUESTION 172
You are the administrator of your company's Windows 2000 domain. The domain contains an organizational unit (OU) named Receptionists. All users in the Receptionists OU use an application named PatientID.

The PatientID application is deployed by means of a Group Policy object (GPO) named PatientApp. The PatientApp GPO is configured to publish the PatientID application by using Microsoft Windows Installer package.

Currently, only users in the Receptionists OU can install the PatientID application. You want all users in the domain to be able to install the PatientID application by using a Start menu shortcut.

What should do?

A. Remove the PatientApp GPO link to the Receptionists OU.
   Link the PatientApp GPO to the domain, and then configure the GPO to assign the PatientID application to users.
B. Remove the PatientApp GPO link to the Receptionists OU.
   Link the PatientApp GPO to the domain, and then configure the GPO to publish the PatientID application to users.
C. Configure the PatientApp GPO to assign the PatientID application to the Authenticated Users group.
D. Configure the PatientApp GPO to assign the PatientID application to the Everyone group.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: We want all the users in the domain to be able to start the PatientID application by using a shortcut on the Start menu. We should make sure the GPO assigns the application to users. Then we should link the GPO to the domain. We could also remove the redundant link to the GPO at the Receptionist OU.

Incorrect Answers:
B: We must assign the application, not publish it, in order to allow installation of the application from a shortcut on the Start menu.
C: We must link the GPO to the domain in order for it to apply to all users of the domain. If we keep the GPO linked to the Receptionists OU only users in this OU would be able to use the application.
D: We must link the GPO to the domain in order for it to apply to all users of the domain. If we keep the GPO linked to the Receptionists OU only users in this OU would be able to use the application.

QUESTION 173
Your company's network consists of two Windows 2000 domains: contoso.com and sales.contoso.com. You are a member of the Domain Admins group in sales.contoso.com. You are located in the company's New York office.

The contoso.com domain contains three domain controllers: dc1.contoso.com, dc2.contoso.com, and dc3.contoso.com. The sales.contoso.com domain contains two domain controllers: sales1.contoso.com and salesdc2.contoso.com.

Salesdc1.contoso.com is in an Active Directory site named New York. Salesdc2.contoso.com is an Active Directory site named Los Angeles. Every night a full backup is performed on all domain controllers. Replication between New York and Los Angeles occurs once a day.

The employees in the Finance department are members of an organizational unit (OU) named Finance. The Finance OU is contained in sales.contoso.com. You link a Group Policy Object (GPO) named DeskLock to the OU. The DeskLock GPO removes the Run command from the Start menu.

You delete all existing accounts and create 100 new user accounts in the Finance OU. The next day, the new users report that they have access to the Run command on the Start Menu. You discover that an Administrator in Los Angeles deleted the Finance OU.

You want to recover the new user accounts as quickly as possible. What should you do?

A. Perform an authoritative restore of the Finance OU from backup tape.
   Link DeskLock to the Finance OU.
B. Perform a nonauthorative restore of all user accounts in sales.contoso.com from backup tape.
   Re-create the Finance OU in sales.contoso.com and move the restored user accounts to the Finance OU.
   Link DeskLock to the Finance OU.
C. Re-create the Finance OU in sales.contoso.com.
   Move the accounts from the LostAndFound folder to the Finance OU.
   Link DeskLock to the Finance OU.
D. Re-create the Finance OU in the LostAndFound folder.
   After the next replication cycle, move the Finance OU to sales.contosol.com.
   Link DeskLock to the Finance OU.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: An administrator deleted the Finance OU which contained 100 user accounts. The GPO DeskLock was linked to the Finance OU. In order to recreate the Finance OU we must perform an authoritative restore of the OU. We must also link the DeskLock GPO to the restored Finance OU.

Incorrect Answers:
A: We should perform an authoritative restore, not a non-authoritative restore. A non-authoritative restore of Active Directory objects would not be replicated throughout the domain. At the restored objects would be removed at the next Active Directory replication.
C: The LostAndFound container contains objects that are orphaned. They are produced when objects are unsuccessfully moved in the Active Directory. If the move fails for some objects they end up in the LostAndFound container. Deleted objects are not moved to the LostAndFound container.
D: The LostAndFound container contains objects that are orphaned. They are produced when objects are unsuccessfully moved in the Active Directory. If the move fails for some objects they end up in the LostAndFound container. We cannot recreate the Finance OU in the LostAndFound folder.

QUESTION 174
You are the administrator of your company's Windows 2000 network. The network consists of a single domain. The domain contains two Windows 2000 DNS servers and one UNIX server that is running BIND DNS. The UNIX server contains the primary zone for the domain.

You configure both Windows 2000 DNS servers as domain controllers. You convert the zones on the servers to Active Directory integrated zones. You want to ensure that DNS record changes on these Windows 2000 DNS servers are replicated to the UNIX server.

What should you do?

A. On the UNIX server, delete the primary zone, and then create a new secondary zone that is linked to a Windows 2000 DNS server.
B. On the UNIX server, import the contents of the Netlogon.dns file from each Windows 2000 DNS server.
C. On each Windows 2000 DNS server, enable forwarding to the UNIX server.
D. On each Windows 2000 DNS server, configure zone transfers to send zone update notifications to the UNIX server.

Answer: A
Section: (none)

Explanation/Reference:

Explanation: The Windows 2000 DNS servers use Active Directory Integrated zones. These servers are authoritative for the zones. Currently the UNIX BIND DNS server contains a primary zone for the domain. A DNS server that hosts a primary DNS zone is authoritative for the zone. Both the Windows 2000 DNS servers and the UNIX DNS server cannot be authoritative for the same zone at the same time. We must delete the primary zone at the UNIX server, and create it as a secondary zone to the Active Directory integrated zone on the Windows 2000 DNS servers.

Reference: Integrating Windows 2000 DNS into an Existing BIND or Windows NT 4.0-Based DNS Namespace (Q255913)

Incorrect Answers:
B: Every Windows 2000 DC has a Netlogon.dns file located in its %SystemRoot%\System32\Config folder. This file contains a list of DNS records that the DC will attempt to register when the Netlogon service starts. Copying this file to the UNIX DNS server would only make sense if the UNIX DNS server were authoritative for the zone. But since the Windows 2000 DNS servers use Active Directory Integrated zones they must be authoritative for the zones.
C: We must configure zone transfers, not forwarding. We must recreate the zone on the DNS server as a secondary zone.
D: We cannot configure Active Directory Zones and Primary Zones to perform zone transfers. Both cannot be authoritative for the zone.

QUESTION 175
You are the administrator of your company's Windows 2000 network. The network contains 5,000 computers running Windows 95 or Windows 2000 Professional. All client computers use DHCP to obtain their TCP/IP configuration. The DHCP servers update the DNS records for the Windows 95 computers. The DHCP lease duration for all client computers is set to 30 days.

You enable ageing and scavenging of DNS records in the domain. Some users report that they cannot access files on other user's computers. You examine the DNS zone for the domain and discover that the A (host) records for the Windows 95 computers are disappearing from the DNS servers after two weeks.

You need to ensure that the A (host) records for all client computers remain on the DNS servers for the duration of the DHCP lease. What should you do?

A. On the DHCP servers, set the DHCP lease duration to 60 days.
B. On the DNS servers, set the No-Refresh interval to 5 days.
C. On the DHCP servers, set the BOOTP lease duration to 30 days.
D. On the DNS servers, set the Refresh interval to 10 days.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: DNS scavenging is disabled by default. In this scenario DNS scavenging is enabled and combined with the long DHCP lease time of 30 days it brings undesired effects: the A (Host) records of the Windows 95 client computers disappear after two weeks.

This is a DNS zone configuration problem. After A (host) records are dynamically registered in a DNZ zone, there follows a **No-Refresh interval**, default value 7 days, when the record cannot be refreshed. After this interval there follows a **Refresh Interval**, default value 7 days, when the records are allowed to be refreshed. In this scenario the DHCP lease time is 30 days (default 8 days), and the DHCP server will try to renew the lease after 15 days (50% of the lease time). However, scavenging will start after 14 days, since both the No-Refresh and the Refresh interval has passed. This is the reason why the DNS records of the Windows 95 clients disappear after two weeks.

By increasing the DNS zone parameter **Refresh Interval** from the default value of 7 days to 10 days, the DNS records could be refreshed from the 7th day up until the 17th day after the registration of the record. The DHCP server would be able to renew the lease 15 days after the lease.

Note: The DNS zone parameter **No-refresh interval** denotes the time during which the server does not accept refreshes for the record. (The server still accepts updates.) This value is the interval between the last time a record was refreshed and the earliest moment it can be refreshed again. The default value of the **No-refresh interval** is 7 days. Refresh interval

The DNS zone parameter **Refresh interval** comes after the **no-refresh interval**. At the beginning of the refresh interval, the server begins accepting refreshes. After the refresh interval expires, the DNS server can scavenge records that have not been refreshed during or after the refresh interval. The default value of the **Refresh interval** is 7 days.

Reference:
Windows 2000 Servers Resource Kit, Chapter 6 DNS, Aging and Scavenging of Stale Records
How to Configure Microsoft DHCP Server for BOOTP Clients (Q174765)

Incorrect Answers:
A: The lease is set for 30 days. The DHCP server will try to renew the DCHP lease after 15 days (50% of lease time), and again after 22.5 days (75% of the lease time). Even though the DHCP renewals fail the DHCP client would still keep its IP configuration until the DHCP lease time expires after 30 days. This is not a DHCP lease problem.
B: The **No-refresh interval** has a default value of 7 days. Decreasing it to 5 days would not help. At the contrary it would enable DNS zone scavenging after 12 days, instead of 14 days. The A (host) records of the Windows 95 clients would disappear two day earlier.
C: Windows 95 is a DHCP client not a BOOTP client. A BOOTP client could be a device like a legacy terminal or router. The BOOTP lease duration parameter does not apply in this scenario.

QUESTION 176
You are the enterprise administrator of a Windows 2000 network. The network has three domains named fabrikam.com, west.fabrikam.com, and east.fabrikam.com. All three domains are in a site named Dallas. All three domains contain organizational units (OUs).

You want to implement new desktop policies for all users on the network. The policies are configured in a Group Policy Object named GPdesktop.

You also want to implement a logon script for users from the W2 OU. The logon script policy is configured in a GPO named GPlogon. The users from the W2 OU always log on to Windows 2000 Professional computers defined in the W3 OU. You do not want to use Group Policy filtering.

What should you do?

To answer Click the Select and Place button, and then drag the GPdesktop and GPscript GPOs to the correct locations.

Dallas Site
C1
fabrikam.com
west.fabrikam.com
W1
east.fabri
E1
W2
W3
E2
E3

Answer:

Section: (none)

Explanation/Reference:
Explanation: In this scenario we have a large site, which includes three domains. Therefore two different Group Policy Objects must be applied to this site.

The GPdesktop Group Policy
The GPdesktop group policy must be implemented for all users on the network. By applying it to the site level it would be applied to the domain hierarchy including all OUs. This is the best solution with least administrative effort.

The GPO could also be applied to all domains of the site. This would require more administrative effort and it is not the best solution.

The GPlogon Group Policy
The **GPlogon** group policy, which includes logon scripts, should be applied to users of the OU named W2. All users of the W2 OU always use computers in the W3 OU. It seems that there is a choice between the OU W2 and the OU W3.

By linking the GPlogon to the W2 OU only users in the W2 OU would be affected.
By linking the GPlogon to the W3 OU all users using computers in W3 OU would be affected.

Applying the GPlogon to the W2 OU is more restrictive and is therefore the preferred solution.

QUESTION 177
You are the administrator of your company's network. The company contains three office buildings. You need to deploy Windows 2000 throughout the network.

Because of budget constraints, you can purchase only two domain controllers for implementation. You deploy one Windows 2000 domain controller in Building 2 and one Windows 2000 domain controller in Building 3. The network is configured as shown in the exhibit.

You create an Active Directory subnet for each building. You want to minimize WAN utilization and ensure that all client computers have access to Windows 2000 directory services.

How should you arrange the Active Directory sites and subnets?

A. Create one site to contain all three buildings.
   Associate three subnets with the site.
B. Create one site for each building.
   Associate the subnet for each building with the site.
C. Create one site to contain Building 1 and Building 2, and associate the subnets for Building 1 and Building 2 with the site.
   Create one site for Building 3, and associate the subnet for Building 3 with the site.
D. Create one site to contain Building 2 and Building 3, and associate the subnets for Building 2 and Building 3 with the site.
   Create one site for Building 1, and associate the subnet for Building 1 with the site.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: The subnets with domain controllers, Building 2 and Building 3, should have separate sites. The subnet of Building 1 could very well be included in the same site as Building 2, since Building 1 doesn't have any domain controllers.

Note: Sites are created to control Active Directory replication between Domain Controllers. Remote locations with Domain Controllers should have separate sites.

Reference: Windows 2000 Server Documentation, When to establish separate sites

Incorrect Answers:
A: One site should be configured for each subnet containing a Domain controller.
B: It is not necessary to create a separate site for Building 1 since it doesn't include any domain controllers. There is no replication traffic between Building 1 and the rest of the network.
D: We should create separate sites for Building 2 and Building 3.

QUESTION 178
You are the administrator of your company's network. All client computers in the network are running Windows 2000 Professional.

You install a Windows 2000 Server computer named Server1 on your network. You install the DNS Server service on Server1, and then you promote Server1 to a domain controller.

When users attempt to log on to the network, they receive an error message stating that a domain controller cannot be located. You discover that the client computers cannot locate a domain controller during LDAP queries. You want to ensure that Server1 is available for user logons.

What should you do?

A. Create the SRV (service) records for Server1 in DNS.
B. Create the PTR (pointer) records for Server1 in DNS.
C. On each client computer, create a Hosts file that contains the SRV (service) records for Server1.
D. On each client computer, create a Hosts file that contains the PTR (service) records for Server1.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: The logon service uses a SRV (service) record to locate the domain controller authenticating the login. This is the source of the problem in this scenario. We must add a SRV (service) for Server1 in DNS.

Incorrect Answers:
B: PTR (pointer) records are used for IP address to host name resolution. PTR (pointer) records are not required during the login process.
C: It is not possible to add SRV records to a Hosts file.
D: PTR (pointer) records are used for IP address to host name resolution. PTR (pointer) records are not required during the login process. The required SRV (service) record should be created in DNS, not in multiple hosts files.

QUESTION 179
You company's network consists of two domains: contoso.com and sales.contoso.com. The contoso.com domain contains one domain controller and one member server. You are a member of the Domain Admins group in sales.contoso.com.

The sales.contoso.com contains two domain controllers: SalesDC1 and SalesDC2. The sales.contoso.com domain contains 50 Windows NT Workstation computers and 50 Windows 2000 Professional computers. All operations master roles are located on SalesDC1.

You want to temporarily take SalesDC1 offline for service. You want to create 3,000 new accounts in sales.contoso.com while SalesDC1 is offline.

What should you do?

To answer, drag the appropriate object to the appropriate destination.

Action	Role	Method
Transfer	the infrastructure master	by using Active Directory Users and Computers.
	the RID master	by using Active Directory Replication Monitor.
Seize	the PDC emulator	by using Active Directory Domains and Trusts.
Query	the domain naming master	by using Active Directory Sites and Services.
	the schema master	

Answer:

Action	Role	Method
Transfer	the RID master	by using Active Directory Users and Computers.
	the infrastructure master	
		by using Active Directory Replication Monitor.
Seize	the PDC emulator	by using Active Directory Domains and Trusts.
Query	the domain naming master	by using Active Directory Sites and Services.
	the schema master	

Section: (none)

Explanation/Reference:
Explanation: We want to create 3000 user accounts. In order to be able to do that, we need a RID master.
Note: The Relative ID (RID) master allocates sequences of relative IDs to each of the various domain controllers in its domain. Whenever a domain controller creates a user, group, or computer object, it assigns the object a unique security ID. The security ID consists of a domain security ID (that is the same for all security IDs created in the domain), and a relative ID that is unique for each security ID created in the domain.

Note: **To transfer the RID master emulator role**
1. Open Active Directory Users and Computers
2. In the console tree, right-click the domain controller node that will become the new RID master, and then click **Connect to Domain**.
3. Type the domain name or click **Browse** and select the domain from the list.
4. In the console tree, right-click **Active Directory Users and Computers**, and then click **Operations Masters**
.

5. On the **RID** tab, click **Change**.

Reference:
Windows 2000 Server documentation, To transfer the PDC emulator role
Flexible Single Master Operation Transfer and Seizure Process (Q223787)
Windows 2000 Active Directory FSMO Roles (Q197132)

Incorrect Answers
PDC emulator
A PDC emulator receives password changes from clients and replicates updates to the BDCs. It does not handle the creation of user accounts however.
Seize

There is no need to seize the role. We can to an orderly transfer of the role.

QUESTION 180
You are the administrator of your company's network. The network consists of a single DNS domain. A Windows NT Server 4.0 computer named Server1 hosts the primary DNS zone for the domain.

You install a new Windows 2000 Server computer named Server2 to function as the first domain controller in the network. Server2 contains a secondary zone for the domain. During the installation of Active Directory, you choose to manually update DNS so that it contains the Active Directory resource records. You need to import these records from Server2 into DNS.

What should you do?

A. Import the contents of the Netlogon.dns file to the standard primary zone file on Server1, and then restart the DNS Server service on both servers.
B. Import the contents of the Netlogon.dns file to the standard secondary zone file on Server2, and then restart the DNS Server service on both servers.
C. Import the contents of the Root.dns file to the standard primary zone file on Server1, and then restart the Net Logon service on both servers.
D. Import the contents of the Root.dns file to the standard secondary zone file on Server2, and then restart the Net Logon service on both servers.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: The records in the Netlogon.dns file on the Windows 2000 domain controller must be imported to the root zone on the Windows NT 4.0 DNS server.

Note: Every Windows 2000 DC has a Netlogon.dns file located in its %SystemRoot%\System32\Config folder. This file contains a list of DNS records that the DC will attempt to register when the Netlogon service starts. Because the non-dynamic DNS server will not accept the domain controller's attempts to dynamically register the A records, the A records have to be manually configured on the authoritative DNS server. On the nondynamic DNS server that is authoritative for the root of the zone, create A records in the root zone.

Reference:
Integrating Windows 2000 DNS into an Existing BIND or Windows NT 4.0-Based DNS Namespace (Q255913)

Incorrect Answers:
B: A secondary zone file is read only. The records of the Netlogon.dns should be imported to the DNS server that is authoritative for the zone, in this scenario to Server1 which has a primary zone file.
C: The Root.dns does not contain relevant Active Directory records.
D: The Root.dns does not contain relevant Active Directory records. Furthermore the zone file on Server2 is read-only.

QUESTION 181
You are the administrator of your company's Windows 2000 network. The network contains 5,000 computers running Windows 2000 Professional. All client computers use dynamic update and DHCP.

The network also contains three DNS servers: Server1, Server2, and Server3. Server1 runs Windows 2000 Server and functions as the primary master server. Server2 and Server3 are UNIX servers that are running the latest version of BIND DNS. Server2 and Server3 also function as secondary servers.

The DNS servers replicate the entire DNS zone several times each day. You want to minimize replication

traffic and ensure that the zone one each server is properly synchronized.

What should you do?

A. Configure Server2 and Server3 to request the incremental zone transfer method, and then set up zone transfer notifications from Server1 to Server2 and Server3.
B. Decrease the Time-To-Live (TTL) of the DNS records in the domain.
C. Configure Server2 and Server3 to request the incremental zone transfer method, and then set up zone transfer notifications from Server2 and Server3 to Server1.
D. Increase the Time-To-Live (TTL) of the DNS records in the domain.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: Bind 8 and later supports incremental zone transfers. These zone transfers will decrease network traffic compared to full zone transfers. We must configure a notify list on the authoritative DNS Server Server1.

Note: A Zone transfer will occur during any of the following scenarios:
- When starting the DNS Service on the secondary DNS server.
- When the refresh time expires.
- When changes are saved to the Primary Zone file and there is a Notify List.

The Microsoft DNS server allows specification of a secondary server list, also known as a notify list. Note that it is a list of secondaries for this zone on this server. It need not be a complete list of secondaries for the zone. Its purpose is to give administrators a fine degree of control over the replication graph for a zone.

This list has two functions:
- Servers in this list are notified when a new version of the zone is available.
- If the SecureSecondaries registry key is used, zone transfers are refused to servers not in this list.

Reference:
Explanation of a DNS Zone Transfer (Q164017)
Microsoft DNS Server Registry Parameters, Part 3 of 3 (Q198410)

Incorrect Answers:
B: TTL only sets life time of DNS records. It doesn't affect the zone synchronization.
C: The transfer notification is initiated by the DNS server that is authoritative for the zone.
D: TTL only sets life time of DNS records. It doesn't affect the zone synchronization.

QUESTION 182
You are the administrator of your company's Windows 2000 network. The network consists of a single domain, which operates in native mode. The domain contains two domain controllers: DC1 and DC2. The network is configured as shown in the exhibit.

DC2 experiences a hardware failure. You replace the faulty hardware component and restart the server. The domain controller fails to load Windows 2000. You cannot correct the problems on DC2. DC1 is operating normally. The most recent backup tape for DC2 is three months old.

You want to restore your network to the previous configuration. What should you do?

To answer, drag the appropriate step number to the appropriate location in the list of actions taken.

Possible actions	Order of actions taken	Step numbers
Restore the server from backup tape.		1
Run DCPromo.exe on DC2.		2
Reinstall Windows 2000 Server on DC2.		3
Seize the PDC emulator FSMO role.		4
Launch the Ntdsutil utility on DC1.		
Launch the Ntdsutil utility on DC2.		
Seize the infrastructure master FSMO role		

Answer:

Possible actions	Order of actions taken	Step numbers
Restore the server from backup tape.		
Run DCPromo.exe on DC2.	2	
Reinstall Windows 2000 Server on DC2.	1	
Seize the PDC emulator FSMO role.		
Launch the Ntdsutil utility on DC1.		
Launch the Ntdsutil utility on DC2.	3	
Seize the infrastructure master FSMO role	4	

Section: (none)

Explanation/Reference:
Explanation: We should reinstall the computer, and then make it a domain controller by installing Active Directory with DCPromo.exe. Then we need to seize the infrastructure master FSMO role with the Ntdsutil utility.

Note 1: The infrastructure master is responsible for updating the group-to-user references whenever the members of groups are renamed or changed. Temporary loss of the infrastructure master is not visible to network users. It will not be visible to network administrators either, unless they have recently moved or renamed a large number of accounts. If the infrastructure master will be unavailable for an unacceptable length of time, you can seize the role to a domain controller

Note 2: To seize the infrastructure master role

1. Click **Start**, click **Run**, and then type **cmd**.
2. At the command prompt, type **ntdsutil**.
3. At the **ntdsutil** prompt, type **roles**.
4. At the **fsmo maintenance** prompt, type **connections**.
5. At the **server connections** prompt, type **connect to server**, followed by the fully qualified domain name.
6. At the **server connections** prompt, type **quit**.
7. At the **fsmo maintenance** prompt, type **seize infrastructure master**.
8. At the **fsmo maintenance** prompt, type **quit**.
9. At the **ntdsutil** prompt, type **quit**.

Reference: Windows 2000 Server documentation, Responding to operations master failures

Incorrect answers:
Restore the server from backup tapes.
The backup tapes are 3 months old. Using them would restore old information.

Seize the PDC emulator FSMO role.
Server2 only had the Infrastructure FSMO role, not the PDC emulator role.

Launch the Ntdsutil utility on DC1.
DC2, not DC1, has crashed.

QUESTION 183
You are a consultant for several different companies. You design the security policies for the computers running Windows 2000 Server and Windows 2000 Professional in your customers' networks.

You use these security policies to configure a server named Server1. You want to deploy the security configuration on Server1 to computers in your customer's networks by using the least amount of administrative effort.

What should you do first?

A. Create a Group Policy Object (GPO) that configures the security settings for all computers to match the settings on Server1, and then link the GPO to the domain.
   Export the console list to a file.
B. In the Security Configuration and Analysis snap-in, analyze Server1 and export the security template in a file.
C. In the System Information snap-in, save the system summary as a system information file.
D. In the Security Templates snap-in, export the console list to a file.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: We are using several policies on Server1. We want to configure the Windows 2000 Professional computers with the same security configuration as Server1. This is accomplished by analyzing Server1 in the Security Configuration and Analysis snap-in. Then we export the resulting security template and apply it to the Windows 2000 Professional computers.

Note: The security configuration and analysis database is a computer-specific data store. The database architecture allows the use of personal databases, security template import and export, and the combination of multiple security templates into one composite security template that can be used for analysis or configuration. New security templates can be incrementally added to the database to create a composite security template; overwriting a template is also an option. You can also create personal databases for storing your own customized security templates.

Reference: MCSE Training kit core requirements, Security Configuration and Analysis

Incorrect Answers:
A: Not all computers are in the same network. Using a single GPO will not work.
C: This is not a way to transfer security configuration.
D: This is not the way to do it.

QUESTION 184
Your company's network consists of three domains: contoso.com, fabrikam.com, and sports.fabrikam.com. You are a user in sports.fabrikan.com. You are a schema administrator in the Schema Admins group.

You want to modify the schema by using an MMC console. Which steps should you take?

To answer, drag the appropriate step number to the appropriate location in the list of actions taken.

Possible actions	Order of actions taken	Step numbers
Become a member of the Enterprise Admins group.		1
Become a member of the Domain Admins group.		2
Open the Active Directory Schema snap-in.		3
Open the Active Directory Users and Computer snap-in.		
Run Regsrv32 Schmmgmt.dll		
Set registry for **Schema Update Allowed.**		
Modify the schema		

Answer:

Possible actions	Order of actions taken	Step numbers
Become a member of the Enterprise Admins group.		
Become a member of the Domain Admins group.		
Open the Active Directory Schema snap-in.	2	
Open the Active Directory Users and Computer snap-in.		
Run Regsrv32 Schmmgmt.dll	1	
Set registry for **Schema Update Allowed.**		
Modify the schema	3	

Section: (none)

Explanation/Reference:
Explanation: First we must register the Active Directory Schema snap-in. This can be done running the Regserv32 Schmmgmt.dll at the command prompt. Then we start it and modify the appropriate schema.

Note: To Enable Schema Updates by Means of the Schema Management Console:
1. At a command prompt, type:
regsvr32 schmmgmt.dll
NOTE : RegSvr32 has been successfully registered when a **DllRegisterServer in schmmgmt.dll succeeded** dialog box is displayed.
2. Open a new management console by clicking **Start** , click **Run** , and then type: **MMC**
3. On the **Console** menu, click **Add/Remove Snap-in**.
4. Click **Add** to open the **Add Standalone Snap-in** dialog box.
5. Click **Active Directory Schema** , and then click **Add** .
6. "Active Directory Schema" is displayed in the Add/Remove snap-in. Click **Close** , and then click **OK** to return to the console.
7. Click **Active Directory Schema** so that the **Classes** and **Attributes** sections are displayed on the righthand side.
8. Right-click **Active Directory Schema** and click **Operations Master** .
9. Click to select the **Schema may be modified on this Domain Controller** check box. Click **OK** , and then exit the console.

Reference: Schema Updates Require Write Access to Schema in Active Directory (Q285172)

Incorrect answers:
Become a member of the Enterprise Admins group.

Only Schema Admins group members can change the schema. And you are already a member of the Schema Admins group.

Become a member of the Domain Admins group.

Only Schema Admins group members can change the schema. And you are already a member of the Schema Admins group.

Open the Active Directory Users and Computer snap-in.

The Active Directory Schema snap-in, not the Active Directory Users and Computer snap-in, is used to modify a schema.

Set registry for Schema Update allowed.

It is not recommended to enable schema updates by directly editing the "Schema Update Allowed" registry key. Schema updates should be enabled through the console method, whenever possible.

QUESTION 185

You company's network consists of two domains: contoso.com and sales.contoso.com. The contoso.com domain contains one domain controller and one member server. You are a member of the Domain Admins group in sales.contoso.com.

The sales.contoso.com contains two domain controllers: SalesDC1 and SalesDC2. The domain also contains one Windows NT BDC named SalesNT1. The sales.contoso.com domain contains 50 Windows NT Workstation computers and 50 Windows 2000 Professional computers. All operations master roles are located on SalesDC1.

You need to takes SalesDC1 offline for two weeks. You want to allows Windows NT users to change their passwords while SalesDC1 is offline.

What should you do?

To answer, drag the appropriate object to the appropriate destination.

Answer:

Action	Role	Method
Transfer	the PDC emulator	by using the Ntdsutil utility.
	the infrastructure master	by using Active Directory Replication Monitor.
	the RID master	by using Active Directory Domains and Trusts.
Seize		by using Active Directory Sites and Services.
Query	the domain naming master	
	the schema master	

Section: (none)

Explanation/Reference:
Explanation: The PDC emulator is responsible for password changes. Since this is a planned shutdown, and not an emergency shutdown, of the PDC emulator, we should transfer the role.

Reference:
Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller (Q255504)
Windows 2000 Server Resource kit, Active Directory Diagnostic Tool (Ntdsutil.exe), Managing Operations Master Roles

Incorrect answers:
Transfers are preferred to seizing a role..
You don't query operations master roles.
The PDC Emulator role, not any other role, changes the passwords in a domain.
The Ntdsutil utility or the Directory Users and Computers can be used to transfer the PDC emulator role. The other listed methods do not work.

QUESTION 186
Your company's network consists of two Windows 2000 domains: contoso.com and sales.contoso.com. Each domain contains one domain controller and one member server. You are a member of the Enterprise Admins group.

You want each domain to contain two domain controllers. Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)

A. Manually install a new server in sales.contoso.com by using the Windows 2000 CD-ROM. During this process, install the server as a domain controller.

B. Manually install a new server in contoso.com by using the Windows 2000 CD-ROM.
During this process, install the server as a domain controller.

C. Manually install a new member server in sales.contoso.com by a network installation point
Then, promote the server to a domain controller.

D. Manually install a new member server in contoso.com by a network installation point
Promote the server to a domain controller by using an unattended setup file to script the promotion process.

E. Install a new member server in sales.contoso.com by using Remote Installation Services (RIS).
Then, promote the server to a domain controller.

F. Install a new member server in contoso.com by using Remote Installation Services (RIS).
Promote the server to a domain controller by using an unattended setup file to script the promotion process.

Answer: CD
Section: (none)

Explanation/Reference:
Explanation: First we must install the servers as member servers. Then we upgrade them to domain controllers. There are two separate steps which cannot be merged into one single step.

Note: To upgrade a member server to domain controller either use dcpromo.exe or the Configure Your Server utilities.

Incorrect Answers:
A, B: It is not possible to configure a domain controller during the installation process.
E, F: It is possible to install a member server with RIS (see Q308508). This would require SP3 and a fix to SP3. No installation of Service Packs is discussed in the scenario. RIS might also seem an unnecessary complicated procedure to install only two servers.
Note: It is possible to use a script to promote a member to a domain controller (see Q224390, Q223757).
Reference:
Unable to Create Windows 2000 Server Image on RIS Server (Q308508)
How to Automate Windows 2000 Setup and Domain Controller Setup (Q224390)
Unattended Promotion and Demotion of Windows 2000 Domain Controllers (Q223757)

QUESTION 187
You are the administrator of a Windows 2000 domain. The domain has a Windows 2000 Server computer named Toronto. Users in the domain frequently work on different Windows 2000 Professional computers. All Windows 2000 Professional computers are in the domain.

You want to enable roaming profiles for all users.

You want to accomplish the following goals:

- All users in the domain will be able to work on all Windows 2000 Professional computers and have their own desktop settings available on all computers.
- All users in the domain will be able to make changes to their desktop settings.
- All users in the domain will be able to access their documents in the My Documents folder from any Windows 2000 Professional computer.
- The amount of data that is copied between the Toronto server and the Windows 2000 Professional computers each time a user logs on or off will be minimized.

What should you do? (Choose two.)

A. Configure a roaming profile for each user in the domain.
Use \\Toronto\Profiles\%Username% as the profile path.

B. Configure a roaming profile for each user in the domain.
Use \\Toronto\Profiles\%Username%\Ntuser.man as the profile path.

C. Create a new Group Policy Object (GPO) named Profilescript.
Assign the Profilescript GPO to the domain.
Configure the Profilescript GPO to assign a logon script to all users.
Include the **runas /profile explorer.exe** command in the logon script.

D. Create a new Group Policy Object (GPO) named Docs.
Assign the Docs GPO to the domain.
Configure the Docs GPO to redirect the My Documents folder to the \\Toronto\Docs\%Username% location.

E. Create a new Group Policy object (GPO) named Profiledocs.
Assign the Profiledocs GPO to the domain.
Configure the Profiledocs GPO to exclude the My Documents folder from each user's roaming profile.

Answer: AD
Section: (none)

Explanation/Reference:
Explanation:
A: We must configure roaming user profiles. Each user must have a unique profile, which should not be mandatory.
D: To reduce network traffic during the logon process the My Documents folder should be redirected to a network share, one separate share for each user.

Reference:
Configuration of the My Documents Folder (Q221837)
Windows 2000 Server documentation, Folder Redirection

Incorrect Answers:
B: We should not use mandatory profiles, profiles named Ntuser.man, since we want the users to be able to make changes to their desktop settings.
C: The **runas /profile explorer.exe** command in a login script would not achieve the required results.
E: Excluding the My Documents from the users roaming profiles would decrease network traffic, but the My Documents folder could no longer be used.

QUESTION 188
You are the administrator of TestKing Inc. The network consists of a single domain. The company's main office is located in South Africa and branch offices are located in Asia and Europe. The offices are connected by dedicated 256-Kbps lines. To minimize logon authentication traffic across the slow links, you create an Active Directory site for each company office and configure site links between the sites.

Users in branch offices report that it takes a long time to log on to the domain. You monitor the network and discover that all authentication traffic is still being sent to the domain controllers in South Africa.

You need to improve network performance. What should you do?

A. Schedule replication to occur more frequently between the sites.
B. Schedule replication to occur less frequently between the sites.
C. Create a subnet for each physical location, associate the subnets with the South Africa site, and move the domain controller objects to the South Africa site.
D. Create a subnet for each physical location, associate each subnet with its site, and move each domain controller object to its site.

Answer: D
Section: (none)

Explanation/Reference:

Explanation: In this scenario no subnets have been associated with any sites. No objects have been added to the subnets. Windows 2000 AD is therefore unable to distinguish between local and remote sources. This results in slow performance.

The subnet of each location must be associated with the local site. The domain controllers must also be moved to the appropriate local site:

Incorrect Answers
A, B: We must configure the sites, not the replication schedule.
C: If we associate all subnets with the South Africa site then Windows 2000 AD would view the entire network as a single site. It would be impossible to distinguish between local and remote sources.

QUESTION 189
Your company's network consists of two Windows 2000 domains: testking.com and newyork.testking.com. The newyork.testking.com domain contains three organizational units (OUs): Sales, Marketing, and Finance. You are a member of the Domain Admins group in newyork.testking.com.

An employee named Maria can reset passwords for the Finance OU. Maria will be moving to the Sales OU and no longer needs access to the Finance OU.

You need to remove Maria's right to reset passwords for Finance. What should you do?

A. In Delegation of Control wizard, specify that Maria cannot reset passwords for the Finance OU.
B. Clear the **Trust computer for delegation** check box in the properties for the domain controller to which Maria's user account authenticates.
C. In the security properties of the Finance OU, remove Maria's right to reset passwords.
D. Copy Maria's user account to the Sales OU, and then delete the account.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: The **Delegation of Control** wizard is used to delegate control of objects in a Windows 2000 Active Directory service container. In this scenario we have to:
1. Open Active Directory Users and Computers
2. Right-click on the Finance OU and select **Delegate Control**.
3. Click **Next**. Add Maria's user account. Click **Next.**
4. Remove the task **Reset passwords on user accounts** (see below).
5. Finish the Wizard.

Reference: Step-by-Step Guide to Using the Delegation of Control Wizard

Incorrect Answers
B: We must change the permissions of the user account, not for a domain controller.
C: OUs do not have any security properties. Instead we should use the **Delegation of Control** wizard
D: It would be drastic to the delete the original user account of Maria. The copied user account might lose rights and permissions since it has a new Security Identifier (SID).

QUESTION 190
You are a member of the Enterprise Admins group in your company's Windows 2000 network. The network consists of a single Windows 2000 domain. The network is configured as shown in the exhibit:

For security reasons, you configure the routers so that Subnet 1 and Subnet 4 cannot directly communicate. After configuring the routers, you notice directory replication errors on DC1 and DC4.

You need to resolve the errors. What should you do?

Exhibit:

A. Configure DC2 and DC3 as global catalog servers.
B. Create a site link bridge that includes Site TestKing and Site Remote
C. Configure DC2 and DC3 as bridgehead servers.
D. Create one site link bridge for Site TestKing and one site link bridge for Site Remote.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: Bridgehead servers are the contact point for exchange of directory information between sites. By selecting DC and DC3 as bridgehead servers all Active Directory replication traffic between the TestKing site and the Remote site will go between subnet 2 and subnet 3. There will be no directory replication between Subnet 1 and subnet 4.

Reference: Windows Help, Using preferred bridgehead servers

Incorrect Answers
A: Global catalog servers would decrease replication traffic. However, replication traffic between subnet 1 and subnet 4 would still be possible.
B, D: By creating a site link, you provide Active Directory with information about what connections are available, which ones are preferred, and how much bandwidth is available. This is not useful in this scenario however.

QUESTION 191
You are the administrator of your company's Windows 2000 network. The network contains a DNS server that hosts two DNS zones; contoso.com and testking.com.

You discover that outdated resource records are accumulating in the contoso.com zone. However, this problem does not occur in the testking.com zone. You must remove the outdated records from contoso.com without affecting testking.com.

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

A. In the server object properties, select the **Secure cache against pollution** check box.
B. In the server object properties, select the **Enable automatic scavenging of stale records** check box.
C. In the server object properties, select the **Disable recursion** check box.
D. In the contoso.com zone properties, select the **Allow zone transfers** check box.
E. In the contoso.com zone properties, select the **Scavenge stale resource records** check box.
F. In the contoso.com zone properties, select the **Use WINS forward lookup** check box.

Answer: AE
Section: (none)

Explanation/Reference:
Explanation:
A: The **Secure cache against pollution** option determines whether the server attempts to clean up responses to avoid cache pollution. Setting this option could help solving the problem at hand. Furthermore, it would not in a negative way affect the testking.com zone.
E: The **Scavenge stale resource records** option is applied to a single zone. We can apply it to the contoso.com zone, and it would not affect the testking.com zone.

Note: To set aging/scavenging properties for a selected zone
1. Open DNS
2. In the console tree, click the applicable zone.
3. On the **Action** menu, click **Properties**.
4. On the **General** tab, click **Aging**.
5. Select the **Scavenge stale resource records** check box.
6. Modify other aging and scavenging properties as needed.

Incorrect Answers
B: The **Enable automatic scavenging of stale records option** affects all zones on the DNS server and it cannot be used.
Note: To set aging/scavenging properties for the DNS server:
1. Open DNS
2. In the console tree, click the applicable DNS server.
3. On the **Action** menu, click **Set Aging/Scavenging for all zones**.
4. Select the **Scavenge stale resource records** check box.

C: Disabling recursion would affect all zones hosted on the DNS server. Furthermore, it would address the problem of stale records.
D: The **Allow zone transfers** option does not affect the problem of outdated records.
F: The **Use WINS forward lookup** would not address the problem of stale records.
Note: The DNS service provides the ability to use Windows Internet Name Service (WINS) servers to look up names not found in the DNS domain namespace by checking the NetBIOS namespace managed by WINS.

QUESTION 192
You are the administrator of your company's Windows 2000 network. The network consists of two domains: testking.com and germany.testking.com.

You need to add 300 users in germany.testking.com to an existing group in testking.com. You want to accomplish this goal by using the least amount of administrative effort.

What should you do?

A. Use the CSVDE utility to modify the group object.
B. Use the LDIFDE utility to modify the user objects.

C. Use the CSVDE utility to modify the user objects.
D. Use the LDIFDE utility to modify the group object.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: The LDIFDE utility can be used to Export and Import Directory Objects. It supports batch operations based on the LDIF file format standard. Furthermore, we should specify objectClass=User

Note 1: Sample code that exports the user accounts from the source domain. The code that specifies user objects is highlighted. ldifde -f Exportuser.ldf -s Server1 -d "dc=testking,dc=com" -p subtree -r "(&(objectCategory=person)(objectClass=User)(givenname=*))" -l "cn,givenName,objectclass,samAccountName"

Note2: The LDAP Data Interchange Format (LDIF) is a draft Internet standard for a file format that may be used for performing batch operations against directories that conform to the LDAP standards.

Reference:

Q237677, Using LDIFDE to Import and Export Directory Objects to Active Directory
Q300409, How to Use Csvde.exe to Import Contacts into Active Directory

Incorrect Answers
A, C: The CSVDE utility enables you to use files that are saved by export utilities in a Comma Separated Value (CSV) format to import contact information into the Windows 2000 Active Directory. However, in this scenario we are required to add users from one domain to another domain.
D: As we want to add user accounts we must modify user objects.

QUESTION 193
You are the administrator of a branch office in your company. The network consists of one Windows 2000 domain. The branch office contains Windows 2000 Server computers. The administrators at the main office create a security policy template that must be applied to all servers in the domain.

Because your office has stricter security requirements than the main office, you verify the security policy before you apply it. You need to modify the security policy on a Windows 2000 Server computer named ServerTK.

What should you do?

A. In the Security Configuration and Analysis snap-in, import the security template and create a new database for serverTK.
   Then, analyze ServerTK and adjust the database settings.
   Finally, use the database settings to configure ServerTK.
B. In the Security Configuration and Analysis snap-in, import the security template and create a new database for ServerTK.
   Then, configure ServerTK and adjust the database settings.
   Finally, analyze ServerTK against the database settings.
C. In the Local Security Policy snap-in, import the security template and then adjust the security by exporting the local policy settings.
D. In the Local Security Policy snap-in, import the security template and then adjust the security by exporting the effective policy settings.

Answer: A
Section: (none)

Explanation/Reference:

Explanation: To import and analyze the security template we must use the Security Configuration and Analysis snap-in. We should follow these steps:
1. Import the security template.
2. Create a new database (set a working database).
3. Analyze the security template.
4. Finally we should apply the security settings.

Incorrect Answers
B: We should first analyze the security settings before we apply them.
C, D: The Local Security Policy snap-in has no option to analyze security.

QUESTION 194
You are an administrator of your company's Windows 2000 domain. The domain contains an organizational unit (OU) named TestK. Another administrator accidentally deletes the Sales OU.

You want to restore the TestK OU without affecting other objects in the directory. Which steps should you take?

To answer, click the Select and Place button, and then drag the appropriate step number to the appropriate location in the list of actions taken.

Possible actions	Order of actions taken	Step numbers
Replay the server transaction logs.		1
Use the Ntdsutil utility to mark the TestK OU as authoritative.		2
Restore the server's Schema partition from backup tape.		3
Restart the domain controller in normal mode.		4
Restart the domain controller in directory service restore mode.		
Restore the server's System State data from backup tape.		
Use Active Directory Users and Computers to precrate the OU		

Answer:

Possible actions	Order of actions taken	Step numbers
Replay the server transaction logs.		
Use the Ntdsutil utility to mark the TestK OU as authoritative.	3	
Restore the server's Schema partition from backup tape.		
Restart the domain controller in normal mode.	4	
Restart the domain controller in directory service restore mode.	1	
Restore the server's System State data from backup tape.	2	
Use Active Directory Users and Computers to precrate the OU		

Section: (none)

Explanation/Reference:
Explanation:
Procedure to restore a subtree:
1. Restart the domain controller.
2. When the Windows 2000 Startup menu is displayed, select Directory Services Restore Mode, and then press ENTER.
3. Restore the System State Data.
4. At a command prompt, type "ntdsutil" (without the quotation marks), and then press ENTER.
5. Type "authoritative restore" (without the quotation marks), and then press ENTER.
6. Type "restore subtree "ou=<OU TestK>,dc=<domain name>,dc=<xxx>"" (without the quotation marks), and then press ENTER..
7. Type "quit" (without the quotation marks), press ENTER, type "quit" (without the quotation marks), and then press ENTER.
8. Type "exit" (without the quotation marks), and then press ENTER.
9. Restart the domain controller.

Reference: Q241594, HOW TO: Perform an Authoritative Restore to a Domain Controller in Windows 20000

Incorrect Answers
Replay the server transaction logs: Not useful.
Restore the server's Schema partition from backup tape: Not useful.
Use Active Directory Users and Computers to recreate the OU: This step is not necessary.

QUESTION 195
You are the administrator of your company's Windows 2000 network. The network contains 10 domain

controllers named TK1 through TK10. The hard disk on TK1 fails. You install a new domain controller to replace TK1.

Active Directory objects that represent TK1 still appear in Active Directory. You want to remove all references to TK1 from the Active Directory database.

What should you do?

A. Run the Ntdsutil utility and configure it to clean up metadata.
B. Use the Active Directory Users and Computers snap-in to delete the server object.
C. Use the Active Directory Sites and Services snap-in to delete the server object.
D. Perform an authoritative restore of TK1.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: To cleanup metadata left behind by decommissioned or failed domain controllers, use the Cleanup command of the Ntdsutil tool. It removes the defunct domain controller's identification and information from the directory.

Incorrect Answers
B: To remove a server object Active Directory Sites and Services should be used.
C: Only the server object can be removed using the Active Directory Sites and Services, not all references to this object.
D: We want to remove TK1, not restore it.

QUESTION 196
You are the administrator of the network at Test King Inc. The network consists of a single Windows NT domain. The network contains a UNIX server that is running BIND DNS.

You are configuring a Windows 2000 DNS server in the network. You want to use dynamic updates on the DNS database. The UNIX server does not support dynamic updates, but management will not allow you to upgrade or remove the UNIX server. You need to synchronize all DNS information between the two servers.

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

A. On the Windows 2000 DNS server, create a standard primary zone and import the existing zone file.
B. On the Windows 2000 DNS server, create a standard secondary zone.
C. On the UNIX server, delete and re-create the primary zone.
D. On the UNIX server, delete the existing zone and create a new secondary zone.
E. On the Windows 2000 DNS server, configure the secondary zone to use the UNIX server standard primary zone as its master zone.
F. On the UNIX server, configure the secondary zone to use the Windows 2000 standard primary zone as its master zone.

Answer: ADF
Section: (none)

Explanation/Reference:
Explanation: To integrate Windows 2000 DNS into an existing namespace based on non-dynamic DNS servers, you can delegate the subdomains used by the locator records (SRV records) so that dynamic updates may be used.

A: First we create a DNS zone, either standard primary or Active Directory integrated, on the Windows 2000 DNS server.
D: The UNIX DNS should only receive zone transfers from the Windows 2000 DNS servers. They should not update the DNS zone. They should therefore host secondary zones.
F: Finally we configure the UNIX DNS servers to use the Windows 2000 standard primary zone as the master zone.

Reference:
Q255913, Integrating Windows 2000 DNS into an Existing BIND or Windows NT 4.0-Based DNS Namespace

Incorrect Answers
B: The Windows 2000 DNS servers must be able to update the DNS records. We cannot use secondary files, since no updates can be made.
C: The UNIX DNS servers are not able to support dynamic updates and they should therefore not host primary zones.
E: The Windows DNS servers must be authoritative for the zone. They cannot host secondary zones.

QUESTION 197
You are the administrator of your company's Windows 2000 network. The network contains two Windows 2000 Server computers: TestKing1 and TestKing2. TestKing1 contains confidential company data and must have strict account security settings. TestKing2 was recently installed and will host the same type of data as TestKing1.

You must configure TestKing2 with the same security settings as TestKing1 without decreasing the security on TestKing1.

Which two actions can you take? (Choose two)

A. In the Security Configuration and Analysis snap-in, configure TestKing1 so that is has the settings from the Basicsv.inf security template, and then configure TestKing2 so that is has the same settings.
B. In the Security Configuration and Analysis snap-in, configure TestKing1 and TestKing2 so that they have the settings from the Setup Security.inf security template.
C. In the Security Configuration and Analysis snap-in, export the security settings on TestKing1 to a template named SecSrv.inf, and then configure TestKing2 so that is has the exported settings.
D. In the Local Security Policy snap-in, import the Basicsv.inf security template to TestKing1 and TestKing2.
E. In the Local Security Policy snap-in, import the Setup Security.inf security template to TestKing1 and TestKing2.
F. In the Local Policy snap-in, export the effective policy settings from TestKing1 to Setup Security.inf, and then import the Setup Security.inf template to TestKing2.

Answer: CF
Section: (none)

Explanation/Reference:
Explanation: We should export the security settings from TestKing1 to TestKing2. We could use the Security Configuration and Analysis snap or the Local Security Policy snap-in.

Reference: - Q309689, HOW TO: Apply Predefined Security Templates in Windows 2000

Incorrect Answers
A: The **Basicsv** security template provides only a basic level of security for file and print servers. It is not adequate for this scenario.
B: The **Setup Security** template applies the default Windows 2000 security configuration. However, we want strict security settings. Furthermore, we should not apply the template on TestKing1. It could decrease the

security on TestKing1.
D, E: We should not apply any security templates on TestKing1. They could decrease the security of the server.

QUESTION 198
You are the administrator of your company's Windows 2000 network. The network consists of a single DNS domain. The network contains one Windows 2000 domain controller named TestKing and one UNIX server named UnixServer1. TestKing functions as a DNS server and hosts the secondary zone for the domain. UnixServer1 is running BIND DNS and hosts the primary zone for the domain.

You want TestKing to be authoritative for the domain. You also want to enable secure dynamic updates for the domain. You want UnixServer1 to function as a backup DNS server.

Which two actions should you take? (Choose two)

A. On TestKing, convert the secondary zone to an Active Directory integrated zone.
B. On TestKing, create a new standard primary zone.
C. On TestKing, enable forwarding of DNS request to UnixServer1.
D. On UnixServer1, delete the existing primary zone and then create a new secondary zone that uses TestKing as the master.
E. On UnixServer1, delete the existing primary zone and then enable forwarding of DNS requests to TestKing.
F. On UnixServer1, add TestKing to the root hints listing.

Answer: BD
Section: (none)

Explanation/Reference:
Explanation:
First we create a new standard primary (or Active Directory Integrated) zone on the Windows 2000 DNS server TestKing. Then we create a new secondary zone on the UNIX DNS server that uses TestKing as the master.

Reference:
Q255913, Integrating Windows 2000 DNS into an Existing BIND or Windows NT 4.0-Based DNS Namespace

Incorrect Answers
A: We must create a new zone.
C, E: Forwarding is not an option in this scenario. We must set up replication between the DNS servers instead.
F: Root hints are used to access public DNS servers and they are not useful here.

QUESTION 199
Your company's network consists of two Windows 2000 domains: testk.com and sales.testk.com. The sales.testk.com domain contains one domain controller.

The domain controller in sales.testk.com fails, and you do not have a usable backup. You want to delete all references to sales.testk.com in the Active Directory database.

What should you do?

A. Delete the A (host) record by using the DNS Server snap-in.
B. Delete the PTR (pointer) record by using the DNS Server snap-in.
C. Delete the SOA (start of authority) record by using DNS Server snap-in.
D. Delete the domain reference by using the Active Directory Sites and Services snap-in.

E. Delete the domain reference by using the Active Directory Domains and Trust snap-in.
F. Delete the domain reference by using the Ntdsutil utility.
G. Delete the domain reference by using the Repadmin utility.

Answer: F
Section: (none)

Explanation/Reference:
Explanation: We use the **Ntdsutil** utility and the **metadata cleanup** command to remove the orphaned domain.

Reference: Q230306, HOW TO: Remove Orphaned Domains from Active Directory

Incorrect Answers
These proposed solutions are all insufficient.

QUESTION 200
You are the administrator of your company's Windows 2000 network. The network consists of a single domain named testking.com. The testking.com domain is contained in an Active Directory integrated zone on Server1.

Your company wants to create a new child domain named research.testking.com. This domain will contain all user and computer accounts in the Research department and will have higher security than the root domain. You install a new Windows 2000 Server computer named Server2. Server2 will be the DNS sever and domain controller for the Research department.

You must maintain a high level of security, and ensure that only administrators for Server2 can modify DNS records for research.testking.com

What should you do?

A. On Server1, create a new Active Directory integrated zone for research.testking.com.
On Server2, create a new standard secondary zone for research.testking.com.
B. On Server2, create a new Active Directory integrated zone for research.testking.com, and then configure the forwarders to point to Server1.
On Server1, delegate research.testking.com to Server2.
C. On Server1, create a new Active Directory integrated zone for research.testking.com.
On Server2, create a new standard primary zone for research.testking.com.
D. On Server2, create a new Active Directory integrated zone for testking.com, and then create a new child domain named research.testking.com.
Delegate testking.com to Server1.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: We want to create a child domain, research.testking.com, and then delegate the Domain Name System (DNS) namespace to a domain controller located in this child domain.

First we should create an Active Directory Integrated zone (or primary zone) on Server2 for the new domain research.testking.com. We could configure forwarding to Server1 to ensure that name resolution outside of the research.testking.com will be handled. Finally we should delegate the control of the new domain to Server2. The delegation must take place in the root zone.

Reference: - Q255248, HOW TO: Create a Child Domain in Active Directory and Delegate the DNS Namespace to the Child Domain

Incorrect Answers
A: A secondary zone would be read-only. Administrators on Server1, but not Administrators on Server2 would be able to change records in the zone.
C: We cannot both have an Active Directory and a primary zone for research.testking.com.
D: The delegation must take place on the root zone.

QUESTION 201
You are the administrator of your company's Windows 2000 network. The network consists of a single DNS zone, testking.com. The network contains three Windows 2000 DNS servers: one primary master server and two secondary servers. External users can directly access one secondary server by means of the Internet.

During a security audit, you discover that an Internet intruder could perform an unauthorized zone transfer of DNS data in the company network. You must tighten the security on the DNS servers to prevent this type of attack.

What should you do?

A. On each DNS server, deny the Everyone group the Read permission for the %systemroot%\System32\DNS folder, and then grant the Authenticated Users group the Read permission for the %systemroot%\System32 \Dns folder.
B. On each secondary DNS server, clear the **Allow zone transfer** check box for the zone.
C. On the primary master DNS server, specify that only the secondary servers in the network can perform zone transfers.
D. On each DNS server, configure the zone to list only the three DNS servers on the **Name Servers** configuration tab.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: On each DNS server we list the servers that are allowed to perform zone transfers. No other servers will be allowed to initiate a zone transfer.

Incorrect Answers
A: File permission is not possible solution.
B: Reconfiguring the secondary servers will not help.
C: Zone transfers might still be possible if the intruder connects to a secondary server.

QUESTION 202
You are the administrator of your company's Windows 2000 domain testking.com. To control the desktop environment of users in the domain, you use a script file named Desktop.vbs to change settings in the current user profile. This script file is deployed as a logon script for all users in the domain.

The Desktop.vbs script usually takes 15 seconds to complete its work. You want to ensure that each user's desktop appears only after the Desktop.vbs is completed. You create a new Group Policy object (GPO) and link the GPO to the domain. Then, you add Desktop.vbs to the GPO as a logon script.

You want to complete the GPO configuration. What should you do?

A. Configure the GPO to run logon scripts asynchronously.
B. Configure the GPO to run logon scripts synchronously.
C. Configure the GPO to set a maximum wait time of 15 seconds for Group Policy scripts.

D. Configure the GPO to set a timeout of 15 seconds for logon dialog boxes.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: The script must be configured to run synchronously so that all scripts are finished before Windows Explorer starts and the Desktop appears.

Incorrect Answers
A: If the logon script is run asynchronously the Desktop could be shown before the script has finished.
C: It usually takes 15 seconds for the script to finish, but it is just an estimate and it could take longer. In that case the desktop could appear before the script has finished.
D: Timeout settings are used for logoff and shutdown scripts not for logon scripts.

QUESTION 203
You are the administrator of TestKing's Windows 2000 network. The network consists of a single domain, which contains all company user and computer accounts. User accounts are placed in three organizational units (OUs) according to the user's job category: Consultants, Finance, and Sales. All client computer accounts exist in the Computers container, and all domain controller accounts exist in the Domain Controllers container.

You want to apply an audit security policy to record any changes made to the user accounts in the Finance OU. Where should you define the policy?

A. In the Default Domain Group Policy object (GPO).
B. In a new Group Policy object (GPO) for the Finance OU.
C. In the Default Domain Controllers Group Policy object (GPO).
D. In a new Group Policy object (GPO) for the Computers container.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: We want to apply a security policy to accounts in the Finance OU. First we create a GPO with the appropriate policies defined. Then we link the GPO to the Finance OU.

Incorrect Answers
A: We don't want to apply the security policy to the whole domain.
C: We don't want to apply the security policy to the domain controllers.
D: We don't want to apply the security policy to the computers in the domain.

QUESTION 204
You are the administrator of your company's Windows 2000 network. The network consists of a single DNS domain named testking.com. A domain controller named TestKing1 contains the DNS domain in an Active Directory integrated zone.

You install the LDAP service on a member server named TestKing2. You must enable all client computers in the network to locate the LDAP server in DNS without providing them with the name or IP address of TestKing2. What should you do?

A. Create a PTR (pointer) record in testking.com, and then specify the host as testking2.testking.com.
B. On TestKing1, create a delegated domain named _ldap.testking.com, and then create an A (host) record for TestKing2.

C. Create an SRV (service) record in testking.com, and then specify the host as testking2.testking.com.
D. On TestKing1, create a subdomain named _ldap.testking.com, and then create an A (host) record for TestKing2.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: SRV (Service) records identify which servers are hosting a particular service. Examples of services are Kerberos and LDAP. With a SRV (service) record for testking2 in the testking.com domain users would be unaware of the exact host name or IP address of the LDAP server, but still they would be able to use it.

Incorrect Answers
A: PTR (Pointer) records are used for reverse mappings; IP addresses mapped to host names. This would not be useful here.
B: A delegated domain offers no solution to the problem. We must hide the name and IP address.
D: A subdomain offers no solution to the problem. We must hide the name and IP address.

QUESTION 205
You are the administrator of TestKing's Windows 2000 network. You implement company security policies by using the Security Configuration and Analysis snap-in on each domain controller.

The password security policy forces all users to change their passwords every five weeks. The policy also prevents users from reusing their last seven passwords. Server users in the domain can bypass this policy by changing a password seven times and then changing it back to the original password.

You change all users' passwords so that they are at least eight characters long. You must ensure that users cannot bypass the policy. You also need to make sure that the template prevents users from reusing the same password for at least five weeks.

You want to configure the password security template to support these requirements. What should you do?

A. Set the minimum password age to 6 days.
B. Set the maximum password age to 42 days.
C. Enable password complexity requirements.
D. Disable the storage of passwords in reversible encryption.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: With a minimum password age of 6 days, the server users would be able to change the password a maximum of 7 times in 5 weeks. For example 1st day, 6th day, 11th day, 16th day, 21st day, 26th, and 31st day. The eighth time would be outside the 5 week period.

Incorrect Answers
B: Changing the maximum password age to 42 days does not help achieving the requirements. Server users would still be able to change passwords as often they wanted and thus be able to reuse passwords frequently. Furthermore, the restriction to change password every 5 weeks is changed to every 6 weeks instead.
C: There is no requirement to meet any complexity requirement of the passwords.
D: The **Store Password Using Reversible Encryption For All Users In The Domain** option is useful with the Challenge Handshake Authentication Protocol (CHAP). It would be of no use in this scenario, however.

QUESTION 206
You are a member of the Enterprise Admins group in your company's Windows 2000 network. The network consists of a single domain named testking.com. The Bonn office has its own organizational unit (OU) named Bonn.

You hire an employee named Sophie as a LAN administrator for the Bonn office. Sophie needs to create child OUs for the Bonn OU. She also needs to verify the existence of the OUs she creates. You need to grant Sophie the minimum permissions on the Bonn OU so that she can accomplish these tasks.

Which permissions should you grant?

A. Read All Properties, Create Organizational Unit Object, Write All Properties.
B. Read All Properties, List Contents, Create Organizational Unit Objects.
C. List Contents, Create All Child Objects.
D. Write All Properties, All Extended Rights.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: She needs to be able to create child OU. This is achieved with the **Create Organizational Unit Objects** permission. The List contents and Read All Properties ensure that she can verify the existence of the child OUs she creates.

Incorrect Answers
A, D: Sophie should not have the **Write All Properties** permission. She should only be able to create OUs.
C: Sophie only needs to create OUs. She should not be able to create other child objects in the OU.

QUESTION 207
You are the administrator of your company's Windows 2000 network. The network consists of two domains: testking.com and finance.testking.com. The network contains an Active Directory site named Madrid. The Madrid site contains three domain controllers and a member server named TestKingApp. The Madrid site is configured as shown in the exhibit.

On TestKingApp, you install an application that frequently uses Active Directory. After the installation, users in the Madrid site report that searching the global catalog takes a long time.

You want to improve search performance for users in the Madrid site. What should you do?

Exhibit:

A. Using the Active Directory Users and Computers snap-in, make DC1 a global catalog.
B. Using the Active Directory Sites and Services snap-in, make DC1 a global catalog server.

C. Using the Active Directory Users and Computers snap-in, make DC2 a global catalog.
D. Using the Active Directory Sites and Services snap-in, make DC2 a global catalog server.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: TestKingApp uses the Active Directory very frequently. This makes the Global Catalog server overburdened. We need to load balance this workload by creating a second Global Catalog. The placement of the 2nd Global Catalog server is crucial. We should create it on DC2 since there are no conflicts between the FSMO roles of Schema Master, RID master, Domain naming maser and Global Catalog server. Finally we create the new global catalog server with the **Active Directory Sites and Services** snap-in.

Procedure to create a new global catalog:

1. Start the Active Directory Sites and Services snap-in
2. In the console tree, double-click **Sites**, and then double-click **sitename**.
3. Double-click **Servers**, click your domain controller, right-click **NTDS Settings**, and then click **Properties**.
4. On the **General** tab, click to select the **Global catalog** check box to assign the role of global catalog to this server.
5. Restart the domain controller.

Note: The Active Directory defines five FSMO (Flexible Single-Master Operational) roles: schema master, domain master, RID master, PDC emulator, and infrastructure master.

Reference: Microsoft Knowledge Base Article - Q223346, FSMO Placement and Optimization on Windows 2000 Domain Controllers
Microsoft Knowledge Base Article - Q313994, HOW TO: Create or Move a Global Catalog in Windows 2000

Incorrect Answers
A, B: As a general rule, the infrastructure master should be located on a nonglobal catalog server. The infrastructure master, if placed on a global catalog server, will never update anything, because it does not contain any references to objects that it does not hold. We should therefore not make DC1 a global catalog server.
C: The **Active Directory Sites and Services** snap-in, not the **Active Directory Users and Computers** snap-in is used to create a new global catalog server.

QUESTION 208
You are the administrator of your company's Windows 2000 network. The network consists of three domains as shown in the following table.

Domain name	Number of users
testking.com	10,000
corp.testking.com	500
research.testking.com	2,000

The network contains four Windows 2000 DNS servers on the same network segment. TestkingA hosts the standard primary zone that contains all three domains. TestKingB, TestKingC, and TestKingD each hold a standard secondary zone that is linked to the zone on TestKingA.

Executives in corp.testking.com report very slow response times when they log on to the network. You discover that the slow response times are occurring because the DNS severs are overloaded.

You need to reconfigure the corp.testking.com domain and the DNS zones to improve the response times for

the executives. On TestKingD, you remove the secondary zone for testking.com

You need to complete the reconfiguration. What should you do?

A. On TestKingA, create a new standard primary zone for the corp.testking.com domain.
On TestKingD, delegate the corp.testking.com domain to TestKingA.
On TestKingA, re-create the static DNS records for the corp.testking.com domain.
B. On TestKingD, create a new standard primary zone for the corp.testking.com domain.
On TestKingA, create a new secondary zone that is linked to the corp.testking.com zone on TestKingD.
C. On TestKingD, create a new standard primary zone for the corp.testking.com domain.
On TestKingA, delegate the corp.testking.com domain to TestKingD.
On TestKingD, re-create the static DNS records for the corp.testking.com domain.
D. On TestKingA, create a new standard primary zone for the corp.testking.com domain.
On TestKingD, create a new secondary zone that is linked to the corp.testking.com zone on TestKingA.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: TestKingA is authoritative for all three DNS zones and is overloaded. We need to configure TestKingD as authoritative for the corp.testking.com zone. This would decrease the workload on TestKingA. First we create a new standard primary zone on TestKingD since TestKingD must be authoritative for this zone to take the workload off TestKingA. On TestKingA we must delegate the control of the subdomain corp.testking.com to TestKingD. This will stop TestKingA from being authoritative for this zone. Finally we should re-create any static DNS record entries in the DNS zone on TestKingD.

Incorrect Answers
A: TestKingA should not be authoritative for the corp.testking.com zone since TestKingA is the bottleneck.
B: TestKingA must delegate the control of the child domain corp.testking.com to TestKingD. If this task is not performed TestKingA would still be authoritative for this zone.
D: This proposed solution would revert to the previous situation which we are required to change.

QUESTION 209
You are the administrator of your company's Windows 2000 network. The network consists of four domains and five Active Directory sites. The network is configured as shown in the Exhibit.

Most company employees use portable computers. These employees report that they can browse the Web from their own offices but not when they travel to other company offices.

You want to use Group Policy to maintain consistent Internet settings for company employees. What should you do?

Exhibit:

A. Create a low security zone for each domain.
B. Create a low security zone for each site.
C. Configure each domain to maintain its own Microsoft Internet Explorer proxy settings.
D. Configure each site to maintain its own Microsoft Internet Explorer proxy settings.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: A likely cause of the problem is different proxy server settings in each site. Each site has a different name and IP address for the local Proxy server. We should therefore configure each site with its own Microsoft Internet Explorer proxy settings.

Incorrect Answers
A, B: The browser problem is not to lack of configuration of the low security zone.
C: This proposed solution would very well in the in the testking.com, newyork.testking.com, and in the arizona. testking.com domains. However, in the marketing.testking.com domain the Florida and the Alabama site would have different Microsoft Explorer proxy settings since their proxy servers have different names and IP addresses.

QUESTION 210
You are a member of the Enterprise Admins group in TestKing's Windows 2000 network. The network consists

of a single Active Directory site. The site contains one subnet, which has an IP address range of 10.5.0.0 and a subnet mask of 255.255.255.0.

The company opens a new branch office and adds 300 client computers to the network. Users report that network performance is slow.

You use a high-performance router to separate the network into two segments. Then, you add a domain controller TestKingB to the new segment named SegmentTK2. The network is now configured as shown in the exhibit.

Users no longer report problems with network performance. However, they now report that changes in Active Directory between the two segments take a long time to replicate.

You want directory replication between the two segments to take place every five minutes. What should you do?

Exhibit:

A. Create a new site and associate it with a new subnet that has an IP address range of 10.5.1.0 and a subnet mask of 255.255.255.0.
B. Associate the existing site with a new subnet that has an IP address range of 10.5.1.0 and a subnet mask of 255.255.255.0.
C. Change the subnet mask for SegmentTK1 from 255.255.255.0 to 255.255.254.0
D. Configure the router to pass broadcast packets between both segments.

Answer: B
Section: (none)

Explanation/Reference:
Explanation: The second domain controller TestKingB belongs to the default site. The replication between TestKingA and TestKingB is therefore considered to be inter-site replication which only occurs every 180 minutes by default. This is the reason for the slow changes in the Active Directory. To enable intra-site replication we add the new subnet of SegmentTK2 to the existing site. All changes in the Active Directory would then be replicated between the Domain Controllers within 5 minutes of the change.

Note: When a domain controller writes a change to its local copy of the Active Directory, a timer is started that determines when the domain controller's intra-site replication partners should be notified of the change. By default, this interval is 300 seconds (5 minutes).

Reference:

Microsoft Knowledge Base Article - Q232264, Replication Schedule for Intra-Site Replication Partners

Incorrect Answers
A: .If we create a second site we would only achieve inter-site replication. Inter-site replication should only occur over slow WAN links, not in a LAN: Furthermore, the default replication interval for inter-site replication is 180 minutes. However, the scenario requires a solution with scheduled replication every 5 minutes.
C: The subnet mask for segment is correct. There is no need to change it.
D: Routing broadcasts would decrease network performance. One of the advantages with routers is that they stop broadcasts. Furthermore, replication does not take place through broadcasts.

QUESTION 211
You are the administrator of your company's Windows 2000 network. The network consists of two domains: testking.com and us.testking.com. The testking.com domain is in native mode. The us.testking.com domain is in mixed mode and contains two Windows 4.0 BDCs that cannot be removed from the domain.

Company sales personnel need access to a shared folder in testking.com. All company sales personnel are members of a universal group that has Read permission for the shared folder.

When they attempt to open the shared folder, sales personnel in us.testking.com report that they receive the following error message: "Access denied". Sales personnel in testking.com do not report any problems.

You need to allow all sales personnel access to the shared folder. What should you do?

A. Convert us.testking.com to native mode.
B. Add a global catalog server to us.testking.com
C. Create a global group in us.testking.com
   Add the user accounts for the sales personnel in us.testking.com to the global group.
   Add the global group to the universal group.
D. Create a universal group in us.testking.com.
   Add the user accounts for the sales personnel in us.testking.com to the universal group.
   Grant the universal group the Read permission for the shared folder.
E. Create a global group in us.testking.com
   Add the user accounts for the sales personnel in us.testking.com to the global group.
   Grant the global group the Read permission for the shared folder.

Answer: C
Section: (none)

Explanation/Reference:
Explanation: In this scenario, some users in the mixed-mode domain us.testking.com want to have read access to a folder in the native mode domain testking.com. We can accomplish this by creating a new Global Group, to which all appropriate users in the us.testking.com domain are added, in the us.testking.com domain and add this Global group to the universal group in the testking.com domain that has read access to the folder. Even though the mixed-mode domain does not allow universal groups, a global group from a mixed-mode domain can be added to a universal group in another domain.

Incorrect Answers:
A: We cannot switch the us.testking.com domain to native mode because we have Windows NT 4.0 BDCs in the domain. When a domain has both Windows NT 4.0 and Windows 2000 servers, it must run in mixed mode.
B: The us.testking.com domain already contains a Global Catalog server. Therefore we need not add another Global Catalog server to the domain, as a domain does not require more than one Global Catalog server.
D: A mixed mode domain does not allow us to create a universal group.
E: Global groups are restricted to permissions and rights to resources within the domain. We cannot assign permissions to resources in other domains to global groups. In other words, a global group in the us.testking.com domain cannot be assigned read permissions on a shared folder in the testking.com domain.

QUESTION 212
You are the network administrator for TestKing Ltd. The network consists of a single Windows 2000 Active Directory domain named testking.internal. The network includes 20 servers running Windows 2000 Server and 700 client computers running Windows 2000 Professional.

All servers belong to the default computer container. All client computers belong to an organization unit (OU) named Clients. All domain controllers belong to the default domain controller OU. Name resolution and IP addressing are controlled by DNS, WINS, and DHCP.

You need to ensure that the DNS suffix in the system properties of each client computer is set to testking.com.

What should you do?

A. Create a new Group Policy object and link it to Clients.
   Set the configuration of the primary DNS suffix to testking.com.
B. Modify the default domain policy.
   Set the configuration of the primary DNS suffix to testking.com.
C. In the DHCP scope options, define the DNS domain name as testking.internal.
D. In the DHCP scope options, define the NIS domain name as testking.internal.

Answer: A
Section: (none)

Explanation/Reference:
Explanation: We can set the primary DNS suffix with a group policy. The policy should be linked to the OU containing the client computers, because we don't want to change the suffix on the servers.

Incorrect Answers:
B: Changing the domain policy would affect all computers, including servers.
C: This is the common way of doing it. However, this answer specifies testking.internal as the suffix. The question states that this should be set to testking.com.
D: Similar to answer C – testking.internal is wrong. Furthermore, NIS (Network information service) is used in UNIX/LINUX domains, not a windows domain.

QUESTION 213
You are the network administrator for TestKing Inc. The company has branch offices in Toronto, San Francisco, and Chicago. All offices are connected by high-speed links.

TestKing implements an Active Directory domain. Each branch office has a domain controller for the default domain. You create one site for each office and place the sites in your default site link. A help desk operator from Toronto contacts you to report a problem. Two hours ago, the operator changed the telephone number on the user property sheet for an employee in Chicago. However, the change is not yet replicated to the Chicago domain controller. According to business rules, changes made in one office must be replicated to all other offices in a timely manner.

When you try to force replication, it completes successfully. You must ensure that all changes are replicated every 15 minutes.

What should you do?

A. Create a new site link and add each of the three offices to the link. Make the cost 15.
B. Change the replication schedule for the server connection options to replicate four times an hour.
C. Create a script that forces replication from Chicago to Toronto four times an hour.

D. Change the replication schedule for the default site link to replicate every 15 minutes.

Answer: D
Section: (none)

Explanation/Reference:
Explanation: This will force any changes to be replicated within 15 minutes as required.

Incorrect Answers:
A: The cost of a link is used for routing. It has nothing to do with replication.
B: This is not the correct setting.
C: It is not necessary to create a script. Furthermore, changes must be replicated to all offices, not just between Chicago and Toronto.

QUESTION 214
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2000. Each client computer runs Windows NT Workstation 4.0, Windows 2000 Professional, or Windows XP Professional. The computer accounts for all client computers are located in an organizational unit (OU) named CompanyComputers. All user accounts are located in an OU named CompanyUsers.

TestKing has a written policy that requires a logon banner to be presented to all users when they log on to any client computer on the network. The banner must display a warning about unauthorized use of the computer.

You need to ensure that the logon banner appears when a user logs on to a client computer.

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

A. Create a Group Policy object (GPO) that includes the appropriate settings in the interactive logon section.
   Link the GPO to the domain.
B. Create a script that presents the required warning.
   Create a Group Policy object (GPO) that will cause the script to run during the startup process.
   Link the GPO to TestKingUsers OU.
C. Create a system policy file named Ntconfig.pol that includes the appropriate settings.
   Place a copy of this file in the appropriate folder on the domain controller.
D. Create a batch file named Autoexec.bat that presents the required warning.
   Copy the file to root folder on ***MISSING***

Answer: AC
Section: (none)

Explanation/Reference:

QUESTION 215
You are the network administrator for TestKing, a company that has three offices. The offices are in Boston, Chicago, and New York. All three offices are connected by leased lines as shown in the exhibit.

TestKing is deploying a Windows Server 2000 forest. You create a single Active Directory domain. You configure each office as a single site. You configure three domain controllers in NYSite. You create a domain controller in each of the other sites. You create site links based on the network topology. Each leased line is represented by a site link. Each site link connects only two sites. The cost and the schedule for all site links is the same. The sites and site links are named as shown in the following table.

Site link name	Linked site	Linked site
NYBoston	NYSite	BosSite
NYChi	NYSite	ChiSite
ChiBoston	ChiSite	BosSite

Users report that network requests between BosSite and ChiSite are taking much longer than they used to take. You discover that replication traffic is using an unacceptably large percentage of the bandwidth between BosSite and ChiSite

You need to reduce replication traffic over the ChiBoston site link.

What should you do?

Exhibit:

A. Create an SMTP-based connection object from a domain controller in NYSite to a domain controller in BosSite.
B. Increase the cost of the ChiBoston site link.
C. Create a site link bridge that includes the NYBoston and NYChi site links.
D. Increase the replication interval for the NYBoston site link.

Answer: B
Section: (none)

Explanation/Reference:

QUESTION 216
You are a network administrator for TestKing that has a main office and five branch offices. The network consists of six Active Directory domains. All servers run Windows Server 2000. Each office is configured as a single domain. Each office is also configured as an Active Directory site.

TestKing uses an application server that queries user information from the global catalog. You install application servers in the main office and in three branch offices. The network is configured as shown in the exhibit.

You monitor the WAN connections between the main office and each branch office and discover that the utilization increased from 70 percent to 90 percent. Users report slow response times when accessing information on the application server.

You need to place global catalog servers in offices where they will improve the response times for the application servers. You need to achieve this goal with a minimum amount of increase in WAN traffic.

In which office or offices should you place a new global catalog server or servers? (Choose all that apply)

Exhibit:

A. Berlin
B. Rio de Janeiro
C. New Delhi
D. St Petersburg
E. Cairo

Answer: BCD
Section: (none)

Explanation/Reference:

QUESTION 217
You are a network administrator for TestKing. The network consists of a single Active Directory domain with two sites. The Active Directory database is backed up every evening.

A network administrator in Site1 deletes an empty organizational unit (OU) named Projects. At about the same time, a network administrator in Site2 moves 20 existing user accounts into the Projects OU. Later, the administrator in Site2 discovers that the Projects OU was deleted from Active Directory. He cannot see the user accounts that he moved into the OU.

You need to provide an OU named Projects and add the 20 user accounts to the Projects OU. The users' access to network resources must not be affected by this process.

What should you do?

A. Perform an authoritative restore operation of the Projects OU and the user accounts on a domain controller in Site2.
B. Perform a nonauthoritative restore operation of the Projects OU and the user accounts on a domain controller in Site2.
C. Create a new OU named Projects.
   Create 20 new user accounts that have the same user principal name (UPN) prefix.
   Move the user accounts into the new Projects OU.
D. Create a new OU named Projects.
   Move the 20 user accounts from the LastAndFound container to the new Projects OU.

Answer: D
Section: (none)

Explanation/Reference:

QUESTION 218
You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains one root domain and one child domain. The forest also contains three separate sites, as shown in the Network Diagram exhibit.

The network is not fully routed and there is no direct physical connection between Site1 and Site3. Site links are not bridged.

You discover that the domain controllers for europe.testking.com located in Site1 have additional accounts that are not on the domain controllers for europe.testking.com located in Site3. You examine the directory service

log in Event Viewer on a domain controller for europe.testking.com- You discover the error message shown in the Error Message exhibit.

```
Event ID: 1311
    Source: NTDS KCC
    Category: Knowledge Consistency Checker
    Event Type: Error
    User: NT AUTHORITY\ANONYNOUS LOGON
    COMPUTER: Server1

Description: The Directory Service consistency checker has determined that there
is not enough physical connectivity published via the Active Directory Sites and
Services Manager to create a spanning tree connecting all the sites connecting the
Naming Context
DC=Europe, DC=testking, DC=com
```

You need to resolve the condition that is causing this error.

What should you do?

Exhibit:

A. Add a domain controller for the europe.testking.com domain to Site2.
B. Configure a site link bridge between the site links for Site1 and Site3.
C. Configure at least one domain controller in each site to be a global catalog server.
D. Create a site link between Site1 and Site3.

Answer: B
Section: (none)

Explanation/Reference: