



70-217

Implementing and Administering a Microsoft
Windows 2000 Directory Services Infrastructure

Q&A

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are not encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

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.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

QUESTION NO: 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: A, D, F

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 NO: 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: A, B, D, E

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 its own record in the DNS zone file. This will prevent the need to manually enter records in the DNS zone.

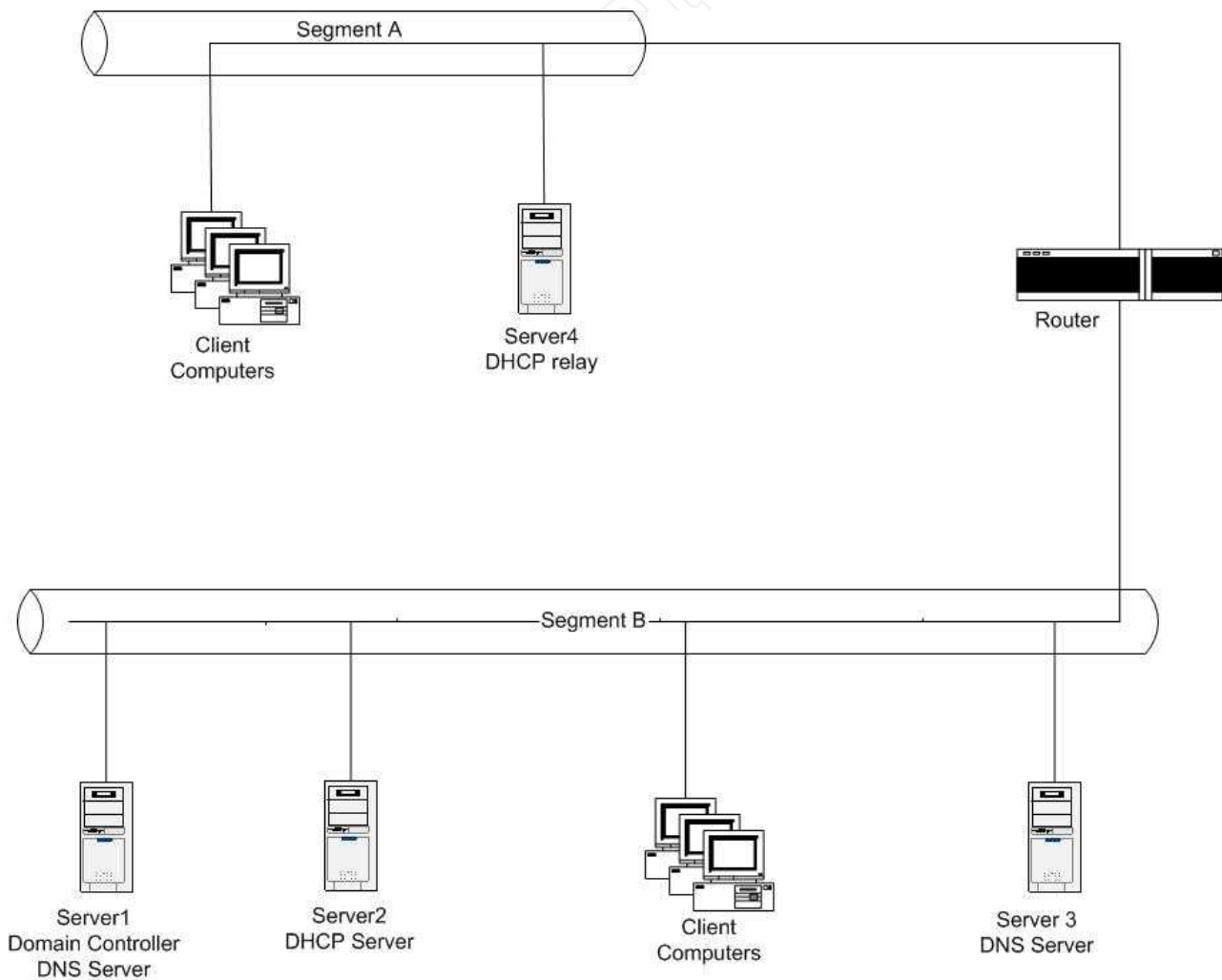
- D:** Selecting the “Allow Zone transfers only to the servers listed on the Name servers tab” option prevents unauthorized servers from updating the zone. Dynamic updates have been enabled.
- E:** Active Directory DNS zones replicate their data as part of Active Directory replication. Active Directory 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 NO: 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?

- 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

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 NO: 4

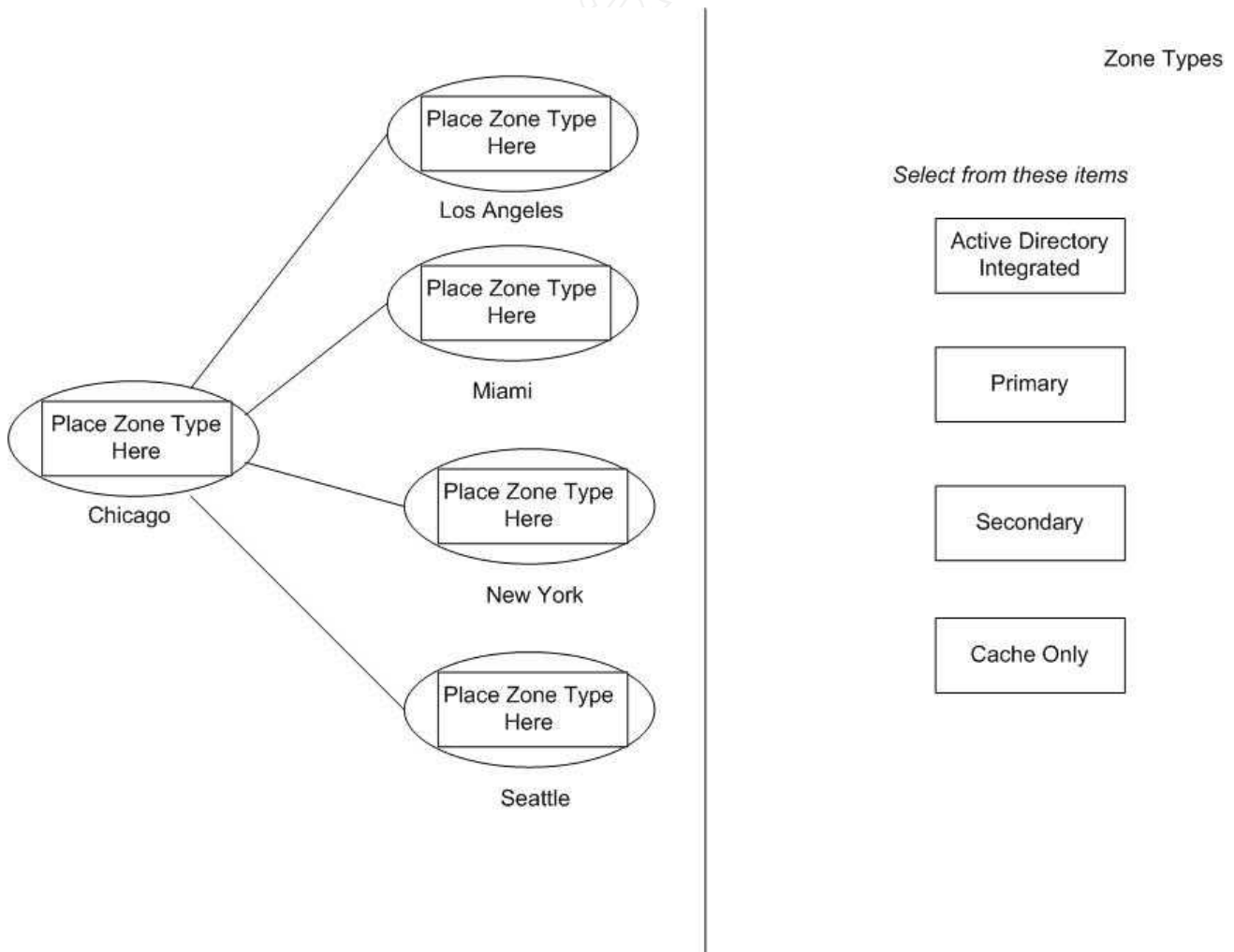
You are the administrator of a Windows 2000 network. Your network consists of five sites in one domain. The Chicago, Los Angeles, and New York sites will have DNS running on their Domain Controllers. Miami and Seattle will have DNS running on dedicated member servers.

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.

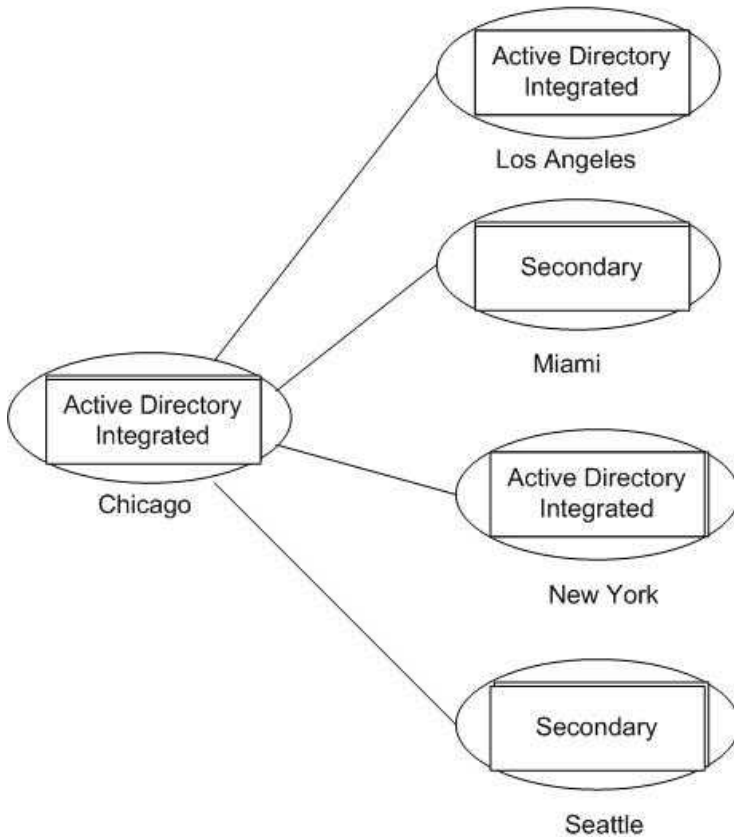
What should you do?

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)

Select And Place



Answer:



Zone Types

Select from these items

Active Directory Integrated

Primary

Secondary

Cache Only

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.

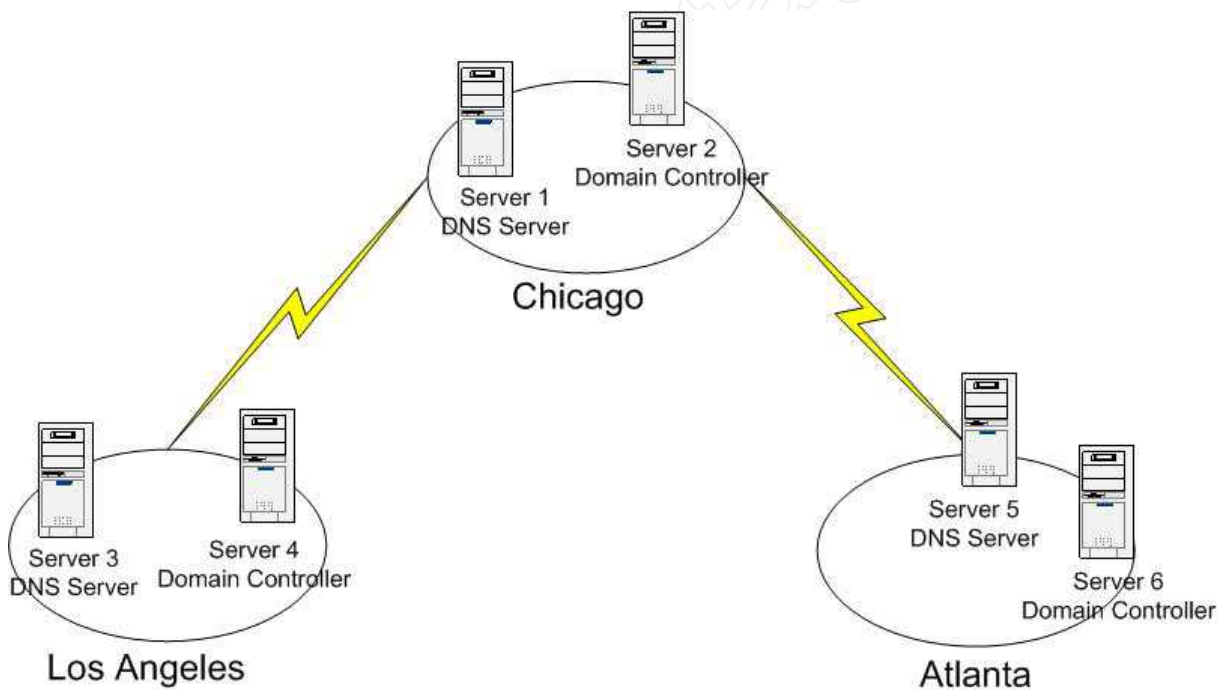
Miami: Secondary zone. A secondary zone is required for full zone replication. The question states a requirement for each location to have a full copy of the zone files. Only a secondary zone can receive a full copy of a zone file from a primary or Active Directory integrated zone.

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 NO: 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

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 NO: 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: B, E

Explanation:

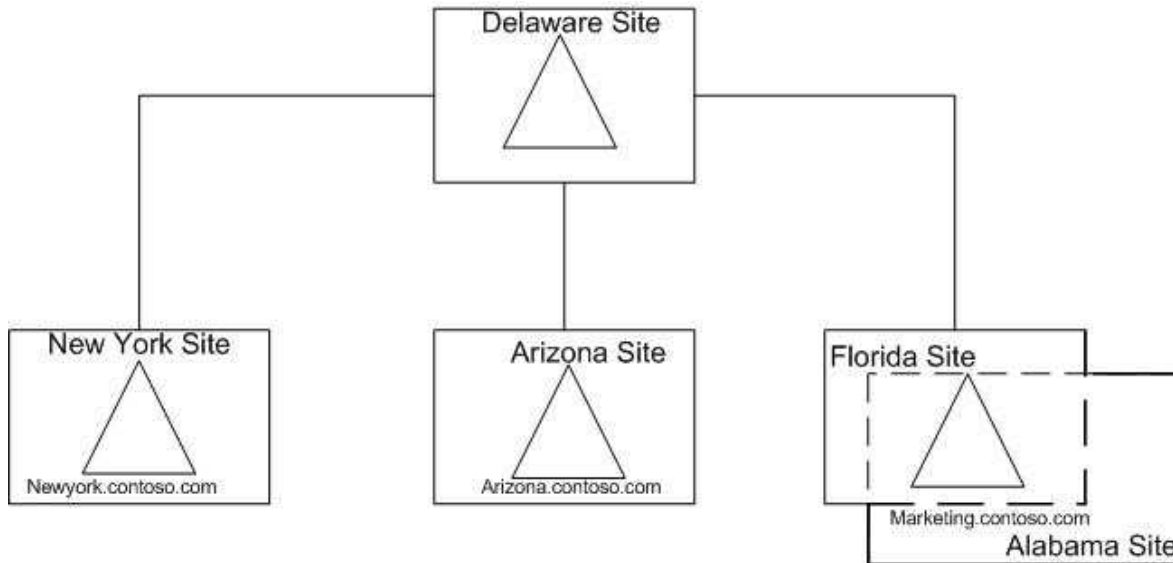
- B:** To install a new Domain Controller we must first install a computer as a member server and then promote it to a Domain Controller. To promote a member server to a Domain Controller, we need to run the Active Directory installation wizard. We can do this by clicking Start, Run and typing DCPROMO 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 NO: 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?

- Create a Group Policy Object for marketing.contoso.com that restricts group access to the HRadmins group.
- 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.
- In each domain except marketing.contoso.com, create a Group Policy Object that restricts group access to the HRadmins group.
- In each domain, create a Group Policy Object that restricts group access to the global security group in that domain.

Answer: A

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 NO: 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: A, F

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 NO: 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

Explanation: A site is comprised of one or more Internet Protocol (IP) subnets that are tied together by high-speed 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 NO: 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

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 NO: 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

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.