Microsoft

70-297

Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Exam

TYPE: DEMO

http://www.examskey.com/70-297.html

Examskey Microsoft 70-297 exam demo product is here for you to test the quality of the product. This Microsoft 70-297 demo also ensures that we have this product ready unlike most companies, which arrange the product for you as you order. These 70-297 exam questions are prepared by Microsoft subject matter specialists. Hence these are most accurate version of the 70-297 exam questions that you can get in the market.

We also offer bundle discount packages for every Microsoft certification track, so you can buy all related exam questions in one convenient bundle. And for corporate clients we also offer bundles for Microsoft certification exams at huge discount.

Check out our 70-297 Exam Page and Microsoft Certification Page for more details of these bundle packages.
Question: 1

You are the network administrator for Company. The network consists of a single Active Directory domain. The network contains three Windows Server 2003 domain controllers named ServerES1, ServerES2 and ServerES3. ServerES1 holds the schema master role and the domain naming master role. ServerES2 holds the relative ID (RID) master role. ServerES3 holds the PDC emulator master role and the infrastructure master role. ServerES2 fails and cannot be restarted. You log on to ServerES3 as the administrator and seize the RID master role. Later, ServerES2 is repaired and can be brought back online. You want ServerES2 to hold the RID master role again. What should you do?

A. Restart ServerES2 while it is connected to the network. Use the Ntdsutil utility and seize the RID master role. Reconnect ServerES2 to the network.
B. Restart ServerES2 while it is disconnected from the network. Use the Ntdsutil and seize the RID master role. Reconnect ServerES2 to the network.
C. Reinstall Windows Server 2003 on ServerES2. Restore the system state from the most recent backup to ServerES2. Reconnect ServerES2 to the network.

Answer: D

Explanation:
A domain controller whose RID master role has been seized can only be brought back online by reinstalling Windows Server 2003.

Incorrect Answers:
A: ServerES2 was the RID master before it failed. That role was seized to ServerES3. If we restart ServerES2, there will be two RID masters. Furthermore, we can only seize a role if the domain controller that holds that role fails.
B: We cannot seize the RID master role if ServerES2 is not connected to the network. Furthermore, we can only seize a role if the domain controller that holds that role fails.
C: ServerES2 was the RID master before it failed. That role was seized to ServerES3. However, if we bring ServerES2 back online, there will be two RID masters.

Reference:
Question: 2

You are a network administrator for Company. The network consists of two Active Directory domains. All servers run Windows Server 2003. Company has offices in New York and Rome. The two offices are connected by a 128-Kbps WAN connection. Each office is configured as a single domain. Each office is also configured as an Active Directory site. Company stores printer location information in Active Directory. Users frequently perform searches of Active Directory to find information on printers by selecting the Entire Directory option. Users in the New York Office report that response time is unacceptably slow when searching for printers. You need to improve the response time for users in the New York office. What should you do?

A. Place a domain controller for the Rome domain in the New York office.
B. Place a domain controller for the New York domain in the Rome office.
C. Enable universal group membership caching in the New York office.
D. Configure a global catalog server in the New York office.

**Answer: D**

**Explanation:**
The global catalog is the central repository of information about Active Directory objects in a tree or forest. The domain controller that holds a copy of the global catalog is called a global catalog server. The global catalog enables a user to log on to a network by providing universal group membership information to a domain controller when a logon process is initiated, and enables finding directory information regardless of which domain in the forest actually contains the data.

**Incorrect Answers:**
A: This would work but it is unnecessary. Replicating the entire Active Directory from the Rome office to the New York office over the slow WAN link is a waste of resources. A global catalog server in the New York office would suffice.
B: This won’t solve the problem at all.
C: Universal Group caching (as its name implies) caches information about universal groups. This scenario involves searching for printers which is nothing to do with universal groups.

**Reference:**
Question: 3

You are the network administrator for Company. The network consists of a single Active Directory forest that contains multiple domains. The functional level of the forest is Windows Server 2003. The forest contains several Active Directory sites that represent branch offices and a site named MainOffice that represent the central data center. A site named Branch1 contains one domain controller named Server1 that is not a global catalog server. The MainOffice site contains one domain controller named Server2 that is a global catalog server. You need to use universal group membership caching in the Branch1 site.

Which component or components should you configure? To answer, select the appropriate component or components in the work area.

Answer: Select the “NTDS Site Settings” for the Branch1 office in the right hand pane.
Explanation:
Universal group membership caching, is enabled or disabled in the NTDS Settings Properties dialog box of the Active Directory Sites and Services console. This must be performed in the site where you want to enable universal group membership caching, i.e., in the Branch1 site.

Question: 4

You are the network administrator for Company. The network consists of an internal network and a perimeter network. The internal network is protected by a firewall. The perimeter network is exposed to the Internet.
You are deploying 10 Windows Server 2003 computers as Web servers. The servers will be located in the perimeter network. The servers will host only publicly available Web pages.
You want to reduce the possibility that users can gain unauthorized access to the servers. You are concerned that a user will probe the Web servers and find ports or services to attack.
What should you do?
A. Disable File and Printer Sharing on the servers.
B. Disable the IIS Admin service on the servers.
C. Enable Server Message Block (SMB) signing on the servers.
D. Assign the Secure Server (Require Security) IPSec policy to the servers.

Answer: A

Explanation:
We can secure the web servers by disabling File and Printer sharing. The File and Printer Sharing for Microsoft Networks component allows other computers on a network to access resources on your computer by using a Microsoft network. This component is installed and enabled by default for all VPN connections. However, it needs to be enabled for PPPoE and dial-up connections. It is enabled per connection and is necessary to share local folders. The File and Printer Sharing for Microsoft Networks component is the equivalent of the Server service in Windows NT 4.0. File and Printer sharing is not required on web servers because the web pages are accessed over web protocols such as http or https, and not over a Microsoft LAN.

Incorrect Answers:
B: This is needed to administer the web servers. Whilst it could be disabled, disabling File and Printer sharing will secure the servers more.
You are the network administrator for Company. The network consists of a single Active Directory domain named Company.com. Company’s perimeter network contains 50 Web servers that host the company’s public Internet site. The Web servers are not members of the domain. The network design team completed a new design specification for the security of servers in specific roles. The network design requires that security settings must be applied to Web servers. These settings include password restrictions, audit settings, and automatic update settings.

You need to comply with the design requirements for securing the Web servers. You also want to be able to verify the security settings and generate a report during routine maintenance. You want to achieve these goals by using the minimum amount of administrative effort.

What should you do?

A. Create a custom security template named Web.inf that contains the required security settings. Create a new organizational unit (OU) named WebServers and move the Web servers into the new OU. Apply Web.inf to the WebServers OU.
B. Create a custom security template named Web.inf that contains the required security settings, and deploy Web.inf to each Web server by using Security Configuration and Analysis.
C. Create an image of a Web server that has the required security settings, and replicate the image to each Web server.
D. Manually configure the required security settings on each Web server.

Answer: B

Explanation:
The easiest way to deploy multiple security settings to a Windows 2003 computer is to create a security template with all the required settings and import the settings using the Security Configuration and Analysis tool.

Incorrect Answers:
A: The web servers are not domain members. Therefore they cannot be moved to an OU in Active Directory.
C: We cannot use imaging in this way.
D: This is a long way of doing it. A security template would simplify the task considerably.
You are a network administrator for Contoso, Ltd. The network consists of a single Active Directory forest as shown in the exhibit.

Your company’s written security policy requires that all domain controllers in the child1.contoso.com domain must accept a LAN Manager authentication level of only NTLMv2. You also want to restrict the ability to start a domain controller to the Domain Admins group. You need to configure the domain controllers in the child1.contoso.com domain to meet the new security requirements. Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)

A. Import the Rootsec.inf security template into the Default Domain Controllers Policy Group Policy object (GPO) in the child1.contoso.com domain.
B. Import the Rootsec.inf security template into the Default Domain Policy Group Policy object (GPO) in the child1.contoso.com domain.
C. Import the Securedc.inf security template into the Default Domain Controllers Policy Group Policy object (GPO) in the child1.contoso.com domain.
D. Import the Securedc.inf security template into the Default Domain Policy Group Policy object (GPO) in the child1.contoso.com domain.
E. Run the system key utility (syskey) on each domain controller in the child1.contoso.com domain. In the Account Database Key dialog box, select the Password Startup option.
F. Run the system key utility (syskey) on each domain controller in the child1.contoso.com domain. In the Account Database Key dialog box, select the Store Startup Key Locally option.

Answer: C, E
Explanation: Secure (Secure*.inf) Template - The Secure templates define enhanced security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings. Additionally, the Secure templates limit the use of LAN Manager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LAN Manager responses. In order to apply Securews.inf to a member computer, all of the domain controllers that contain the accounts of all users that log on to the client must run Windows NT 4.0 Service Pack 4 or higher. The system key utility (SYSKEY) is a security measure used to restrict logon names to user accounts and access to computer systems and resources. By running the syskey utility with the Password startup option, the account information in the directory services is encrypted and a password needs to be entered during system start. The start of the Domain Controllers is therefore restricted to everybody with this password.

Incorrect Answers:
A: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
B: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
D: We need to apply the policy to the domain controllers container, not the entire domain.
F: The System Key Utility (syskey) is used to encrypt the account password information that is stored in the SAM database or in the directory services. By selecting "Store Key locally" the computer stores an encrypted version of the key on the local computer. This doesn’t help in controlling the start of the Domain Controllers.

Reference:

Question: 7

You are a network administrator for your company. The network consists of a single Active Directory domain. The functional level of the domain is Windows Server 2003. All domain controllers run Windows Server 2003. The domain controllers are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Server name</th>
<th>Server role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server1</td>
<td>Global catalog server, schema master, domain naming master</td>
</tr>
<tr>
<td>Server2</td>
<td>Domain controller, infrastructure master, PDC emulator</td>
</tr>
<tr>
<td>Server3</td>
<td>Domain controller</td>
</tr>
<tr>
<td>Server4</td>
<td></td>
</tr>
</tbody>
</table>

Complete collection of 70-296 Exam's Question and answers.
http://www.ExamsKey.com
Global catalog server, relative ID (RID) master
You plan to take Server4 offline for maintenance. Another network administrator plans to add 1,250 new user accounts while Server4 is offline. You need to ensure that the network administrator can add the user accounts while Server4 is offline. You also need to ensure that there is no disruption of user account creation after Server4 is brought back online. Which two actions should you take? (Each correct answer presents part of the solution.

A. Connect to Server3 by using the Ntdsutil utility.
B. Connect to Server4 by using the Ntdsutil utility.
C. Remove the global catalog server role from Server4.
D. Add the global catalog server role to Server3.
E. Transfer the RID master role.

Answer: A, E

Explanation:
The RID master is assigned to allocate unique sequences of relative IDs to each domain controller in its domain. As the domain controllers use the IDs allocated, they contact the RID master and are allocated additional sequences as needed. At any time, the RID master role can be assigned to only one domain controller in each domain. The Relative ID is part of a security ID (SID) that uniquely identifies an account or group within a domain. We will be creating 1250 new user accounts so the domain controller will need to contact the RID master to obtain more RIDs. We can transfer the RID master role using the ntdsutil utility.

Incorrect Answers:
B: We need to connect to the computer we will be transferring the role to, not from.
C: We have a Global Catalog on Server4. We don’t need another one.
D: Server3 is already a global catalog server.

Question: 8

You are the network administrator for Tailspin Toys. The network consists of a single Active Directory forest. The functional level of the forest is Windows 2000. The forest consists of a root domain named tailspintoy.com and two child domains named child1.tailspintoy.com and child2.tailspintoy.com. The functional level of all domains is Windows 2000 native. All domain controllers in the tailspintoy.com domain run Windows Server 2003. All domain controllers in the child1.tailspintoy.com and child2.tailspintoy.com domains run Windows 2000 Server. You need to able to rename all domain controllers in tailspintoy.com. You want to minimize impact to the network. What should you do? To answer, drag the appropriate action or actions to the correct location or locations in the work area.

Complete collection of 70-296 Exam's Question and answers.
http://www.ExamsKey.com
Question: 9

You are a network administrator for Company. The network consists of an intranet and a perimeter network, as shown in the work area. The perimeter network contains:
All servers on the perimeter network are members of the same workgroup. The design team plans to create a new Active Directory domain that uses the existing servers on the perimeter network. The

Complete collection of 70-296 Exam's Question and answers.
http://www.ExamsKey.com
new domain will support Web applications on the perimeter network. The design team states that the perimeter network domain must be fault tolerant. You need to select which server or servers on the perimeter network need to be configured as domain controllers. Which server or servers should you promote?

To answer, select the appropriate server or servers in the work area.
Explanation:
We know web editions can’t be domain controllers, and we want fault tolerance, which means two Domain Controllers. The answer is promote the two servers to dc’s (Company2 and Company3).

Reference:

Question: 10

You are a network administrator for Company. The network consists of a single Active Directory forest. All domain controllers run Windows Server 2003. The bank decides to provide access to its mortgage application services from a real estate agency that has offices throughout the country. You install a Company domain controller in each real estate agency office. You need to further protect the domain controllers’ user account databases from unauthorized access. You want to achieve this goal by using the minimum amount of administrative effort. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A. Use the system key utility (syskey) with the most secure security level on the domain controllers.
B. Create a Group Policy object (GPO), import the Securedc.inf security template, and apply the GPO to the domain controllers.
C. Create a Group Policy object (GPO), configure the Network security: LAN Manager authentication level security option to the Send NTLMv2 response only\refuse LM setting, and apply the GPO to the domain controllers.
D. Create a Group Policy object (GPO), import the DC security.inf security template, and apply the GPO to the domain controllers.

Answer: A, B

Explanation:
On domain controllers, password information is stored in directory services. It is not unusual for password-cracking software to target the Security Accounts Manager (SAM) database or directory services to access passwords for user accounts. The System Key utility (Syskey) provides an extra line of defence against offline password-cracking software. Syskey uses strong encryption techniques to secure account password information that is stored in directory services. Mode 3 is the most secure Syskey utility, because it uses a computer-generated random key and stores the key on a floppy disk. This disk is required for the system to start, and it must be inserted at a prompt during the startup sequence. The system key is not stored anywhere on the computer.

Secure (Secure*.inf) Template
The Secure templates define enhanced security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings. Additionally, the Secure templates limit the use of LAN Manager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LAN Manager responses.

Incorrect Answers:
C: You should be importing the Securedc.inf security template instead of configuring the Network security: LAN Manager authentication level security option to the Send NTLMv2 response only\refuse LM setting.
D: DC Security.inf templates contain a large number of settings, and in particular a long list of file-system permission assignments. For this reason, you should not apply these templates to a computer by using group policies.

Reference:
You are the network administrator for Company. The company has a main office and 20 branch offices.

You recently completed the design of the company network. The network design consists of a single Active Directory domain named Company.com. All domain controllers will run Windows Server 2003. The main office will contain four domain controllers, and each branch office will contain one domain controller. The branch office domain controllers will be administered from the main office.

You need to ensure that the domain controllers are kept up-to-date with software updates for Windows Server 2003 after their initial deployment. You want to ensure that the domain controllers automatically install the updates by using the minimum amount of administrative intervention. You also want to configure the settings by using the minimum amount of administrative effort.

What should you do?

A. In System Properties, on the Automatic Update tab, enable Keep my computer up to date, and then select Download the updates automatically and notify me when they are ready to be installed.

B. In the Default Domain Controllers Policy Group Policy object (GPO), enable Configure Automatic Updates with option 3 – Auto download and notify for install.

C. In the Default Domain Controllers Policy Group Policy object (GPO), enable Configure Automatic Updates with option 4 – Auto download and schedule the install.

D. In System Properties, on the Automatic Updates tab, enable Keep my computer up to date, and then select Automatically download the updates, and install them on the schedule that I specify.

Answer: C

Explanation:
The question states that You want to ensure that the domain controllers automatically install the updates by using the minimum amount of administrative intervention. The way to do this is to configure the automatic updates with the option to Auto download and schedule the install. The easiest way to configure the domain controllers with this setting is to configure a group policy object for the domain controllers.

The problem with this solution is that the domain controllers may automatically restart after the updates are installed. Scheduling the updates to install out of business hours will minimize any disruption.

Incorrect Answers:
A: It is easier to configure the domain controllers using group policy.
B: This solution will download the updates, but it won’t install them until an administrator manually clicks the install button in the notification dialog box. Answer C automates the procedure more by scheduling the installation to occur at a set time without any further administrative intervention.
D: It is easier to configure the domain controllers using group policy.

Reference:
You are the network administrator for Company. The network consists of a single Active Directory domain named Company.com. The company plans to deploy 120 Windows Server 2003 member servers as file servers in the domain.

The new file servers will be located in a single organizational unit (OU) named File Servers. The security department provides you with a security template that must be applied to the new file servers. You need to apply and maintain the security settings contained in the security template to the new file servers. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

A. On a reference computer, use the Local Security Settings console to import the security template. Use imaging technology to install and configure the new file servers based on the configuration of the reference computer.
B. On a reference computer, run the secedit command to apply the security template. Use imaging technology to install and configure the new file servers based on the configuration of the reference computer.
C. Create a new Group Policy object (GPO). Import the security template into the Security Settings of the Computer Configuration section of the GPO. Link the GPO to the File Servers OU.
D. On the PDC emulator master in the domain, run the secedit command to apply the security template.

Answer: C

Explanation:
We have a security template with the required security settings. We can simply import the template into a Group Policy Object and apply the settings to the File Servers OU.

Incorrect Answers:
A: This would work, but there is a catch in the question. The question states that you need to apply and maintain the security settings contained in the security template to the new file servers. Using a GPO, the settings will be periodically refreshed, ensuring that the security settings ‘maintained’.
B: This would work, but there is a catch in the question. The question states that you need to apply and maintain the security settings contained in the security template to the new file servers. Using a GPO, the settings will be periodically refreshed, ensuring that the security settings ‘maintained’.
D: This would have no effect on the file servers.

Reference:

Each domain contains two Windows Server 2003 domain controllers named DC1 and DC2. DC1 in the Company.com domain performs the following two operations master roles: schema master and domain naming master. DC1 in each child domain performs the following three operations master roles: PDC emulator master, relative ID (RID) master, and infrastructure master. DC1 in each domain is also a global catalog server.

The user account for Sheets Sheet in the africa.Company.com domain is a member of the Medicine Students security group. Because of a name change, the domain administrator of africa.Company.com changes the Last name field of Sheets’s user account from Sheet to Edwards. The domain administrator of asia.Company.com discovers that the user account for Sheets is still listed as Sheets Sheet.

You need to ensure that the user account for Sheets Edwards is correctly listed in the Medicine Students group.

What should you do?

A. Transfer the PDC emulator master role from DC1 to DC2 in each domain.
B. Transfer the infrastructure master role from DC1 to DC2 in each domain.
C. Transfer the RID master role from DC1 to DC2 on each domain.
D. Transfer the schema master role from DC1 to DC2 in the Company.com domain.

Answer: B

Explanation:
Problems like this can occur when the Infrastructure master role is on the same domain controller as the Global Catalog.

The infrastructure master updates the group-to-user reference whenever group memberships change and replicates these changes across the domain. The infrastructure master compares its data with that of a global catalog. Global catalogs receive regular updates for objects in all domains through replication, so the global catalog data will always be up to date. If the infrastructure master finds that its data is out of date, it requests the updated data from a global catalog. The infrastructure master then replicates that updated data to the other domain controllers in the domain. Unless there is only one domain controller in the domain, the infrastructure master role should not be assigned to the domain controller that is hosting the global catalog. If the infrastructure master and global catalog are on the same domain controller, the infrastructure master will not function. The infrastructure master will never find data that is out of date, so it will never replicate any changes to the other domain controllers in the domain. Transferring the Infrastructure master role to a different computer would resolve this problem. There is no reason to transfer any other master roles.

Incorrect Answers:
A: The PDC Emulator is responds to Windows NT 4 BDCs. It also receives all new password and lockout information changes immediately for the entire domain. Neither of these functions will ensure that the user account changes are updated in the domain.
C: The RID Master keeps track of the allocation RIDs to domain controllers to ensure that two
domain controllers do not hand out the same SID.
D: The Schema Master controls what is allowed in the Active Directory directory.

Reference:

Question: 14

You are the network administrator for Company. The network consists of a single Active Directory
domain with two sites. Each site contains two domain controllers. One domain controller in each site
is a global catalog server.
You add a domain controller to each site. Each new domain controller has a faster processor than
the existing domain controllers.
Company requires Active Directory replication to flow through the servers that have the most
powerful CPUs in each site.
You need to configure the intersite replication to comply with Company’s requirement for Active
Directory replication.
What should you do?

A. Configure the new domain controllers as global catalog servers.
B. Configure the new domain controller in each site as a preferred bridgehead server for the IP
transport.
C. Configure the new domain controller in each site as a preferred bridgehead server for the SMTP
transport.
D. Configure an additional IP site link between the two sites. Assign a lower site link cost to this site
link than the site link cost for the original site link.

Answer: B

Explanation:
Directory information is replicated both within and among sites. Active Directory replicates
information within a site more frequently than across sites. This balances the need for up-to-date
directory information with the limitations imposed by available network bandwidth. You can
customize how Active Directory replicates information using site links to specify how your sites are
connected. Active Directory uses the information about how sites are connected to generate
Connection objects that provide efficient replication and fault tolerance. You provide information
about the cost of a site link, times when the link is available for use and how often the link should be
used. Active Directory uses this information to determine which site link will be used to replicate
information. Customizing replication schedules so replication occurs during specific times, such as
when network traffic is low, will make replication more efficient. Ordinarily, all domain controllers
are used to exchange information between sites, but you can further control replication behavior by
specifying a bridgehead server for inter-site replicated information. A bridgehead server is dedicated
for inter-site replication. You can also establish a bridgehead server when your deployment uses
proxy servers, such as for sending and receiving information through a firewall.
Incorrect Answers:
A: The global catalog is the central repository of information about Active Directory objects in a tree or forest. The domain controller that holds a copy of the global catalog is called a global catalog server. The global catalog enables a user to log on to a network by providing universal group membership information to a domain controller when a logon process is initiated, and enables finding directory information regardless of which domain in the forest actually contains the data. It does not control replication.
C: You can use either IP or SMTP as the protocol for replication traffic. However, SMTP replication requires an Enterprise Certification Authority (ECA) because Public Key encryption and certificates are used to verify identity of domain controllers and provide digital signatures.
D: We can control the flow of replication traffic by creating a new site link with a lower cost. Replication will then occur across the site link with the lower cost. However, this option does not specify that the new site link must be between MainDC3 and BranchDC3.

Reference:

Question: 15
You are the network administrator for Company. The network consists of a single Active Directory forest that contains five domains. The functional level of the forest is Windows 2000. You have not configured any universal groups in the forest.
One domain is a child domain named usa.Company.com that contains two domain controllers and 50 client computers. The functional level of the domain is Windows Server 2003. The network includes an Active Directory site named Site1 that contains two domain controllers. Site1 represents a remote clinic and the location changes every few months. All of the computers in usa.Company.com are located in the remote clinic. The single WAN connection that connects the remote clinic to the main network is often saturated or unavailable. Site1 does not include any global catalog servers. You create several new user accounts on the domain controllers located in Site1.
You need to ensure that users in the remote clinic can always quickly and successfully log on to the domain.
What should you do?

A. Enable universal group membership caching in Site1.
B. Add the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key to the registry on both domain controllers in Site1.
C. Add the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key to the registry on all global catalog servers in the forest.
D. Raise the functional level of the forest to Windows Server 2003.

Answer: B

Explanation:
When all domain controllers are at least Windows 2000 domain controllers and the domain is switched to Windows 2000 native mode, the usage of universal groups. When processing a logon request for a user in a native-mode domain, a domain controller sends a query to a global catalog server to determine the user's universal group memberships. Since you can explicitly deny a group access to a resource, complete knowledge of a user’s group memberships is necessary to enforce access control correctly. If a domain controller of a native-mode domain cannot contact a global catalog server to determine universal group membership when a user wants to log on, the domain controller refuses the logon request. The following registry key can be set so that the domain controller ignores the global catalog server failure when expanding universal groups:  
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures
The domain controller still tries to connect to the global catalog server, however, and the timeout for that query must expire.

Incorrect Answers:
A: Universal group membership caching allows the domain controller to cache universal group membership information for users. This eliminates the need for a global catalog server at every site in a domain, which minimizes network bandwidth usage because a domain controller does not need to replicate all of the objects located in the forest. It also reduces logon times because the authenticating domain controllers do not always need to access a global catalog to obtain universal group membership information. However, new user accounts would not be located on the global catalog until Active Directory replication occurs.
B: Logon requests are processed by the domain controller; therefore, the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key must be added to the registry the both domain controllers in Site1, not the global catalog servers.
D: Raising the functional level of the forest to Windows Server 2003 won’t solve the problem as Windows 2000 native mode is sufficient.

You are a network administrator for Company. Company is developing a new Web application that connects to an SQL back-end environment. The design team decides that the new application must be fault tolerant. You interview the Web developers and the SQL administrators to establish the size of the environment.

The Web developers state that they need at least three Web servers to share the load. Each Web server requires two processors and 1 GB of RAM. The Web developers state if one of the Web servers fails, the Web application can run for several hours in a degraded state. Responsiveness will be below specifications in a degraded state.

The SQL administrators state that they need two Microsoft SQL Server computers to support the new application. They want the SQL server environment to be redundant. Each SQL Server computer requires four processors and 3 GB of RAM. The SQL administrators state that only one SQL Server computer is required to maintain the application.

You need to ensure that two of the Web servers and one of the SQL Server computers are always available. You need to select the lowest edition of Windows Server 2003 that meets the requirements in order to minimize costs.

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

C. Install Windows Server 2003, Enterprise Edition on all three Web servers. Install a shared fiber-attached disk array for the Web servers. Implement a three-node server cluster for the Web servers. Configure the cluster so that all three nodes are active.
F. Install Windows Server 2003, Enterprise Edition on both SQL Server computers. Install a shared fiber-attached disk array for the SQL Server computers. Implement a two-node server cluster for the SQL servers. Configure the cluster so that one node is active and the second node is a hot standby node.

Answer: A, F

Explanation:
For the web servers we can three servers connected using Network Load Balancing. We can use Network Load Balancing because the content will be the same on the web servers. Windows Server 2003 Web Edition supports Network Load Balancing. For the SQL servers we need a two-node server cluster. For a server cluster, we need Windows Server 2003 Enterprise edition.

Incorrect Answers:
C: We can use Network Load Balancing because the content will be the same on the web servers. We don’t need a server cluster.
D: We can’t use Network Load Balancing for the SQL servers. Network Load Balancing should only be used when you have static content.

E: We can’t use Network Load Balancing for the SQL servers. Network Load Balancing should only be used when you have static content.

Reference:

Question: 17

You are the network administrator for Company. The network contains a single Active Directory domain named company.com. All computers on the network are members of the domain.
Company has a main office and 20 branch offices. Each branch office has a connection to the main office. Only the main office has a connection to the Internet.
You are planning a security update infrastructure for your network. You deploy a central Software Update Services (SUS) server at the main office and an SUS server at each branch office. The SUS server at the main office uses Windows Update to obtain security patches.
You want to minimize the amount of bandwidth used on the connection to the Internet and on the connection between the offices to download security patches.
Which two actions should you take?  (Each correct answer presents part of the solution. (Choose two)

A. Configure the SUS servers at the branch office to use Windows Update to obtain security patches.
B. Configure the SUS servers at the branch offices to use the central SUS server for updates.
C. Configure Automatic Updates on the SUS servers at the branch offices to use the central SUS server for updates.
D. Configure Automatic Updates on all computers to use the SUS server on the local network.
E. Configure Automatic Updates on all computers to use the default update service location.

Answer: B, D

Explanation:
We must set up the SUS branch offices server to pickup the updates form the server in the main office. By configuring a SUS server in the main office you save network bandwidth, because the branch office servers will not need to use the internet connection. With this solution, the main office SUS server downloads the updates from Microsoft; the branch office SUS servers download the updates from the main office SUS server and the client computers download the updates from the local SUS server.
Incorrect Answers:
A: This is an unnecessary use of the internet connection.
C: You need to configure the SUS server software to download the updates, not automatic updates.
E: The default update service location is Microsoft. This is an unnecessary use of the internet connection.

Reference:

Question: 18

You are the network administrator for Company. Company is deploying a public Web server farm on Windows Server 2003 computers. This Web server farm will allow the public to view company information. The Web servers in the Web server farm will be placed in Company’s perimeter network, which uses a public Internet address space. Company wants to reduce the probability of external unauthorized users breaking into the public Web servers.
You need to make the Web servers less vulnerable to attack. You also want to ensure that the public will be able to view information that is placed in Company’s perimeter network.
What should you do?

A. Configure each Web server’s IP address to a private reserved Internet address.
B. Configure the Web servers to allow only IPSec communications.
C. Disable any unneeded services on the Web servers.
D. Disable TCP/IP filtering on all adapters in the Web servers.

Answer: C

Explanation:
We should disable any unneeded services on the Web servers. This includes unneeded web services and unneeded server services. This will also ensure that no unnecessary ports are open on the servers.

Reducing the Attack Surface of the Web Server
Immediately after installing Windows Server 2003 and IIS 6.0 with the default settings, the Web server is configured to serve only static content. If your Web sites consist of static content and you do not need any of the other IIS components, then the default configuration of IIS minimizes the attack surface of the server. When your Web sites and applications contain dynamic content, or you require one or more of the additional IIS components, you will need to enable additional features. However, you still want to ensure that you minimize the attack surface of the Web server. The attack surface of the Web server is the extent to which the server is exposed to a potential attacker.
However, if you reduce the attack surface of the Web server too much, you can eliminate functionality that is required by the Web sites and applications that the server hosts. You need to ensure that only the functionality that is necessary to support your Web sites and applications is enabled on the server. This ensures that the Web sites and applications will run properly on your Web server, but that the attack surface is minimized.
Incorrect Answers:
A: The public web servers need public IP addresses.
B: You can’t use IPSec on public web servers. No one would be able to access the web pages.
D: TCP/IP filtering should be enabled, not disabled.

Reference

Question: 19


You attempt to promote Company3 to be an additional domain controller of the mombasa.Company.com domain. The promotion fails and you receive the error message shown in the exhibit.

You need to resolve the error in order to promote Company3 to be an additional domain controller of the mombasa.Company.com domain.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A. Force replication between the schema master and the PDC emulator of only the Company.com domain.
B. Force replication between the schema master and the PDC emulator of the Company.com domain and the mombasa.Company.com domain.
C. Run the adprep /forestprep command on the schema master of the Company.com domain.
D. Run the adprep /domainprep command on the infrastructure master of only the Company.com domain.
E. Run the adprep /domainprep command on the infrastructure masters of the Company.com domain and the mombasa.Company.com domain.

Answer: C, E

Explanation:
To promote a Windows Server 2003 member server to a domain controller in a Windows 2000 domain, You must run the adprep /forestprep command on the existing Windows 2000 Server domain controller holding the schema operations master role. You must also run the adprep /domainprep command on the Windows 2000 Server domain controller holding InfrastructureOperations Master role for the domain that you are going to upgrade.
Incorrect Answers:A, B: The PDC Emulator is used for authentication purposes for Windows NT 4.0 machines.
D: You must run the adprep /domainprep command on the Windows 2000 Server domain controller holding Infrastructure Operations Master role for the domain that you are going to upgrade, i.e., miami.Company.com.

Question: 20

You are the network administrator for your company. The Company consists of two subsidiaries named Contoso, Ltd., and City Power & Light. The network contains two Active Directory forests. The functional level of each domain is Windows 2000 native. All domain... controllers run
User accounts and resources are located in the child domains. All user principal names (UPNs) in each forest comply with a standard company e-mail address.

Each domain controller functions as a DNS server. All DNS zones are Active Directory-integrated zones. The Contoso.com and cpandl.net DNS zones have no root (".") zone. DNS servers in each forest root DNS zone are configured with root hints to Internet root servers.

You upgrade each domain controller in both forests to Windows Server 2003. You raise the functional level for each domain to Windows Server 2003. You plan to implement a smart-card authentication strategy for the entire company.

You need to ensure that users are able to access resources in all domains in each forest and on the Internet. You want to accomplish this task by using the minimum amount of administrative effort. You also need to ensure that access to resources is not disrupted.

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

A. Create a two-way external trust relationship between the two forest root domains. Raise the functional level of the forest to Windows Server 2003.
B. Raise the functional level of the forest to Windows Server 2003. Replace existing trust relationships with a two-way forest trust relationship between the two forest root domains.
C. Create root hints between DNS servers in each child domain and DNS servers in the root domain for the opposite forest.
D. Create conditional DNS forwarders between domain controllers in each root domain.

Answer: B, D

Explanation:
Raising the forest functional level to Windows Server 2003 enables you to take advantage of all Windows Server 2003 forest-level features. If any domains in the forest are still operating at the Windows Server 2003 interim functional level, you will be unable to raise the forest functional level to Windows Server 2003. Ensure that all domains are operating at the Windows Server 2003 functional level before you raise the forest functional level. To have a complete trust between all the Company domains and all the mimex domains, we need to create a forest trust relationship between the two forest root domains. This can only be done after the functional level of the forests has been raised to Windows Server 2003.
raised to Windows Server 2003. If your internal network does not have a private root and your users need access to other namespaces, such as a network belonging to a partner company, use conditional forwarding to enable servers to query for names in other name spaces. Conditional forwarding in Windows Server 2003 DNS eliminates the need for secondary zones by configuring DNS servers to forward queries to different servers based on the domain name. In order to avoid traffic and get the resources from any of the forest we need to configure conditional forwarding in each zone. With option D we will create in Company.com a conditional forwarder to mimex.com, and in mimex.com a conditional forwarder to Company.com.

Incorrect answers:
A: In order to create a two-way external trust relationship between the two forest root domains, you first need to raise the functional level of the forest to Windows Server 2003
C: There is no need to root hints between DNS servers in each child domain when all that is necessary is to create conditional forwarding between the two domain controllers in each root domain.

Reference:
Thank You for Trying Our Product

Microsoft

70-297

Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Exam

TYPE: DEMO

http://www.examskey.com/70-297.html

View list of All certification exams:
http://www.examskey.com/all_certifications.php

• Average 100% Success Rate.
• 100% Money Back Guarantee
• Study Material Updated On Regular Basis.
• Instant Download Access! After Purchased
• Services Of Professional & Certified Experts Available Via Support
• Round-The-Clock Client Support, Safe Website For Shopping

Besides money back guarantee, we also offer 3 months free updates to the 70-297 exam questions to reflect the changes as (& if) they are introduced by the Microsoft.