Microsoft

Exam Questions 70-640

Windows Server 2008 Active Directory - Configuring
**NEW QUESTION 1**
At the ntdsutil prompt, type files, and then press ENTER.

**Answer:**

**NEW QUESTION 2**
Your company has an Active Directory domain. All servers run Windows Server 2008 R2. Your company uses an Enterprise Root certification authority (CA) and an Enterprise Intermediate CA.

The Enterprise Intermediate CA certificate expires.

You need to deploy a new Enterprise Intermediate CA certificate to all computers in the domain.

What should you do?

A. Import the new certificate into the Intermediate Certification Store on the Enterprise Root CA server
B. Import the new certificate into the Intermediate Certification Store on the Enterprise Intermediate CA server
C. Import the new certificate into the Intermediate Certification Store in the Default Domain Controllers group policy object
D. Import the new certificate into the Intermediate Certification Store in the Default Domain group policy object

**Answer:** B

**Explanation:**

Certification Authority Trust Model Certification Authority Hierarchies The Windows 2000 public key infrastructure supports a hierarchical CA trust model, called the certification hierarchy, to provide scalability, ease of administration, and compatibility with a growing number of commercial third-party CA services and public key-aware products. In its simplest form, a certification hierarchy consists of a single CA. However, the hierarchy usually contains multiple CAs that have clearly defined parent-child relationships. Figure 16.5 shows some possible CA hierarchies.

C:\Documents and Settings\usernwz1\Desktop\1.PNG

You can deploy multiple CA hierarchies to meet your needs. The CA at the top of the hierarchy is called a root CA. Root CAs are the most trusted CAs in the organization and it is recommended that they have the highest security of all. There is no requirement that all CAs in an enterprise share a common top-level CA parent or root. Although trust for CAs depends on each domain's CA trust policy, each CA in the hierarchy can be in a different domain. Child CAs are called subordinate CAs. Subordinate CAs are certified by the parent CAs. A parent CA certifies the subordinate CA by issuing and signing the subordinate CA certificate. A subordinate CA can be either an intermediate or an issuing CA. An intermediate CA issues certificates only to subordinate CAs. An issuing CA issues certificates to users, computers, or services.

**NEW QUESTION 3**
Your company has an Active Directory domain that has an organizational unit named Sales. The Sales organizational unit contains two global security groups named sales managers and sales executives.

You need to apply desktop restrictions to the sales executives group. You must not apply these desktop restrictions to the sales managers group.

You create a GPO named DesktopLockdown and link it to the Sales organizational unit.

What should you do next?

A. Configure the Deny Apply Group Policy permission for Authenticated Users on the DesktopLockdown GP
B. Configure the Deny Apply Group Policy permission for the sales executives on the DesktopLockdown GP
C. Configure the Allow Apply Group Policy permission for Authenticated Users on the DesktopLockdown GP
D. Configure the Deny Apply Group Policy permission for the sales managers on the DesktopLockdown GP

**Answer:** D

**Explanation:**
http://support.microsoft.com/kb/816100 How to prevent domain Group Policies from applying to certain user or computer accounts Typically, if you want Group Policy to apply only to specific accounts (either user accounts, computer accounts, or both), you can put the accounts in an organizational unit, and then apply Group Policy at that organizational unit level. However, there may be situations where you want to apply Group Policy to a whole domain, although you may not want those policy settings to also apply to administrator accounts or to other specific users or groups. http://www.grouppolicy.biz/2010/05/how-to-exclude-individual-users-or-computers-from-a-group-policy-object/ Best Practice: How to exclude individual users or computers from a Group Policy Object One of the common
question I see on the forums from time to time is how to exclude a user and/or a computer from having a Group Policy Object (GPO) applied. This is a relatively straight forward process however I should stress this should be used sparingly and should always be done via group membership to avoid the administrative overhead of having to constantly update the security filtering on the GPO. Step 1. Open the Group Policy Object that you want to apply an exception and then click on the “Delegation” tab and then click on the “Advanced” button.

Step 2. Click on the “Add” button and select the group (recommended) that you want to exclude from having this policy applied.

Step 3. In this example I am excluding the “Users GPO Exceptions” group for this policy. Select this group in the “Group or user names” list and then scroll down the permission and tick the “Deny” option against the “Apply Group Policy” permission.
Now any members of this “User GPO Exceptions” security group will not have this Group Policy Object applied. Having a security group to control this exception makes it much easier to control as someone only needs to modify the group membership of the group to makes changes to who (or what) get the policy applied. This makes the delegation of this task to level 1 or level 2 support much more practical as you don’t need to grant them permission to the Group Policy Objects.

NEW QUESTION 4
Your network consists of a single Active Directory domain. The domain contains 10 domain controllers. The domain controllers run Windows Server 2008 R2 and are configured as DNS servers. You plan to create a new Active Directory-integrated zone.

You need to ensure that the new zone is only replicated to four of your domain controllers.

What should you do first?

A. From the command prompt, run dnscmd and specify the /createdirectorypartition parameter
B. Create a new delegation in the ForestDnsZones application directory partition
C. From the command prompt, run dnscmd and specify the /enlistdirectorypartition parameter
D. Create a new delegation in the DomainDnsZones application directory partition

Answer: A

Explanation:
Practically the same question as D/Q25 and K/Q17, different set of answers. To control which servers get a copy of the zone we have to store the zone in an application directory partition. That application directory partition must be created before we create the zone, otherwise it won’t work. So that’s what we have to do first. Directory partitions are also called naming contexts and we can create one using ntdsutil. Here I tried to create a zone with dnscmd /zoneadd. It failed because the directory partition I wanted to use did not exist yet. To fix that I used ntdsutil to create the directory partition dc=venomous,dc=contoso,dc=com. Note that after creating it a new naming context had been added. Then, after a minute or two, I tried to create the new zone again, and this time it worked.
**Explanation 1:** http://technet.microsoft.com/en-us/library/cc725739.aspx Store Data in an AD DS Application Partition You can store Domain Name System (DNS) zones in the domain or application directory partitions of Active Directory Domain Services (AD DS). An application directory partition is a data structure in AD DS that distinguishes data for different replication purposes. When you store a DNS zone in an application directory partition, you can control the zone replication scope by controlling the replication scope of the application directory partition. Explanation 2: http://technet.microsoft.com/en-us/library/cc730970.aspx Partition management Manages directory partitions for Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS). This is a subcommand of Ntdsutil and Dsmgmt. Examples To create an application directory partition named AppPartition in the contoso.com domain, complete the following steps:

1. To open an elevated Command Prompt window, click Start, point to All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.
2. Type: ntdsutil
3. Type: Ac in ntds
4. Type: partition management
5. Type: connections
6. Type: Connect to server DC_Name
7. Type: quit
8. Type: list The following partitions will be listed: 0 CN=Configuration,DC=contoso,DC=com 1 DC=contoso,DC=com 2 DC=Schema,CN=Configuration,DC=contoso,DC=com 3 DC=DomainDnsZones,DC=contoso,DC=com 4 DC=ForestDnsZones,DC=contoso,DC=com 5 DC=venomous,DC=contoso,DC=com partition management: create nc dc=venomous,dc=contoso,dc=com server01.contoso.com
9. At the partition management prompt, type: create nc dc=AppPartition,dc=contoso,dc=com ConDc1.contoso.com
10. Run the list command again to refresh the list of partitions.

**NEW QUESTION 5**
Your network contains a domain controller that has two network connections named Internal and Private.
Internal has an IP address of 192.168.0.20. Private has an IP address of 10.10.10.5. You need to prevent the domain controller from registering Host (A) records for the 10.10.10.5 IP address.

What should you do?

A. Modify the netlogon.dns file on the domain controller
B. Modify the Name Server settings of the DNS zone for the domain
C. Modify the properties of the Private network connection on the domain controller
D. Disable netmask ordering on the DNS server that hosts the DNS zone for the domain

Answer: C

Explanation:
http://support.microsoft.com/kb/2023004 Steps to avoid registering unwanted NIC(s) in DNS on a Multi-homed Domain Controller Symptoms On Domain Controllers with more than one NIC where each NIC is connected to separate Network, there is a possibility that the Host A DNS registration can occur for unwanted NIC(s). If the client queries for DC’s DNS records and gets an unwanted record or the record of a different network which is not reachable to client, the client will fail to contact the DC causing authentication and many other issues.

Cause The DNS server will respond to the query in a round robin fashion. If the DC has multiple NICs registered in DNS. The DNS will serve the client with all the records available for that DC. To prevent this, we need to make sure the unwanted NIC address is not registered in DNS. Below are the services that are responsible for Host A record registration on a DC

1. Netlogon service
2. DNS server service (if the DC is running DNS server service)
3. DHCP client /DNS client (2003/2008): If the NIC card is configured to register the connection address in DNS, then the DHCP /DNS client service will Register the record in DNS. Unwanted NIC should be configured not to register the connection address in DNS. If the DC is running DNS server service, then the DNS service will register the interface Host A record that it has set to listen on. The Zone properties, “Name server” tab list out the IP addresses of interfaces present on the DC. If it has listed both the IPs, then DNS server will register Host A record for both the IP addresses. We need to make sure only the required interface listens for DNS and the zone properties, name server tab has required IP address information

Resolution To avoid this problem perform the following 3 steps (It is important that you follow all the steps to avoid the issue).

1. Under Network Connections Properties: On the Unwanted NIC TCP/IP Properties -> Advanced -> DNS -> Uncheck “Register this connections Address in DNS”
2. Open the DNS server console: highlight the server on the left pane Action-> Properties and on the “Interfaces” tab select “listen on only the following IP addresses”. Remove unwanted IP address from the list
3. On the Zone properties, select Name server tab. Along with FQDN of the DC, you will see the IP address associated with the DC. Remove unwanted IP address if it is listed. After performing this delete the existing unwanted Host A record of the DC.

NEW QUESTION 6

You have an enterprise subordinate certification authority (CA) configured for key archival. Three key recovery agent certificates are issued. The CA is configured to use two recovery agents.

You need to ensure that all of the recovery agent certificates can be used to recover all new private keys.

What should you do?

A. Add a data recovery agent to the Default Domain Policy
B. Modify the value in the Number of recovery agents to use box
C. Revoke the current key recovery agent certificates and issue three new key recovery agent certificate
D. Assign the Issue and Manage Certificates permission to users who have the key recovery agent certificate

Answer: B

Explanation:
MS Press - Self-Paced Training Kit (Exams 70-648 & 70-649) (Microsoft Press, 2009) page 357

You enable key archival on the Recovery Agents tab of the CA Properties in the CA console by selecting the Archive The Key option and specifying a key recovery agent. In the number of recovery agents to use, select the number of key recovery agent (KRA) certificates you have added to the CA. This ensures that each KRA can be used to recover a private key. If you specify a smaller number than the number of KRA certificates installed, the CA will randomly select that number of KRA certificates from the available total and encrypt the private key, using those certificates. This complicates recovery because you then have to figure out which recovery agent certificate was used to encrypt the private key before beginning recovery.

NEW QUESTION 7

Your network contains an Active Directory domain. The domain contains four domain controllers.

You modify the Active Directory schema.

You need to verify that all the domain controllers received the schema modification. Which command should you run?

A. dcdiag.exe /a
B. netdom.exe query fsmo
C. repadmin.exe /showrepl *
D. sc.exe query nds

Answer: C

Explanation:

Status Checking Replmon had the option to generate a status report text file. It could tell you which servers were configured to replicate with each other, if they had any errors, and so on. It was pretty useful actually, and one of the main reasons people liked the tool.

Repadmin.exe offers similar functionality within a few of its command line options. For example, we can get a summary report:
Several DCs have been taken offline. Repadmin shows the correct error of 58 – that the other DCs are not available and cannot tell you their status.

You can also use more verbose commands with Repadmin to see details about which DCs are or are not replicating:

Repadmin /showrepl *

NEW QUESTION 8

Your network contains an Active Directory domain controller named DC1. DC1 runs Windows Server 2008 R2. You need to defragment the Active Directory database on DC1. The solution must minimize downtime on DC1.

What should you do first?

A. At the command prompt, run net stop ntds
B. At the command prompt, run net stop netlogon
C. Restart DC1 in Safe Mode
D. Restart DC1 in Directory Services Restore Mode (DSRM).

Answer: A

Explanation:
To perform offline defragmentation of the directory database
1. Open a Command Prompt as an administrator.
2. At the command prompt, type the following command, and then press ENTER: net stop ntds
3. Type Y to agree to stop additional services, and then press ENTER.
4. At the command prompt, type ndsutil, and then press ENTER.
NEW QUESTION 9
You need to receive an e-mail message whenever a domain user account is locked out. Which tool should you use?

A. Active Directory Administrative Center
B. Event Viewer
C. Resource Monitor
D. Security Configuration Wizard

Answer: B

Explanation:
MS Press - Self-Paced Training Kit (Exam 70-642) (2nd Edition, 2011) page 525 Automatically Responding to Events One of the most useful ways to use Task Scheduler is to launch a task in response to a specific event type that appears in Event Viewer. You can respond to events in three ways: Start A Program - Launches an application. Often, administrators write a script that carries out a series of tasks that they would otherwise need to manually perform, and automatically run that script when an event appears.
Send An E-mail - Sends an email by using the Simple Mail Transport Protocol (SMTP) server you specify. Often, administrators configure urgent events to be sent to a mobile device.
Display A Message - Displays a dialog box showing a message. This is typically useful only when a user needs to be notified of something happening on the computer.
To trigger a task when an event occurs, follow one of these three procedures:
Find an example of the event in Event Viewer. Then, right-click the event and click Attach Task To This Event. A wizard will guide you through the process.

NEW QUESTION 10
You deploy an Active Directory Federation Services (AD FS) Federation Service Proxy on a server named Server1. You need to configure the Windows Firewall on Server1 to allow external users to authenticate by using AD FS. Which protocol should you allow on Server1?

A. Kerberos
B. SSL
C. SMB
D. RPC

Answer: B

Explanation:
MS Press - Self-Paced Training Kit (Exam 70-640) (2nd Edition, July 2012) page 903 AD FS relies on secure HTTP communications by using SSL authentication certificates to verify the identity of both the server and the client during communications. Because of this, all communications occur through port 443 over HTTPS.

NEW QUESTION 11
Your network contains an Active Directory domain. The domain is configured as shown in the exhibit. (Click the Exhibit button.)

Users in the Finance organizational unit (OU) frequently log on to client computers in the Human Resources OU. You need to meet the following requirements:

1. All of the user settings in the Group Policy objects (GPOs) linked to both the Finance OU and the Human Resources OU must be applied to finance users when they log on to client computers in the Engineering OU.
2. Only the policy settings in the GPOs linked to the Finance OU must be applied to finance users when they log on to client computers in the Finance OU. Policy settings in the GPOs linked to the Finance OU must not be applied to users in the Human Resources OU.

What should you do?
A. Modify the Group Policy permission
B. Enable block inheritance
C. Configure the link order
D. Enable loopback processing in merge mode
E. Enable loopback processing in replace mode
F. Configure WMI filtering
G. Configure Restricted Group
H. Configure Group Policy Permissions
I. Link the GPO to the Finance OU
J. Link the GPO to the Human Resources OU

Answer: D

Explanation:
Very similar question to K/Q11.
We have to use loopback processing in merge mode if we want all User Configuration settings from the GPOs that are linked to the Sales OU and the Engineering OU to be applied.

Explanation 1:
Loopback processing with merge or replace
Setting loopback causes the User Configuration settings in GPOs that apply to the computer to be applied to every user logging on to that computer, instead of (in replace mode) or in addition to (in merge mode) the User Configuration settings of the user. This allows you to ensure that a consistent set of policies is applied to any user logging on to a particular computer, regardless of their location in Active Directory.
Loopback can be set to Not Configured, Enabled, or Disabled. In the Enabled state, loopback can be set to Merge or Replace. In either case the user only receives user-related policy settings.
Loopback with Replace—In the case of Loopback with Replace, the GPO list for the user is replaced in its entirety by the GPO list that is already obtained for the computer at computer startup (during step 2 in Group Policy processing and precedence). The User Configuration settings from this list are applied to the user.
Loopback with Merge—In the case of Loopback with Merge, the Group Policy object list is a concatenation. The default list of GPOs for the user object is obtained, as normal, but then the list of GPOs for the computer (obtained during computer startup) is appended to this list. Because the computer's GPOs are processed after the user's GPOs, they have precedence if any of the settings conflict.

Explanation 2:
For a clear and easy explanation of Loopback Processing. Recommended!

Explanation 3:
Windows Server 2008 R2 Unleashed (SAMS, 2010) page 1028
Loopback Processing
When a user is processing domain policies, the policies that apply to that user are based on the location of the user object in the Active Directory hierarchy. The same goes for domain policy application for computers. There are situations, however, when administrators or organizations want to ensure that all users get the same policy when logging on to a particular computer or server. For example, on a computer that is used for training or on a Remote Desktop Session Host, also known as a Terminal Server, when the user desktop environment must be the same for each user, this can be controlled by enabling loopback processing in Replace mode on a policy that is applied to the computer objects.

To explain a bit further, if a domain policy has the loopback settings enabled and set to Replace mode, any settings defined within that policy in the User Configuration node are applied to all users who log on to the computer this particular policy is applied to. When loopback processing is enabled and configured in Merge mode on a policy applied to a computer object and a user logs on, all of the user policies are applied and then all of the user settings within the policy applied to the computer object are also applied to the user. This ensures that in either Replace or Merge mode, loopback processing applies the settings contained in the computer-linked policies last.

NEW QUESTION 12
Your network contains a server named Server1. The Active Directory Rights Management Services (AD RMS) server role is installed on Server1. An administrator changes the password of the user account that is used by AD RMS. You need to update AD RMS to use the new password. Which console should you use?

A. Active Directory Rights Management Services
B. Active Directory Users and Computers
C. Local Users and Groups
D. Services

Answer: A

Explanation:
AD RMS How To: Change the RMS Service Account Password
The Active Directory Rights Management Services management console provides a wizard to change or update the AD RMS service account. The most common use for this process is to update the service account password when it has been changed.
It is important to use this process to update or change the AD RMS service account. This ensures the necessary components are updated properly.

Guaranteed success with Our exam guides
visit - https://www.certshared.com
NEW QUESTION 13
Your network contains a domain controller that runs Windows Server 2008 R2. You run the following command on the domain controller:
```shell
dsamain.exe C dbpath c:\$SNAP_201006170326_VOLUMEC$\Windows\NTDS\ntds.dit C ldapport 389 -allowNonAdminAccess
```
The command fails.
You need to ensure that the command completes successfully.
How should you modify the command?
A. Change the value of the -dbpath parameter
B. Include the path to Dsamain
C. Change the value of the -ldapport parameter
D. Remove the CallowNonAdminAccess parameter

Answer: C

Explanation: MS Press - Self-Paced Training Kit (Exam 70-640) (2nd Edition, July 2012) page 690 Use the AD DS database mounting tool to load the snapshot as an LDAP server. dsamain -dbpath c:\$SNAP_datetime_VOLUMEC$\windows\ntds\ntds.dit -ldapport portnumber Be sure to use ALL CAPS for the -dbpath value and use any number beyond 40,000 for the -ldapport value to ensure that you do not conflict with AD DS.
Also note that you can use the minus (--) sign or the slash (/) for the options in the command.

NEW QUESTION 14
DRAG DROP
ABC.com has an Active Directory forest on a single domain. The domain operates Windows Server 2008. A new administrator accidentally deletes the entire organizational unit in the Active Directory database that hosts 6000 objects.
You have backed up the system state data using third-party backup software. To restore backup, you start the domain controller in the Directory Services Restore Mode (DSRM).
You need to perform an authoritative restore of the organizational unit and restore the domain controller to its original state.
Which three actions should you perform?

Answer:
Explanation:

NEW QUESTION 15
Your network contains an Active Directory forest. The forest contains one domain named contoso.com.
You discover the following event in the Event log of domain controllers: "The request for a new accountidentifier pool failed. The operation will be retried until the request succeeds. The error is " %1 ""
You need to ensure that the domain controllers can acquire new account-identifier pools successfully.
What should you do?
A. Move the PDC emulator role
B. Move the schema master role
C. Move the global catalog server
D. Move the domain naming master role
E. Move the infrastructure master role
F. Move the RID master role
G. Restart the Active Directory Domain Services (AD DS) service
H. Deploy an additional global catalog server
I. Move the bridgehead server
J. Install a read-only domain controller (RODC).

Answer: F

Explanation:
Event ID 16651 — RID Pool Request
Users, computers, and groups stored in Active Directory are collectively known as security principals. Each security principal is assigned a unique alphanumeric string called a SID. The SID includes a domain prefix identifier that uniquely identifies the domain and a relative identifier (RID) that uniquely identifies the security principal within the domain. The RID is a monotonically increasing number at the end of the SID. Each domain controller is assigned a pool of RIDs from the global RID pool by the domain controller that holds the RID master role (also known as flexible single master operations or FSMO) in each Active Directory domain. The RID master (also known as the RID pool manager, RID manager, or RID operations master) is responsible for issuing a unique RID pool to each domain controller in its domain. By default, RID pools are obtained in increments of 500. (...) Newly promoted domain controllers must acquire a RID pool before they can advertise their availability to Active Directory clients or share the SYSVOL. Existing domain controllers require additional RID allocations in order to continue creating security principals when their current RID pool becomes depleted.

Event Details Message The request for a new account-identifier pool failed. The operation will be retried until the request succeeds.
The error is " %1 " Resolve Check connectivity to the RID master, and check its replication status A relative ID (RID) pool was not allocated to the local domain controller. Ensure that the local domain controller can communicate with the domain controller that is identified as the RID operations master.
Ensure that the RID master is online and replicating to other domain controllers.

NEW QUESTION 16
Your network contains an Active Directory domain named contoso.com.
You have an organizational unit (OU) named Sales and an OU named Engineering.
You have two Group Policy objects (GPOs) named GPO1 and GPO2. GPO1 and GPO2 are linked to the Sales OU and contain multiple settings.
You discover that GPO2 has a setting that conflicts with a setting in GPO1. When the policies are applied, the setting in GPO2 takes effect.
You need to ensure that the settings in GPO1 supersede the settings in GPO2. The solution must ensure that all non-conflicting settings in both GPOs are applied.

A. Configure Restricted Group
B. Configure the link order
C. Link the GPO to the Sales O
D. Link the GPO to the Engineering O
E. Enable loopback processing in merge mode
F. Modify the Group Policy permission
G. Configure WMI Filtering
H. Configure Group Policy PExplanation
I. Enable loopback processing in replace mode
J. Enable block inheritance

Answer: B

Explanation:
Precedence of Multiple Linked GPOs An OU, domain, or site can have more than one GPO linked to it. In the event of multiple GPOs, the GPOs' link order determines their precedence. In Figure 6-10, two GPOs are linked to the People OU. Figure 6-10 GPO link order
The object higher on the list, with a link order of 1, has the highest precedence. Therefore, settings that are enabled or disabled in the Power User Configuration GPO have precedence over these same settings in the Standard User Configuration GPO.
To change the precedence of a GPO link:
1. Select the OU, site, or domain in the GPMC console tree.
2. Click the Linked Group Policy Objects tab in the details pane.
3. Select the GPO.
4. Use the Up, Down, Move To Top, and Move To Bottom arrow icons to change the link order of the selected GPO.

NEW QUESTION 17
You have an Active Directory domain named contoso.com.
You need to view the account lockout threshold and duration for the domain.
Which tool should you use?

A. Computer Management
B. Net Config
C. Active Directory Users and Computers
D. Gpresult

Answer: C
NEW QUESTION 18
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain and 10 domain controllers. All of the domain controllers run Windows Server 2008 R2 Service Pack 1 (SP1).
The forest contains an application directory partition named dc=app1,dc=contoso,dc=com. A domain controller named DC1 has a copy of the application directory partition.
You need to configure a domain controller named DC2 to receive a copy of dc=app1,dc=contoso,dc=com.
Which tool should you use?
A. Dsamain
B. Ntdsutil
C. Active Directory Sites and Services
D. Dcpromo

Answer: C

Explanation: Active Directory Sites and Services is a Microsoft Management Console (MMC) snap-in that you can use to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest.
You can use the Active Directory Sites and Services snap-in to manage the site-specific objects that implement the intersite replication topology.

NEW QUESTION 19
Your network contains an Active Directory forest. The forest contains two domains. The forest contains four domain controllers. The domain controllers are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Server name</th>
<th>Domain name</th>
<th>FSMO role</th>
<th>Global catalog server</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC1</td>
<td>Contoso.com</td>
<td>Schema master</td>
<td>No</td>
</tr>
<tr>
<td>DC2</td>
<td>Contoso.com</td>
<td>Domain naming master</td>
<td>No</td>
</tr>
<tr>
<td>DC3</td>
<td>Contoso.com</td>
<td>RID master</td>
<td>Infrastructure master</td>
</tr>
<tr>
<td>DC4</td>
<td>Child.contoso.com</td>
<td>PDC emulator</td>
<td>Yes</td>
</tr>
<tr>
<td>DC5</td>
<td>Child.contoso.com</td>
<td>Infrastructure master</td>
<td>No</td>
</tr>
</tbody>
</table>

All user accounts are located in the child.contoso.com domain. Users in the child.contoso.com domain are members of several security groups in the contoso.com domain.
Your company decides to change the naming standard of user accounts.
You rename all of the user accounts to comply with the new standard.
You discover that the old user names are listed in the members' list of the security groups in the contoso.com domain.
You need to ensure that the members' list of the security groups in the contoso.com domain displays the new user names.
What should you do?
A. Transfer the PDC emulator role from DC2 to DC3.
B. Configure DC5 as a global catalog server
C. Configure DC1 as a global catalog server
D. Transfer the infrastructure master role from DC3 to DC2.

Answer: D

NEW QUESTION 20
The research department maintains its own DNS servers and hosts a zone named research.contoso.com on a UNIX-based server named Server1.
The perimeter network contains a DNS server named Server2. Server2 is a standalone server that runs Windows Server 2008 R2.
You need to configure the DNS settings of Server2 to meet the following requirements:
- Server2 must maintain a copy of all the records in research.contoso.com.
- DC1 must query Server2 to resolve the names of Internet hosts.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)
A. Create a secondary zone
B. Create a conditional forwarder
C. Create a stub zone
D. Create a primary zone
E. Create a Forwarder

Answer: AE

Explanation: When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at
this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS
server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another
server, it cannot be stored in AD DS.
E: * A forwarder is a Domain Name System (DNS) server on a network that is used to
forward DNS queries for external DNS names to DNS servers outside that network.
Incorrect:
Not B: You can configure your server to forward queries according to specific domain
names using conditional forwarders.

NEW QUESTION 21

......
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

70-640 Practice Exam Features:

* 70-640 Questions and Answers Updated Frequently
* 70-640 Practice Questions Verified by Expert Senior Certified Staff
* 70-640 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 70-640 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 70-640 Practice Test Here