70-640 Q&As

TS: Windows Server 2008 Active Directory Configuring

Pass Microsoft 70-640 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/70-640.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You need to validate whether Active Directory successfully replicated between two domain controllers.What should you do?

A. Run the DSget command.

B. Run the Dsquery command.

C. Run the RepAdmin command.

D. Run the Windows System Resource Manager.

Correct Answer: C

http://technet.microsoft.com/en-us/library/cc794749.aspx You can use the repadmin /showrepl command to verify successful replication to a specific domain controller.

QUESTION 2

Your network contains an Active Directory domain named contoso.com. Contoso.com contains three servers. The servers are configured as shown in the following table.

Server name	Server role service
Server1	Certification authority (CA)
Server2	Certificate Enrollment Web Service
Server3	Certificate Enrollment Policy Web Service

You need to ensure that users can manually enroll and renew their certificates by using the Certificate Enrollment Web Service. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Configure the policy module settings.

B. Configure the issuance requirements for the certificate templates.

C. Configure the Certificate Services Client - Certificate Enrollment Policy Group Policy setting.

D. Configure the delegation settings for the Certificate Enrollment Web Service application pool account.

Correct Answer: BD

Reference 1:

http://technet.microsoft.com/en-us/library/dd759245.aspx

The Certificate Enrollment Web Service can process enrollment requests for new certificates and for certificate renewal. In both cases, the client computer submits the request to the Web service and the Web service submits the request to

the certification authority (CA) on behalf of the client computer. For this reason, the Web service account must be trusted for delegation in order to present the client identity to the CA.

Reference 2:

http://social.technet.microsoft.com/wiki/contents/articles/7734.certificate-enrollment-web-services-in- active-directory-certificate-services.aspx

Delegation is required for the Certificate Enrollment Web Service account when all of the following are true:

The CA is not on the same computer as the Certificate Enrollment Web Service Certificate Enrollment Web Service needs to be able to process initial enrollment requests, as opposed to only processing certificate renewal requests the

authentication type is set to Windows Integrated Authentication or Client certificate authentication

QUESTION 3

Your network contains an Active Directory forest named contoso.com. You need to identify whether a fine-grained password policy is applied to a specific group. Which tool should you use?

A. Group Policy Management Editor

B. Authorization Manager

C. Local Security Policy

D. ADSI Edit

Correct Answer: A

QUESTION 4

Your company has a single Active Directory domain named intranet.adatum.com. The domain controllers run Windows Server 2008 and the DNS server role. All computers, including non-domain members, dynamically register their DNS records.

You need to configure the intranet.adatum.com zone to allow only domain members to dynamically register DNS records.

What should you do?

A. Set dynamic updates to Secure Only.

B. Remove the Authenticated Users group.

C. Enable zone transfers to Name Servers.

D. Deny the Everyone group the Create All Child Objects permission.

Correct Answer: A

Answer: Set dynamic updates to Secure Only.

http://technet.microsoft.com/en-us/library/cc753751.aspx Allow Only Secure Dynamic Updates

Domain Name System (DNS) client computers can use dynamic update to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records,

especially for clients that frequently move or change locations and use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address. Dynamic updates can be secure or nonsecure. DNS update security is available only for zones that

are integrated into Active Directory Domain Services (AD DS). After you directory-integrate a zone, access control list (ACL) editing features are available in DNS Manager so that you can add or remove users or groups from the ACL for a

specified zone or resource record.

Further information:

http://technet.microsoft.com/en-us/library/cc771255.aspx Understanding Dynamic Update

---

QUESTION 5

Your network contains a single Active Directory domain. The functional level of the forest is Windows Server 2008. The functional level of the domain is Windows Server 2008 R2. All DNS servers run Windows Server 2008. All domain controllers run Windows Server 2008 R2.

You need to ensure that you can enable the Active Directory Recycle Bin.

What should you do?

A. Change the functional level of the forest.

B. Change the functional level of the domain.

C. Modify the Active Directory schema.

D. Modify the Universal Group Membership Caching settings.

Correct Answer: A

Reference: http://technet.microsoft.com/en-us/library/dd392261.aspx Active Directory Recycle Bin Step-by-Step Guide By default, Active Directory Recycle Bin in Windows Server 2008 R2 is disabled. To enable it, you must first raise the forest functional level of your AD DS or AD LDS environment to Windows Server 2008 R2, which in turn requires all forest domain controllers or all servers that host instances of AD LDS configuration sets to be running Windows Server 2008 R2.

QUESTION 6

You are one of two network administrators for your organization.

Your IT partner does most of the work in Active Directory.

While working in Active Directory, your partner accidently deleted a user from the Sales OU. You recover the user from tape backup but you want to help prevent this from happening again in the future.

What can you do?

A. Enable the Active Directory Recycle Bin.

B. Use ADSI Edit to restore the user.

C. Take away all rights from the other administrator.

D. Use the Directory Services Restore Mode Lockout command.

Correct Answer: A

http://technet.microsoft.com/en-us/library/dd392261%28v=ws.10%29.aspx Active Directory Recycle Bin Step-by-Step Guide

Active Directory Recycle Bin helps minimize directory service downtime by enhancing your ability to preserve and restore accidentally deleted Active Directory objects without restoring Active Directory data from backups, restarting Active Directory Domain Services (AD DS), or rebooting domain controllers.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion. For example, restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains.

Active Directory Recycle Bin is functional for both AD DS and Active Directory Lightweight Directory Services (AD LDS) environments.

Important By default, Active Directory Recycle Bin in Windows Server 2008 R2 is disabled. To enable it, you must first raise the forest functional level of your AD DS or AD LDS environment to Windows Server 2008 R2, which in turn requires all forest domain controllers or all servers that host instances of AD LDS configuration sets to be running Windows Server 2008 R2. After you set the forest functional level of your environment to Windows Server 2008 R2, you can use the instructions in this guide to enable Active Directory Recycle Bin. In this release of Windows Server 2008 R2, the process of enabling Active Directory Recycle Bin is irreversible. After you enable Active Directory Recycle Bin in your environment, you cannot disable it.

QUESTION 7

Your company has a main office and a branch office. The main office contains two domain controllers. You create an Active Directory site named BranchOfficeSite. You deploy a domain controller in the branch office, and then add the domain controller to the BranchOfficeSite site.

You discover that users in the branch office are randomly authenticated by either the domain controller in the branch office or the domain controllers in the main office.

You need to ensure that the users in the branch office always attempt to authenticate to the domain controller in the branch office first.

What should you do?

A. Create organizational units (OUs).

B. Create Active Directory subnet objects.

C. Modify the slow link detection threshold.

D. Modify the Location attribute of the computer objects.

Correct Answer: B

http://technet.microsoft.com/en-us/library/cc754697.aspx Understanding Sites, Subnets, and Site Links Sites overview Sites in AD DS represent the physical structure, or topology, of your network. AD DS uses network topology information, which is stored in the directory as site, subnet, and site link objects, to build the most efficient replication topology. The replication topology itself consists of the set of connection objects that enable inbound replication from a source domain controller to the destination domain controller that stores the connection object. The Knowledge Consistency Checker (KCC) creates these connection objects automatically on each domain controller. .. Associating sites and subnets A subnet object in AD DS groups neighboring computers in much the same way that postal codes group neighboring postal addresses. By associating a site with one or more subnets, you assign a set of IP addresses to the site.

Note The term "subnet" in AD DS does not have the strict networking definition of the set of all addresses behind a single router. The only requirement for an AD DS subnet is that the address prefix conforms to the IP version 4 (IPv4) or IP version 6 (IPv6) format. When you add the Active Directory Domain Services server role to create the first domain controller in a forest, a default site (Default-First-Site-Name) is created in AD DS. As long as this site is the only site in the directory, all domain controllers that you add to the forest are assigned to this site. However, if your forest will have multiple sites, you must create subnets that assign IP addresses to Default-First- Site-Name as well as to all additional sites. .. Locating domain controllers by site Domain controllers register service (SRV) resource records in Domain Name System (DNS) that identify their site names. Domain controllers also register host (A) resource records in DNS that identify their IP addresses. When a client requests a domain controller, it provides its site name to DNS. DNS uses the site name to locate a domain controller in that site (or in the next closest site to the client). DNS then provides the IP address of the domain controller to the client for the purpose of connecting to the domain controller. For this reason, it is important to ensure that the IP address that you assign to a domain controller maps to a subnet that is associated with the site of the respective server object. Otherwise, when a client requests a domain controller, the IP address that is returned might be the IP address of a domain controller in a distant site. When a client connects to a distant site, the result can be slow performance and unnecessary traffic on expensive WAN links.

QUESTION 8

Your network contains an Active Directory forest. The forest contains one domain. The domain contains two domain controllers named DC1 and DC2 that run Windows Server 2008 R2.

DC1 was installed before DC2.

DC1 fails.

You need to ensure that you can add 1,000 new user accounts to the domain.

What should you do?

A. Modify the permissions of the DC2 computer account.

B. Seize the schema master FSMO role.

C. Configure DC2 as a global catalog server.

D. Seize the RID master FSMO role.

Correct Answer: D

Reference:

MS Press - Self-Paced Training Kit (Exam 70-640) (2nd Edition, July 2012) pages 536-537 RID master failure

A failed RID master eventually prevents domain controllers from creating new SIDs and, therefore, prevents you from

creating new accounts for users, groups, or computers. However, domain controllers receive a sizable pool of RIDs from

the RID master, so unless you are generating numerous new accounts, you can often go for some time without the RID master online while it is being repaired. Seizing this role to another domain controller is a significant action. After the RID

master role has been seized, the domain controller that had been performing the role cannot be brought back online.

QUESTION 9

You install a read-only domain controller (RODC) named RODC1. You need to ensure that a user named User1 can administer RODC1. The solution must minimize the number of permissions assigned to User1.

Which tool should you use?

A. Active Directory Administrative Center

B. Active Directory Users and Computers

C. Dsadd

D. Dsmgmt

Correct Answer: B

Reference 1:

http://technet.microsoft.com/en-us/library/cc755310.aspx

Delegating local administration of an RODC

Administrator Role Separation (ARS) is an RODC feature that you can use to delegate the ability to administer an RODC to a user or a security group. When you delegate the ability to log on to an RODC to a user or a security group, the user

or group is not added the Domain Admins group and therefore does not have additional rights to perform directory service operations.

Steps and best practices for setting up ARS

You can specify a delegated RODC administrator during an RODC installation or after it.

To specify the delegated RODC administrator after installation, you can use either of the following options:

Modify the Managed By tab of the RODC account properties in the Active Directory Users and Computers snap-in, as shown in the following figure. You can click Change to change which security principal is the delegated RODC

administrator. You can choose only one security principal. Specify a security group rather than an individual user so you can control RODC administration permissions most efficiently. This method changes the managedBy attribute of the

computer object that corresponds to the RODC to the SID of the security principal that you specify. This is the recommended way to specify the delegated RODC administrator account because the information is stored in AD DS, where it can

be centrally managed by domain administrators.

Use the ntdsutil local roles command or the dsmgmt local roles command. You can use this command to view, add, or remove members from the Administrators group and other built-in groups on the RODC. [See also the second reference

for more information on how to use dsmgmt.]

Using ntdsutil or dsmgmt to specify the delegated RODC administrator account is not recommended because the information is stored only locally on the RODC.

Therefore, when you use ntdsutil local roles to delegate an administrator for the RODC, the account that you specify does not appear on the Managed By tab of the RODC account properties. As a result, using the Active Directory Users and

Computers snap-in or a similar tool will not reveal that the RODC has a delegated administrator.

In addition, if you demote an RODC, any security principal that you specified by using ntdsutil local roles remains stored in the registry of the server. This can be a security concern if you demote an RODC in one domain and then promote it to

be an RODC again in a different domain. In that case, the original security principal would have administrative rights on

the new RODC in the different domain.

Reference 2:

http://technet.microsoft.com/en-us/library/cc732301.aspx

Administrator Role Separation Configuration

This section provides procedures for creating a local administrator role for an RODC and for adding a user to that role.

To configure Administrator Role Separation for an RODC

1.

Click Start, click Run, type cmd, and then press ENTER.

2.

At the command prompt, type dsmgmt.exe, and then press ENTER.

3.

At the DSMGMT prompt, type local roles, and then press ENTER.

4.

For a list of valid parameters, type ?, and then press ENTER. By default, no local administrator role is defined on the RODC after AD DS installation. To add the local administrator role, use the Add parameter.

5.

Type add \ For example, type add CONTOSO\testuser administrators

QUESTION 10

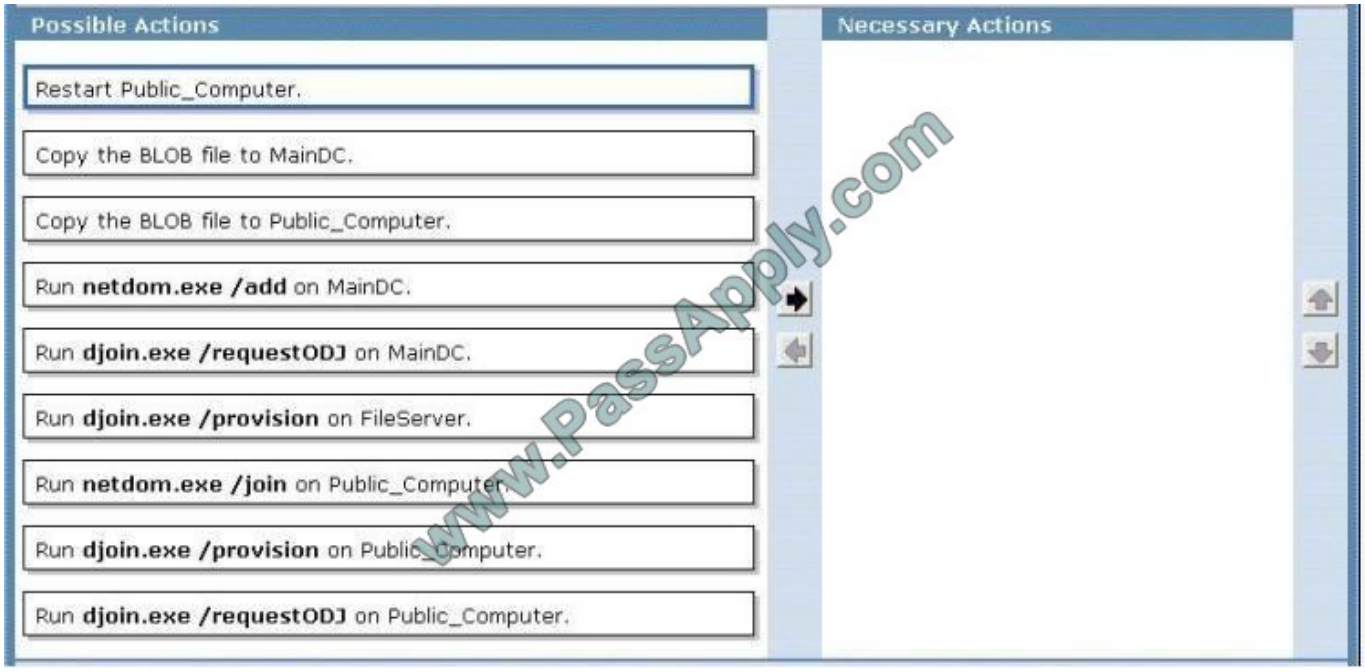
Your company has a main office and a branch office. All servers are located in the main office. The network contains an Active Directory forest named adatum.com. The forest contains a domain controller named MainDC that runs Windows Server 2008 R2 Enterprise and a member server named FileServer that runs Windows Server 2008 R2 Standard.

You have a kiosk computer named Public_Computer that runs Windows 7. Public_Computer is not connected to the network.

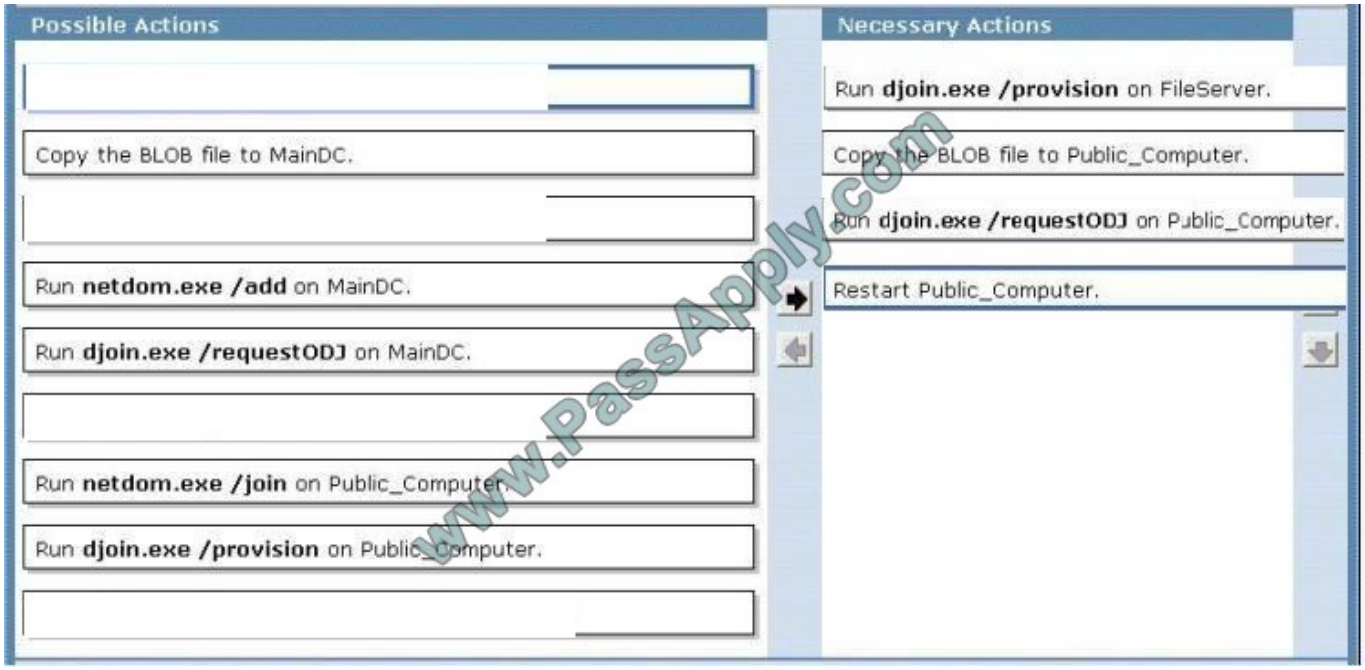
You need to join Public_Computer to the adatum.com domain.

What should you do? To answer, move the appropriate actions from the Possible Actions list to the Necessary Actions area and arrange them in the correct order.

Select and Place:



Correct Answer:



Reference 1:

MS Press - Self-Paced Training Kit (Exam 70-640) (2nd Edition, July 2012) pages 217, 218 Offline Domain Join Offline domain join is also useful when a computer is deployed in a lab or other disconnected environment.

When the computer is connected to the domain network and started for the first time, it will already be a member of the domain. This also helps to ensure that Group Policy settings are applied at the first startup.

Four major steps are required to join a computer to the domain by using offline domain join:

1. Log on to a computer in the domain that is running Windows Server 2008 R2 or Windows 7 with an account that has

permissions to join computers to the domain.

2. Use the DJoin command to provision a computer for offline domain join. This step prepopulates Active Directory with the information that Active Directory needs to join the computer to the domain, and exports the information called a blob to a text file.

3. At the offline computer that you want to join the domain use DJoin to import the blob into the Windows directory.

4. When you start or restart the computer, it will be a member of the domain.

QUESTION 11

Your network contains a single Active Directory domain named contoso.com. An administrator accidentally deletes the _msdsc.contoso.com zone. You recreate the _msdsc.contoso.com zone.

You need to ensure that the _msdsc.contoso.com zone contains all of the required DNS records.

What should you do on each domain controller?

A. Restart the Netlogon service.

B. Restart the DNS Server service.

C. Run dcdiag.exe /fix.

D. Run ipconfig.exe /registerdns.

Correct Answer: A

Reference 1:

http://support.microsoft.com/kb/817470

To register the required records to the single root domain controller, restart the Net Logon service on all the domain controllers. The replication works correctly if the replication window is not less than the default DNS Time to Live (TTL) entry.

To restart the Net Logon service, follow these steps:

1.

Click Start, click Run, type cmd in the Open box, and then press ENTER.

2.

At the command prompt, type the following command, and then press ENTER: net stop netlogon

3.

Type net start netlogon, and then press ENTER.

Reference 2:

http://serverfault.com/questions/383915/how-do-i-manually-create-the-msdcs-dns-zone-for-a-domain- that-wascreated-pre-s

Be sure to restart the Netlogon services on all DC\\'s when the zone has been replicated to them. This forces the DC\\'s to register their SRV records in the _msdcs zone.

QUESTION 12

A corporate network includes an Active Directory-integrated zone. All DNS servers that host the zone are domain controllers. You add multiple DNS records to the zone.

You need to ensure that the new records are available on all DNS servers as soon as possible.

Which tool should you use?

A. Repadmin

B. Active Directory Domains and Trusts console

C. Ldp

D. Ntdsutil

Correct Answer: A

To make sure that the new DNS records are replicated to all DNS servers we can use the repadmin tool.

Reference:

http://technet.microsoft.com/en-us/library/cc811569.aspx

Forcing Replication

Sometimes it becomes necessary to forcefully replicate objects and entire partitions between domain controllers that may or may not have replication agreements.

Force a replication event with all partners

The repadmin /syncall command synchronizes a specified domain controller with all replication partners.

Syntax

repadmin /syncall [] []

Parameters Specifies the host name of the domain controller to synchronize with all replication partners.

Specifies the distinguished name of the directory partition.

Performs specific actions during the replication.