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

A corporate network includes a single Active Directory Domain Services (AD DS) 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 an Active Directory-integrated zone.

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

What should you do first?

A. Use the ntdsutil tool to modify the DS behavior for the domain.

B. Use the ntdsutil tool to add a naming context.

C. Create a new delegation in the ForestDnsZones application directory partition.

D. Use the dnscmd tool with the /zoneadd parameter.

Correct Answer: B

Administrator: Command Prompt

```
C:\Users\Administrator>dnscmd server01.contoso.com /zoneadd test.contoso.com /DsPrimary /DP venomous
.contoso.com

Command failed: DNS_ERROR_DP_DOES_NOT_EXIST     9901    0x26AD


C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: partition management
partition management: connections
server connections: connect to server server01
Binding to server01 ...
Connected to server01 using credentials of locally logged on user.
server connections: quit
partition management: list
Note: Directory partition names with International/Unicode characters will only display correctly if
 appropriate fonts and language support are loaded
Found 5 Naming Context(s)
0 - CN=Configuration,DC=contoso,DC=com
1 - DC=contoso,DC=com
2 - CN=Schema,CN=Configuration,DC=contoso,DC=com
3 - DC=DomainDnsZones,DC=contoso,DC=com
4 - DC=ForestDnsZones,DC=contoso,DC=com
partition management: create nc dc=venomous,dc=contoso,dc=com server01.contoso.com
adding object dc=venomous,dc=contoso,dc=com
partition management: list
Note: Directory partition names with International/Unicode characters will only display correctly if
 appropriate fonts and language support are loaded
Found 6 Naming Context(s)
0 - CN=Configuration,DC=contoso,DC=com
1 - DC=contoso,DC=com
2 - CN=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: quit
ntdsutil: quit

C:\Users\Administrator>dnscmd server01.contoso.com /zoneadd test.contoso.com /DsPrimary /DP venomous
.contoso.com
DNS Server server01.contoso.com created zone test.contoso.com:

Command completed successfully.


C:\Users\Administrator>_
```

Reference 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.

Reference 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, rightclick 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 CN=Schema,CN=Configuration,DC=Contoso,DC=com 3 DC=DomainDnsZones,DC=Contoso,DC=com 4 DC=ForestDnsZones,DC=Contoso,DC=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.

QUESTION 2

A corporate network includes a single Active Directory Domain Services (AD DS) domain. All regular user accounts reside in an organizational unit (OU) named Employees. All administrator accounts reside in an OU named Admins.

You need to ensure that any time an administrator modifies an employee\\'s name in AD DS, the change is audited.

What should you do first?

A. Enable the Audit directory service access setting in the Default Domain Controllers Policy Group PolicyObject.

B. Create a Group Policy Object with the Audit directory service access setting enabled and link it to the Employees OU.

C. Enable the Audit directory service access setting in the Default Domain Policy Group Policy Object.

D. Modify the searchFlags property for the User class in the schema.

Correct Answer: A

To audit changes made to objects in AD DS we have to use Directory Service Changes auditing, which indicates the old and new values of the changed properties of the objects that were changed. DirectoryService Changes auditing is a

subcategory of Audit directory service access, and is not enabled by default.

To use it we have to enable it first, and we can do that specifically for Directory Service Changes by using auditpol.exe, or we can use Group Policy Management to enable Audit directory service access, which enables all subcategories,

including Directory Service Changes. You do this by modifying the Default Domain Controllers Policy.

Reference:

http://technet.microsoft.com/en-us/library/cc731607.aspx

In Windows 2000 Server and Windows Server 2003, there was one audit policy, Audit directory service access, that controlled whether auditing for directory service events was enabled or disabled. In Windows Server 2008, this policy is

divided into four subcategories:

Directory Service Access

Directory Service Changes

Directory Service Replication

Detailed Directory Service Replication

This step includes procedures to enable change auditing with either the Windows interface or a command line:

By using Group Policy Management, you can turn on the global audit policy, Audit directory service access, which enables all the subcategories for AD DS auditing.

To enable the global audit policy using the Windows interface

1.

 Click Start, point to Administrative Tools, and then Group Policy Management.

2.

 In the console tree, double-click the name of the forest, double-click Domains, double-click the name of your domain, double-click Domain Controllers, right-click Default Domain Controllers Policy, and then click Edit.

3.

 Under Computer Configuration, double-click Policies, double-click Windows Settings, double-click Security Settings, double-click Local Policies, and then click Audit Policy.

4.

 In the details pane, right-click Audit directory service access, and then click Properties.

5.

 Select the Define these policy settings check box.

6.

 Under Audit these attempts, select the Success, check box, and then click OK.

QUESTION 3

Your network consists of an Active Directory forest that contains one domain named contoso.com. All domain controllers run Windows Server 2008 R2 and are configured as DNS servers. You have two Active Directory-integrated zones: contoso.com and nwtraders.com.

You need to ensure a user is able to modify records in the contoso.com zone. You must prevent the user from modifying the SOA record in the nwtraders.com zone.

What should you do?

A. From the Active Directory Users and Computers console, run the Delegation of Control Wizard.

B. From the Active Directory Users and Computers console, modify the permissions of the Domain Controllers organizational unit (OU).

C. From the DNS Manager console, modify the permissions of the contoso.com zone.

D. From the DNS Manager console, modify the permissions of the nwtraders.com zone.

Correct Answer: C

Answer: From the DNS Manager console, modify the permissions of the contoso.com zone.
http://technet.microsoft.com/en-us/library/cc753213.aspx Modify Security for a Directory-Integrated Zone

You can manage the discretionary access control list (DACL) on the DNS zones that are stored in Active Directory Domain Services (AD DS). You can use the DACL to control the permissions for the Active Directory users and groups

that may control the DNS zones.

Membership in DnsAdmins or Domain Admins in AD DS, or the equivalent, is the minimum required to complete this procedure.

To modify security for a directory-integrated zone:

1.

 Open DNS Manager.

2.

 In the console tree, click the applicable zone.

Where?

DNS/applicable DNS server/Forward Lookup Zones (or Reverse Lookup Zones)/applicable zone

3.

 On the Action menu, click Properties.

4.

 On the General tab, verify that the zone type is Active Directory-integrated.

5.

 On the Security tab, modify the list of member users or groups that are allowed to securely update the applicable zone and reset their permissions as needed.

Further information:

http://support.microsoft.com/kb/163971

The Structure of a DNS SOA Record

The first resource record in any Domain Name System (DNS) Zone file should be a Start of Authority (SOA) resource record. The SOA resource record indicates that this DNS name server is the best source of information for the data within

this DNS domain.

The SOA resource record contains the following information:

Source host - The host where the file was created.

Contact e-mail - The e-mail address of the person responsible for administering the domain\\'s zone file. Note that a "." is used instead of an "@" in the e-mail name.

Serial number - The revision number of this zone file. Increment this number each time the zone file is changed. It is important to increment this value each time a change is made, so that the changes will be distributed to any secondary DNS

servers.

Refresh Time - The time, in seconds, a secondary DNS server waits before querying the primary DNS server\\'s SOA record to check for changes. When the refresh time expires, the secondary DNS server requests a copy of the current SOA

record from the primary. The primary DNS server complies with this request.

The secondary DNS server compares the serial number of the primary DNS server\\'s current SOA record and the serial number in it\\'s own SOA record. If they are different, the secondary DNS server will request a zone transfer from the

primary DNS server. The default value is 3,600.

Retry time - The time, in seconds, a secondary server waits before retrying a failed zone transfer. Normally, the retry time is less than the refresh time. The default value is 600. Expire time - The time, in seconds, that a secondary server will

keep trying to complete a zone transfer. If this time expires prior to a successful zone transfer, the secondary server will expire its zone file. This means the secondary will stop answering queries, as it considers its data too old to be reliable.

The default value is 86,400.

Minimum TTL - The minimum time-to-live value applies to all resource records in the zone file. This value is supplied in query responses to inform other servers how long they should keep the data in cache. The default value is 3,600.

http://technet.microsoft.com/en-us/library/cc787600%28v=ws.10%29.aspx Modify the start of authority (SOA) record for a zone

..

Notes: To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins

group might be able to perform this procedure. As a security best practice, consider using Run as to perform this procedure.

QUESTION 4

Your network contains a single Active Directory domain. The domain contains five read-only domain controllers (RODCs) and five writable domain controllers. All servers run Windows Server 2008. You plan to install a new RODC that runs Windows Server 2008 R2. You need to ensure that you can add the new RODC to the domain. You want to achieve this goal by using the minimum amount of administrative effort.

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

A. From Active Directory Domains and Trusts, raise the functional level of the domain.

B. At the command prompt, run adprep.exe /forestprep.

C. From Active Directory Users and Computers, pre-stage the RODC computer account.

D. At the command prompt, run adprep.exe /domainprep.

E. At the command prompt, run adprep.exe /rodcprep.

Correct Answer: CD

C:

*

During the first stage of the installation, the wizard records all the data about the RODC that will be stored in the distributed Active Directory database, including the read-only domain controller account name and the site in which it will be placed. This stage must be performed by a member of the Domain Admins group.

*

To create an RODC account by using the Windows interface Click Start, click Administrative Tools, and then click Active Directory Users and Computers. Double-click the domain container, then you can either right-click the Domain Controllers container or click the Domain Controllers container, and then click Action.

Click Pre-create Read-only Domain Controller account

QUESTION 5

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

You need to modify the Password Replication Policy on a read-only domain controller (RODC).

Which tool should you use?

A. Group Policy Management

B. Active Directory Domains and Trusts

C. Active Directory Users and Computers

D. Computer Management

E. Security Configuration Wizard

Correct Answer: C

Reference: http://technet.microsoft.com/en-us/library/rodc-guidance-for-administering-the-password-replication-policy.aspx

Administering the Password Replication Policy This topic describes the steps for viewing, configuring, and monitoring the Password Replication Policy (PRP) and password caching for read-only domain controllers (RODCs). To configure the PRP using Active Directory Users and Computers

1.

Open Active Directory Users and Computers as a member of the Domain Admins group.

2.

Ensure that you are connected to a writeable domain controller running Windows Server 2008 in the correct domain.

3.

Click Domain Controllers, and in the details pane, right-click the RODC computer account, and then click Properties.

4.

Click the Password Replication Policy tab.

5.

The Password Replication Policy tab lists the accounts that, by default, are defined in the Allowed list and the Deny list on the RODC. To add other groups that should be included in either the Allowed list or the Deny list, click Add.

To add other accounts that will have credentials cached on the RODC, click Allow passwords for the account to replicate to this RODC.

To add other accounts that are not allowed to have credentials cached on the RODC, click Deny passwords for the account from replicating to this RODC.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
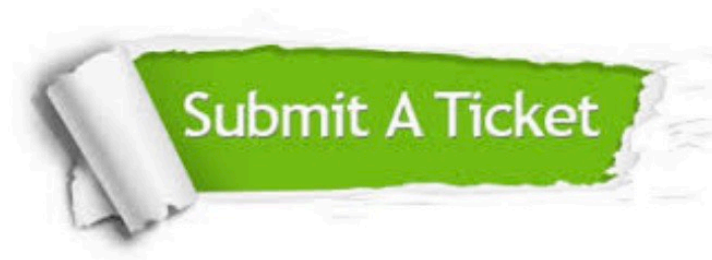Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.passapply.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: