



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.pass4itsure.com/70-640.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

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.

Correct Answer: A

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.



```
Administrator: Command Prompt
C:\Users\Administrator>dnscommand 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>dnscommand 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



Your network contains an Active Directory forest named fabrikam.com. You perform a test installation of an enterprise certification authority (CA). After the installation, you discover that the Issuer Statement option on every certificate issued

by the CA is unavailable.

You need to ensure that the Issuer Statement option is available when you install the enterprise CA to the production environment.

What should you do?

- A. Before you install the enterprise CA, install the Certification Authority Web Enrollment role service.
- B. After you install the enterprise CA, modify the Authority Information Access (AIA) extension settings.
- C. During the installation of the enterprise CA, click the Allow administrator interaction when the private key is accessed by the CA cryptographic option.
- D. Before you install the enterprise CA, create a custom CAPolicy.inf file and place the file in the Windows directory.

Correct Answer: D

QUESTION 3

Your network contains an Active Directory domain named contoso.com. The network has a branch office site that contains a read-only domain controller (RODC) named RODC1. RODC1 runs Windows Server 2008 R2.

A user logs on to a computer in the branch office site.

You discover that the user's password is not stored on RODC1. You need to ensure that the user's password is stored on RODC1 when he logs on to a branch office site computer.

What should you do?

- A. Modify the RODC's password replication policy by removing the entry for the Allowed RODC Password Replication Group.
- B. Modify the RODC's password replication policy by adding RODC1's computer account to the list of allowed users, groups, and computers.
- C. Add the user's user account to the built-in Allowed RODC Password Replication Group on RODC1.
- D. Add RODC1's computer account to the built-in Allowed RODC Password Replication Group on RODC1.

Correct Answer: C

Reference: MS Press - Self-Paced Training Kit (Exam 70-640) (2nd Edition, July 2012) pages 416-417 Password Replication Policy Password Replication Policy (PRP) determines which users' credentials can be cached on a specific RODC. If PRP allows an RODC to cache a user's credentials, authentication and service ticket activities of that user can be processed by the RODC. If a user's credentials cannot be cached on an RODC, authentication and service ticket activities are referred by the RODC to a writable domain controller. An RODC's PRP is determined by two multivalued attributes of the RODC's computer account. These attributes are commonly known as the Allowed List and the Denied List. If a user's account is on the Allowed List, the user's credentials are cached. You can include groups



on the Allowed List, in which case all users who belong to the group can have their credentials cached on the RODC. If the user is on both the Allowed List and the Denied List, the user's credentials will not be cached--the Denied List takes precedence.

Configuring Domain-Wide Password Replication Policy To facilitate the management of PRP, Windows Server 2008 R2 creates two domain local security groups in the Users container of Active Directory. The first group, Allowed RODC Password Replication Group, is added to the Allowed List of each new RODC. By default, the group has no members. Therefore, by default, a new RODC will not cache any user's credentials. If you have users whose credentials you want to be cached by all domain RODCs, add those users to the Allowed RODC Password Replication Group.

QUESTION 4

Your network contains an Active Directory forest named contoso.com. The functional level of the forest is Windows Server 2008 R2. The DNS zone for contoso.com is Active Directory-integrated.

You deploy a read-only domain controller (RODC) named RODC1.

You install the DNS Server server role on RODC1.

You discover that RODC1 does not have any application directory partitions. You need to ensure that RODC1 has a directory partition of contoso.com.

What should you do?

- A. From DNS Manager, create secondary zones.
- B. Run Dnscmd.exe, and specify the /enlistdirectorypartition parameter.
- C. From DNS Manager, right-click RODC1 and click Update Server Data Files.
- D. Run Dnscmd.exe and specify the /createbuiltindirectorypartitions parameter.

Correct Answer: B

Reference: <http://technet.microsoft.com/en-us/library/cc742490.aspx>

RODC Post-Installation Configuration If you install DNS server after the AD DS installation, you must also enlist the RODC in the DNS application directory partitions. The RODC is not enlisted automatically in the DNS application directory partitions by design because it is a privileged operation. If the RODC were allowed to enlist itself, it would have permissions to add or remove other DNS servers that are enlisted in the application directory partitions.

To enlist a DNS server in a DNS application directory partition

1.

Open an elevated command prompt.

2.

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

```
dnscmd /EnlistDirectoryPartition
```

For example, to enlist RODC01 in the domain-wide DNS application directory partition in a domain named child.contoso.com, type the following command:



dnscmd RODC01 /EnlistDirectoryPartition DomainDNSZones.child.contoso.com

QUESTION 5

You are the administrator of an organization with a single Active Directory domain. One of your senior executives tries to log onto a machine and receives the error "This user account has expired. Ask your administrator to reactivate your account".

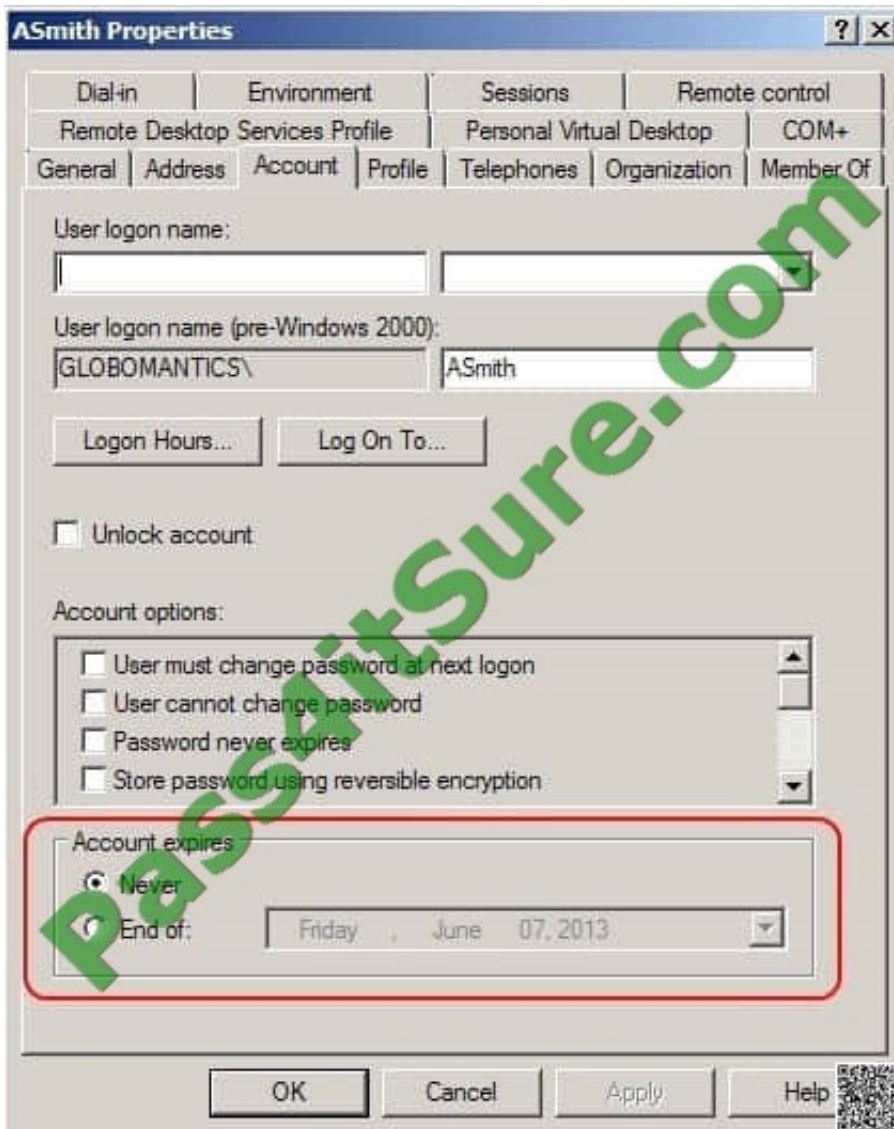
You need to make sure this doesn't happen again to this user.

What do you do?

- A. Configure the domain policy to disable account lockouts.
- B. Configure the password policy to extend the maximum password age to 0.
- C. Modify the user's properties to set the Account Never Expires setting.
- D. Modify the user's properties to extend the maximum password age to 0.

Correct Answer: C

Basically the same as A/Q36:



Further information:

<http://technet.microsoft.com/en-us/library/dd145547.aspx>

User Properties - Account Tab

Account expires

Sets the account expiration policy for this user. You can select between the following options:

Use Never to specify that the selected account will never expire. This option is the default for new users.

Select End of and then select a date if you want to have the user's account expire on a specified date.

[70-640 VCE Dumps](#)

[70-640 Study Guide](#)

[70-640 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

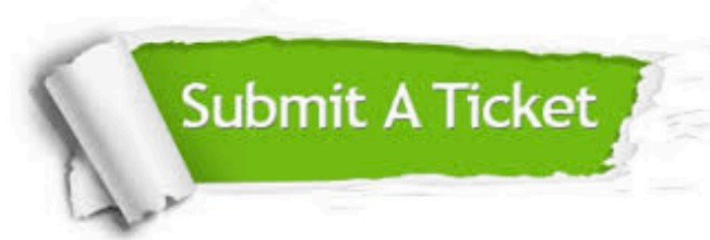
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [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.pass4itsure.com/allproducts>

Need Help

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



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © pass4itsure, All Rights Reserved.