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.pass4lead.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

Your company has an Active Directory forest.

You plan to install an Enterprise certification authority (CA) on a dedicated stand-alone server. When you attempt to add the Active Directory Certificate Services (AD CS) role, you find that the Enterprise CA option is not available.

You need to install the AD CS role as an Enterprise CA.

What should you do first?

A. Add the DNS Server role.

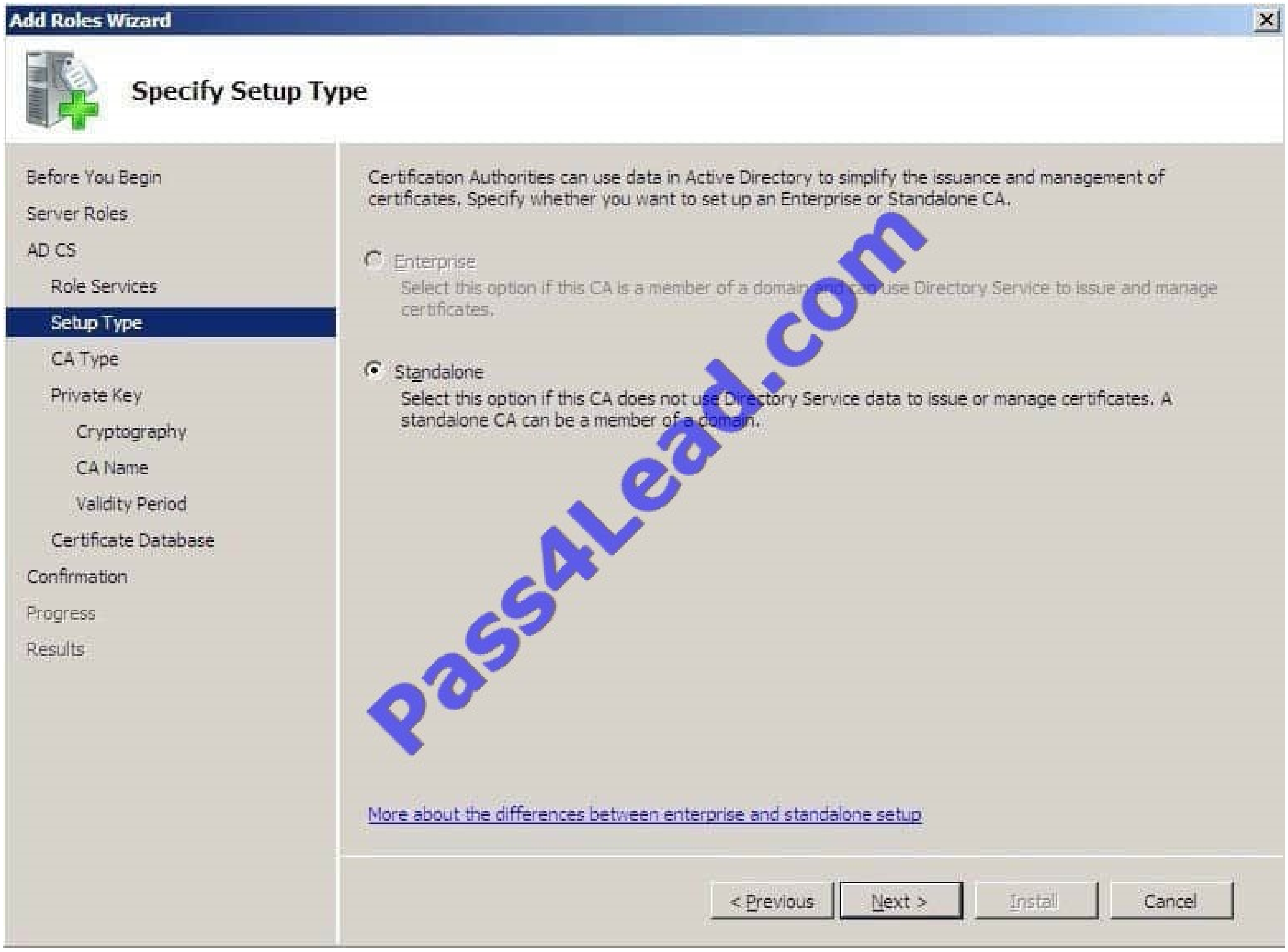
B. Add the Active Directory Lightweight Directory Service (AD LDS) role.

C. Add the Web server (IIS) role and the AD CS role.

D. Join the server to the domain.

Correct Answer: D

http://technet.microsoft.com/en-us/library/cc772393%28v=ws.10%29.aspx Active Directory Certificate Services Step-by-Step Guide http://kazmierczak.eu/itblog/2012/09/23/enterprise-ca-option-is-greyed-out-unavailable/ Enterprise CA option is greyed out / unavailable Many times, administrators ask me what to do when installing Active Directory Certificate Services they cannot choose to install Enterprise Certification Authority, ecause it\\'s unavailable as in following picture:



Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

○ Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

● Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

More about the differences between enterprise and standalone setup

Well, you need to fulfill basic requirements:

Server machine has to be a member server (domain joined). You can run an Enterprise CA on the Standard, Enterprise, or Data Center Windows Edition. The difference is the number of ADCS features and components that can be enabled.

To get full functionality, you need to run on Enterprise or Data Center Windows Server 2008 /R2/ Editions. It includes functionality like Role separation, Certificate manager restrictions, Delegated enrollment agent restrictions, Certificate

enrollment across forests, Online Responder, Network Device Enrollment. In order to install an Enterprise CA, you must be a member of either Enterprise Admins or Domain Admins in the forest root domain (either directly or through a group

nesting). If issue still persists, there is probably a problem with getting correct credentials of your account. There are many thing that can cause it (network blockage, domain settings, server configuration, and other issues). In all cases I got,

this troubleshooting helped perfectly:

First of all, carefully check all above requirements.

Secondly, install all available patches and Service Packs with Windows Update before trying to install Enterprise CA.

Check network settings on the CA Server. If there is no DNS setting, Certificate Authority Server cannot resolve and find domain.

Sufficient privileges for writing the Enterprise CA configuration information in AD configuration partition are required. Determine if you are a member of the Enterprise Admins or Domain Admins in the forest root domain. Think about the

account you are currently trying to install ADCS with. In fact, you may be sure, that your account is in Enterprise Admins group, but check this how CA Server "sees" your account membership by typing whoami /groups.

You also need to be a member of local Administrators group. If you are not, you wouldn\\'t be able to run Server Manager, but still needs to be checked.

View C:\windows\certocm.log file. There you can find helpful details on problems with group membership. For example status of ENUM_ENTERPRISE_UNAVAIL_REASON_NO_INSTALL_RIGHTS indicates that needed memberships are not

correct.

Don\\'t forget to check event viewer on CA Server side and look for red lines. Verify that network devices or softwareandhardware firewalls are not blocking access from/to server and Domain Controllers. If so, Certificate Authority Server may not be communicating correctly with the domain. To check that, simply run nltest /sc_verify:DomainName Check also whether Server CA is connected to a writable Domain Controller. Enterprise Admins groups is the most powerful group and has ADCS required full control permissions, but who knows maybe someone changed default permissions? Run adsiedit.msc on Domain Controller, connect to default context and first of all check if CN=Public Key Service,CN=Services,CN=Configuration,DC=Your,DC=Domain,DC=Com container does exist. If so, check permissions for all subcontainers under Public Key Service if Enterprise Admins group has full control permissions. The main subcontainers to verify are Certificate Templates, OID, KRA containers. If no above tips help, disjoin the server from domain and join again. Ultimately reinstall operation system on CA Server.

QUESTION 2

Your company has two Active Directory forests named Forest1 and Forest2, The forest functional level and the domain functional level of Forest1 are set to Windows Server 2008.

The forest functional level of Forest2 is set to Windows 2000, and the domain functional levels in Forest2 are set to Windows Server 2003.

You need to set up a transitive forest trust between Forest1 and Forest2.

What should you do first?

A. Raise the forest functional level of Forest2 to Windows Server 2003 Interim mode.

B. Raise the forest functional level of Forest2 to Windows Server 2003.

C. Upgrade the domain controllers in Forest2 to Windows Server 2008.

D. Upgrade the domain controllers in Forest2 to Windows Server 2003.

Correct Answer: B

Reference:

http://technet.microsoft.com/en-us/library/cc816810.aspx

Creating Forest Trusts

You can link two disjoined Active Directory Domain Services (AD DS) forests together to form a one- way or two-way, transitive trust relationship.

The following are required to create forest trusts successfully:

You can create a forest trust between two Windows Server 2003 forests, between two Windows Server 2008 forests, between two Windows Server 2008 R2 forests, between a Windows Server 2003 forest and a Windows Server 2008 forest,

between a Windows Server 2003 forest and a Windows Server 2008 R2 forest, or between a Windows Server 2008 forest and a Windows Server 2008 R2 forest. Forest trusts cannot be extended implicitly to a third forest. To create a forest

trust, the minimum forest functional level for the forests that are involved in the trust relationship is Windows Server 2003.

QUESTION 3

Your company has an Active Directory forest that contains eight linked Group Policy Objects (GPOs). One of these GPOs publishes applications to user objects. A user reports that the application is not available for installation.

You need to identify whether the GPO has been applied.

What should you do?

A. Run the Group Policy Results utility for the user.

B. Run the GPRESULT /S /Z command at the command prompt.

C. Run the GPRESULT /SCOPE COMPUTER command at the command prompt.

D. Run the Group Policy Results utility for the computer.

Correct Answer: A

Personal note:

You run the utility for the user and not for the computer because the application publishes to user objects

http://technet.microsoft.com/en-us/library/bb456989.aspx How to Use the Group Policy Results (GPResult.exe) Command Line Tool Intended for administrators, the Group Policy Results (GPResult.exe) command line tool verifies all policy

settings in effect for a specific user or computer. Administrators can run GPResult on any remote computer within their scope of management. By default, GPResult returns settings in effect on the computer on which GPResult is run.

To run GPResult on your own computer:

1.

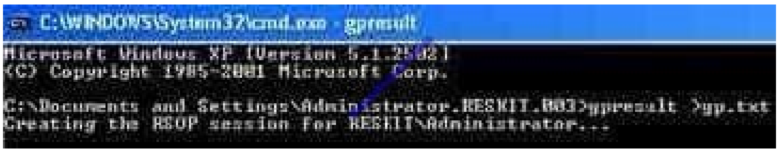
Click Start, Run, and enter cmd to open a command window.

2.

Type gpresult and redirect the output to a text file as shown in Figure 1 below:

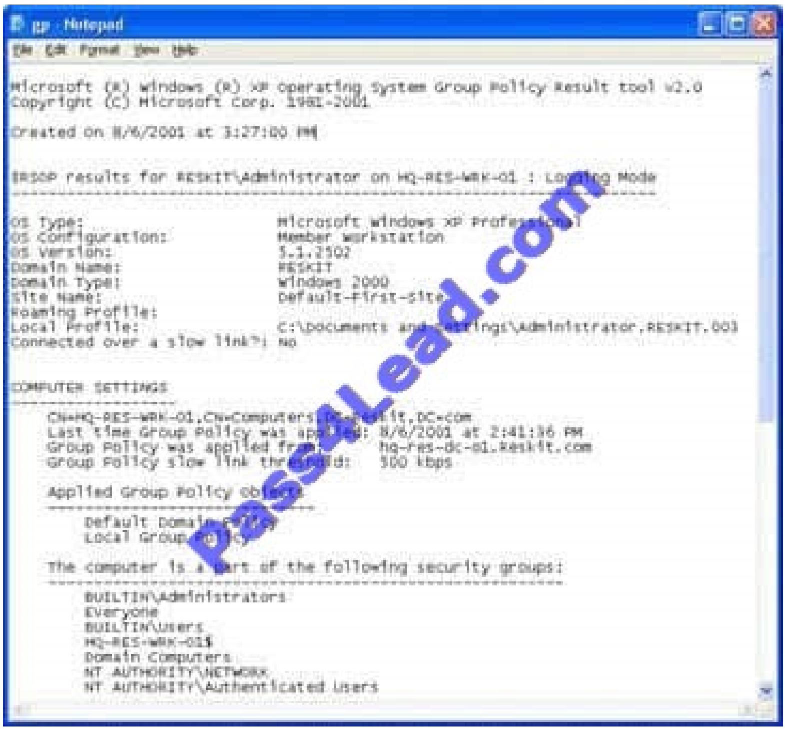
3.

Enter notepad gp.txt to open the file. Results appear as shown in the figure below.



```
Microsoft Windows XP [Version 5.1.2502]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator.RESKIT.003>gpresult >gp.txt
Creating the RSOP session for RESKIT\Administrator...
```



```
Microsoft (R) Windows (R) XP Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 8/6/2001 at 3:27:00 PM


RSOP results for RESKIT\Administrator on HQ-RES-WRK-01 : Logging Mode
----------------------------------------------------------------------

OS Type:                     Microsoft Windows XP Professional
OS Configuration:            Member Workstation
OS Version:                  5.1.2502
Domain Name:                 RESKIT
Domain Type:                 Windows 2000
Site Name:                   Default-First-Site
Roaming Profile:
Local Profile:               C:\Documents and Settings\Administrator.RESKIT.003
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=HQ-RES-WRK-01,CN=Computers,DC=Reskit,DC=com
    Last time Group Policy was applied: 8/6/2001 at 2:41:36 PM
    Group Policy was applied from:      hq-res-dc-01.Reskit.com
    Group Policy slow link threshold:   500 kbps

    Applied Group Policy objects
    -----------------------------
        Default Domain Policy
        Local Group Policy

    The computer is a part of the following security groups:
    --------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Users
        HQ-RES-WRK-01$
        Domain Computers
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
```

QUESTION 4

Your company has a main office and 50 branch offices. Each office contains multiple subnets. You need to automate the creation of Active Directory subnet objects.

What should you use?

A. the Dsadd tool

B. the Netsh tool

C. the New-ADObject cmdlet

D. the New-Object cmdlet

Correct Answer: C

http://technet.microsoft.com/en-us/library/ee617260.aspx New-ADObject Creates an Active Directory object.

Syntax:

New-ADObject [-Name] [-Type] [-AuthType { | }] [-Credential] [-Description] [-DisplayName] [-Instance] [-

OtherAttributes] [-PassThru]

[-Path] [- ProtectedFromAccidentalDeletion] [-Server] [-Confirm] [-WhatIf] []

Detailed Description

The New-ADObject cmdlet creates a new Active Directory object such as a new organizational unit or new user account. You can use this cmdlet to create any type of Active Directory object. Many object properties are defined by setting

cmdlet parameters. Properties that are not set by cmdlet parameters can be set by using the OtherAttributes parameter.

You must set the Name and Type parameters to create a new Active Directory object. The Name specifies the name of the new object. The Type parameter specifies the LDAP display name of the Active Directory Schema Class that

represents the type of object you want to create. Examples of Type values include computer, group, organizational unit, and user.

The Path parameter specifies the container where the object will be created.. When you do not specify the Path parameter, the cmdlet creates an object in the default naming context container for Active Directory objects in the domain.

QUESTION 5

Your company has an Active Directory domain. You have a two-tier PKI infrastructure that contains an offline root CA and an online issuing CA. The Enterprise certification authority is running Windows Server 2008 R2.

You need to ensure users are able to enroll new certificates.

What should you do?

A. Renew the Certificate Revocation List (CRL) on the root CA. Copy the CRL to the CertEnroll folder on the issuing CA.

B. Renew the Certificate Revocation List (CRL) on the issuing CA, Copy the CRL to the SysternCertificates folder in the users\\' profile.

C. Import the root CA certificate into the Trusted Root Certification Authorities store on all client workstations.

D. Import the issuing CA certificate into the Intermediate Certification Authorities store on all client workstations.

Correct Answer: A

http://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority- ca.aspx

Offline Root Certification Authority (CA)

A root certification authority (CA) is the top of a public key infrastructure (PKI) and generates a self- signed certificate. This means that the root CA is validating itself (self-validating). This root CA could then have subordinate CAs that

effectively trust it. The subordinate CAs receive a certificate signed by the root CA, so the subordinate CAs can issue certificates that are validated by the root CA. This establishes a CA hierarchy and trust path.

CA Compromise

If a root CA is in some way compromised (broken into, hacked, stolen, or accessed by an unauthorized or malicious person), then all of the certificates that were issued by that CA are also compromised. Since certificates are used for data

protection, identification, and authorization, the compromise of a CA could compromise the security of an entire organizational network. For that reason, many organizations that run internal PKIs install their root CA offline. That is, the CA is

never connected to the company network, which makes the root CA an offline root CA. Make sure that you keep all CAs in secure areas with limited access.

To ensure the reliability of your CA infrastructure, specify that any root and non-issuing intermediate CAs must be offline. A non-issuing CA is one that is not expected to provide certificates to client computers, network devices, and so on. This

minimizes the risk of the CA private keys becoming compromised, which would in turn compromise all the certificates that were issued by the CA.

How Do Offline CAs issue certificates?

Offline root CAs can issue certificates to removable media devices (e.g. floppy disk, USB drive, CD/DVD) and then physically transported to the subordinate CAs that need the certificate in order to perform their tasks. If the subordinate CA is

a non-issuing intermediate that is offline, then it will also be used to generate a certificate and that certificate will be placed on removable media. Each CA receives its authorization to issue certificates from the CA directly above it in the CA

hierarchy. However, you can have multiple CAs at the same level of the CA hierarchy. Issuing CAs are typically online and used to issue certificates to client computers, network devices, mobile devices, and so on. Do not join offline CAs to an

Active Directory Domain Services domain Since offline CAs should not be connected to a network, it does not make sense to join them to an Active Directory Domain Services (AD DS) domain, even with the Offline Domain Join [This link is

external to TechNet Wiki. It will open in a new window.] option introduced with Windows 7 and Windows Server 2008 R2.

Furthermore, installing an offline CA on a server that is a member of a domain can cause problems with a secure channel when you bring the CA back online after a long offline period. This is because the computer account password changes

every 30 days. You can get around this by problem and better protect your CA by making it a member of a workgroup, instead of a domain. Since Enterprise CAs need to be joined to an AD DS domain, do not attempt to install an offline CA

as a Windows Server Enterprise CA.

http://technet.microsoft.com/en-us/library/cc740209%28v=ws.10%29.aspx Renewing a certification authority

A certification authority may need to be renewed for either of the following reasons:

Change in the policy of certificates issued by the CA

Expiration of the CA\\'s issuing certificate

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

Try our product !

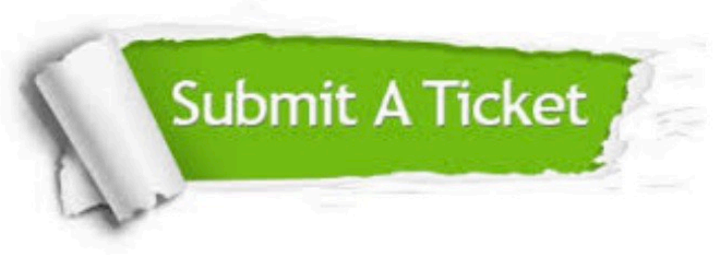
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.pass4lead.com/allproducts

Need Help

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



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.

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.

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.