Microsoft

Exam Questions 70-640
Windows Server 2008 Active Directory - Configuring
NEW QUESTION 1
The default domain GPO in your company is configured by using the following account policy settings:
- Minimum password length: 8 characters
- Maximum password age: 30 days
- Enforce password history: 12 passwords remembered
- Account lockout threshold: 3 invalid logon attempts
- Account lockout duration: 30 minutes

You install Microsoft SQL Server on a computer named Server1 that runs Windows Server 2008 R2. The SQL Server application uses a service account named SQLSrv. The SQLSrv account has domain user rights.

The SQL Server computer fails after running successfully for several weeks. The SQLSrv user account is not locked out.

You need to resolve the server failure and prevent recurrence of the failure. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Reset the password of the SQLSrv user account
B. Configure the local security policy on Server1 to grant the Logon as a service right on the SQLSrv user account
C. Configure the properties of the SQLSrv account to Password never expire
D. Configure the properties of the SQLSrv account to User cannot change password
E. Configure the local security policy on Server1 to explicitly grant the SQLSrv user account the Allow logon locally user right

Answer: AC

Explanation:
Personal comment:
- Maximum password age: 30 days
- The most probable cause for the malfunction is that the password has expired.
- You need to reset the password and set it to never expire.

NEW QUESTION 2
ABC.com has a domain controller that runs Windows Server 2008. The ABC.com network boasts 40 Windows Vista client machines.

As an administrator at ABC.com, you want to deploy Active Directory Certificate service (AD CS) to authorize the network users by issuing digital certificates.

What should you do to manage certificate settings on all machines in a domain from one main location?

A. Configure Enterprise CA certificate settings
B. Configure Enterprise trust certificate settings
C. Configure Advance CA certificate settings
D. Configure Group Policy certificate settings
E. All of the above

Answer: D

Explanation:

AD CS: Policy Settings
In the Windows Server, 2008 operating system, certificate-related Group Policy settings enable administrators to manage certificate validation settings according to...
the security needs of the organization.

What are certificate settings in Group Policy?

Certificate settings in Group Policy enable administrators to manage the certificate settings on all the computers in the domain from a central location.

NEW QUESTION 3
There are 100 servers and 2000 computers present at your company's headquarters. The DHCP service is installed on a two-node Microsoft failover cluster named CKMFO to ensure the high availability of the service. The nodes are named as CKMFON1 and CKMFON2. The cluster on CKMFO has one physical shared disk of 400 GB capacity. A 200GB single volume is configured on the shared disk. Company has decided to host a Windows Internet Naming Service (WINS) on CKMFON1. The DHCP and WINS services will be hosted on other nodes. Using High Availability Wizard, you begin creating the WINS service group on cluster available on CKMFON1 node. The wizard shows an error "no disks are available" during configuration. Which action should you perform to configure storage volumes on CKMFON1 to successfully add the WINS Service group to CKMFON1?

A. Backup all data on the single volume on CKMFON1 and configure the disk with GUID partition table and create two volume
B. Restore the backed up data on one of the volumes and use the other for WINS service group
C. Add a new physical shared disk to the CKMFON1 cluster and configure a new volume on it
D. Use this volume to fix the error in the wizard
E. Add new physical shared disks to CKMFON1 and EMBFON2. Configure the volumes on these disk and direct CKMOFON1 to use CKMFON2 volume for the WINS service group
F. Add and configure a new volume on the existing shared disk which has 400GB of space
G. Use this volume to fix the error in the wizard
H. None of the above

Answer: B

Explanation:
http://class10e.com/Microsoft/which-action-should-you-perform-to-configure-storage-volumes-on-ckmfon1-to-successfully-add-the-wins-service-group-to-ckmfon1/

To configure storage volumes on CKMFON1 to successfully add the WINS Service group to CKMFON1, you need to add a new physical shared disk to the CKMFON1 cluster and configure a new volume on it. Use this volume to fix the error in the wizard. This is because a cluster does not use shared storage. A cluster must use a hardware solution based either on shared storage or on replication between nodes.

NEW QUESTION 4
One of the remote branch offices is running a Windows Server 2008 read only domain controller (RODC). For security reasons you don't want some critical credentials like (passwords, encryption keys) to be stored on RODC. What should you do so that these credentials are not replicated to any RODC's in the forest? (Select 2)

A. Configure RODC filtered attribute set on the server
B. Configure RODC filtered set on the server that holds Schema Operations Master role
C. Delegate local administrative permissions for an RODC to any domain user without granting that user any user rights for the domain
D. Configure forest functional level server for Windows server 2008 to configure filtered attribute set
E. None of the above

Answer: BD

Explanation:
http://technet.microsoft.com/en-us/library/cc753223.aspx Adding attributes to the RODC filtered attribute set The RODC filtered attribute set is a dynamic set of attributes that is not replicated to any RODCs in the forest. You can configure the RODC filtered attribute set on a schema master that runs Windows Server 2008. When the attributes are prevented from replicating to RODCs, that data cannot be exposed unnecessarily if an RODC is stolen or compromised. A malicious user who compromises an RODC can attempt to configure it in such a way that it tries to replicate attributes that are defined in the RODC filtered attribute set. If the RODC tries to replicate those attributes from a domain controller that is running Windows Server 2008, the replication request is denied. However, if the RODC tries to replicate those attributes from a domain controller that is running Windows Server 2003, the replication request could succeed. Therefore, as a security precaution, ensure that forest functional level is Windows Server 2008 if you plan to configure the RODC filtered attribute set. When the forest functional level is Windows Server 2008, an RODC that is compromised cannot be exploited in this manner because domain controllers that are running Windows Server 2003 are not allowed in the forest.

NEW QUESTION 5
Your network contains an Active Directory forest. The forest contains a single domain. You want to access resources in a domain that is located in another forest. You need to configure a trust between the domain in your forest and the domain in the other forest. What should you create?

A. an incoming external trust
B. an incoming realm trust
C. an outgoing external trust
D. an outgoing realm trust

Answer: A

Explanation:
A one-way, incoming, external trust allows users in your domain (the domain that you are logged on to at the time that you run the New Trust Wizard) to access resources in another Active Directory domain (outside your forest).

**NEW QUESTION 6**
Your network contains an Active Directory forest. The forest contains two domains. You have a standalone root certification authority (CA). On a server in the child domain, you run the Add Roles Wizard and discover that the option to select an enterprise CA is disabled. You need to install an enterprise subordinate CA on the server.

What should you use to log on to the new server?

A. an account that is a member of the Certificate Publishers group in the child domain
B. an account that is a member of the Certificate Publishers group in the forest root domain
C. an account that is a member of the Schema Admins group in the forest root domain
D. an account that is a member of the Enterprise Admins group in the forest root domain

**Answer:** D

**Explanation:**
http://social.technet.microsoft.com/Forums/uk/winserversecurity/thread/8874cec-12f6-4c15-a506-568db21d46b
In order to install Enterprise CA you MUST have Enterprise Admins permissions, because Configuration naming context is replicated between domain controllers in the forest (not only current domain) and are writable for Enterprise Admins (domain admins permissions are insufficient).

**NEW QUESTION 7**
You need to create a Password Settings object (PSO). Which tool should you use?

A. Active Directory Users and Computers
B. ADSI Edit
C. Group Policy Management Console
D. Ntdsutil

**Answer:** B

**Explanation:**

**NEW QUESTION 8**
Your network contains an Active Directory domain. All domain controllers run Windows Server 2008 R2. You need to create a snapshot of Active Directory. What should you do?

A. Run the dsquery.exe command
B. Run the dsamain.exe command
C. Create custom views from Event Viewer
D. Configure subscriptions from Event Viewer
E. Create a Data Collector Set (DCS).
F. Configure the Active Directory Diagnostics Data Collector Set (DCS).
G. Run the repadmin.exe command
H. Run the ntdsutil.exe command
I. Run the eventcreate.exe command
J. Run the eventcreate.exe command

**Answer:** H

**Explanation:**
http://technet.microsoft.com/en-us/library/cc753609.aspx To create an AD DS or AD LDS snapshot
1. Log on to a domain controller as a member of the Enterprise Admins groups or the Domain Admins group.
2. Click Start, right-click Command Prompt, and then click Run as administrator.
3. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.
4. At the elevated command prompt, type the following command, and then press ENTER: repadmin
5. At the ndsutil prompt, type the following command, and then press ENTER: snapshot
6. At the snapshot prompt, type the following command, and then press ENTER: activate instance ndsutil
7. At the snapshot prompt, type the following command, and then press ENTER: create

**NEW QUESTION 9**

When you ping Server1, you discover that the name fails to resolve. You are able to successfully ping server2.contoso.com. You need to ensure that you can resolve names by using the GlobalNames zone.

Which command should you run?

A. Dnscmd DC1.contoso.com /ZoneAdd GlobalNames /DsPrimary /DP /domain
B. Dnscmd DC1.contoso.com /config /Enableglobalnamesupport forest
C. Dnscmd DC1.contoso.com /config /Enableglobalnamesupport 1

Guaranteed success with Our exam guides visit https://www.certshared.com
NEW QUESTION 10
Your network contains an Active Directory domain named adatum.com. You need to ensure that IP addresses can be resolved to fully qualified domain names (FQDNs). Under which node in the DNS snap-in should you add a zone?
A. Reverse Lookup Zones
B. adatum.com
C. Forward Lookup Zones
D. Conditional Forwarders
E. _msdcs.adatum.com

Answer: A

Explanation:
Mastering Microsoft Windows Server 2008 R2 (Sybex, 2010) page 193
A forward lookup means the client provides a fully qualified domain name and the DNS server returns an IP address. A reverse lookup does the opposite: the client provides an IP address, and then the DNS server returns an FQDN.

NEW QUESTION 11
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and woodgrovebank.com. You have a custom attribute named Attribute 1 in Active Directory. Attribute 1 is associated to User objects. You need to ensure that Attribute1 is included in the global catalog. What should you do?
A. From the Active Directory Schema snap-in, modify the properties of the Attribute 1 attributeSchema object
B. In Active Directory Users and Computers, configure the permissions on the Attribute 1 attribute for User object
C. From the Active Directory Schema snap-in, modify the properties of the User classSchema object
D. In Active Directory Sites and Services, configure the Global Catalog settings for all domain controllers in the forest

Answer: A

Explanation:
Global Catalog Partial Attribute Set
The attributes that are replicated to the global catalog by default include a base set that have been defined by Microsoft as the attributes that are most likely to be used in searches. Administrators can use the Microsoft Management Console (MMC) Active Directory Schema snap-in to specify additional attributes to meet the needs of their installation. In the Active Directory Schema snap-in, you can select the Replicate this attribute to the global catalog check box to designate an attributeSchema object as a member of the PAS, which sets the value of the isMemberOfPartialAttributeSet attribute to TRUE. Global Catalog Replication of Additions to the Partial Attribute Set Each global catalog server in an AD DS forest hosts a copy of every existing object in that forest. For the objects of its own domain, a global catalog server has information related to all attributes that are associated with those objects. For the objects in domains other than its own, a global catalog server has only information that is related to the set of attributes that are marked in the AD DS schema to be included in the partial attribute set (PAS). As described earlier, the PAS is defined by Microsoft as those attributes that are most likely to be used for searches. These attributes are replicated to every global catalog server in an AD DS forest. If you want to add an attribute to the PAS, you can mark the attribute by using the Active Directory Schema snap-in to edit the isMemberOfPartialAttributeSet value on the respective attributeSchema object. You mark the attribute by placing a checkmark next to isMemberOfPartialAttributeSet. If the isMemberOfPartialAttributeSet value is checked (set to TRUE), the attribute is replicated to the global catalog. If the value is not checked (set to FALSE), the attribute is not replicated to the global catalog.

NEW QUESTION 12
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 zone
B. Run Dnscmd.exe, and specify the /enlistdirectorypartition parameter
C. From DNS Manager, right-click RODC1 and click Update Server Data File
D. Run Dnscmd.exe and specify the /createbuiltindirectorypartitions parameter

Answer: B

Explanation:

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<ServerName> /EnlistDirectoryPartition <FQDN>`
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`

NEW QUESTION 13
DRAG DROP
Your network contains an Active Directory forest named contoso.com. You need to create an Active Directory Rights Management Services (AD RMS) licensing-only cluster.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
NEW QUESTION 14
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. Active Directory Sites and Services
B. Active Directory Users and Computers
C. Security Configuration Wizard (SCW)
D. Local Security Policy

Answer: A

NEW QUESTION 15
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. Active Directory Users and Computers
B. Security Configuration Wizard (SCW)
C. Group Policy Management Editor
D. Active Directory Sites and Services

Answer: A

NEW QUESTION 16
You need to deactivate the UGMC option on some of your domain controllers.
At which level in Active Directory would you deactivate UGMC?

A. Server
B. Site
C. Domain
D. Forest

Answer: B

Explanation:
http://www.ntweekly.com/?p=788
http://gallery.technet.microsoft.com/scriptcenter/c1bd08d2-1440-40f8-95be-ad2050674d91 Script to Disable Universal Group Membership Caching in all Sites
How to Disable Universal Group Membership Caching in all Sites using a Script Starting with Windows Server 2003, a new feature called Universal Group Membership Caching (UGMC) caches a user's membership in Universal Groups on domain controllers authenticating the user. This feature allows a domain controller to have knowledge of Universal Groups a user is member of rather than contacting a Global Catalog.
Unlike Global group memberships, which are stored in each domain, Universal Group memberships are only stored in a Global Catalog. For example, when a user who belongs to a Universal Group logs on to a domain that is set to the Windows 2000 native domain functional level or higher, the Global Catalog provides Universal Group membership information for the user's account at the time the user logs on to the domain to the authenticating domain controller.
UGMC is generally a good idea for multiple domain forests when:
1. Universal Group membership does not change frequently.
2. Low WAN bandwidth between Domain Controllers in different sites.
It is also recommended to disable UGMC if all Domain Controllers in a forest are Global Catalogs.
NEW QUESTION 17
Your company, Contoso, Ltd., has a main office and a branch office. The offices are connected by a WAN link. Contoso has an Active Directory forest that contains a single domain named ad.contoso.com.
The ad.contoso.com domain contains one domain controller named DC1 that is located in the main office. DC1 is configured as a DNS server for the ad.contoso.com DNS zone. This zone is configured as a standard primary zone.
You need to ensure that DC2 can resolve DNS queries for ad.contoso.com in the event that a WAN link fails. The solution must prevent DC2 from updating records in ad.contoso.com.
What should you do?
A. Configure the DNS server on DC2 to forward requests to DC1.
B. Convert the ad.contoso.com zone on DC1 to an Active Directory-integrated zone
C. Create a new secondary zone named ad.contoso.com on DC2.
D. Create a new stub zone named ad.contoso.com on DC2.

Answer: B

NEW QUESTION 18
Your network contains an Active Directory domain named contoso.com.
The domain contains an enterprise certification authority (CA).
You plan to deploy certificates to all of the domain users. The certificates will be based on a custom Smartcard Logon template.
You need to recommend a solution to ensure that the users can log on to the domain by using smart cards.
What should you include in the recommendation?
A. From Certificate Templates, set the minimum certificate key size to 512.
B. From Active Directory Users and Computers, select Use Kerberos DES encryption types for this account
C. From Certificate Templates, include the user principal name (UPN) in the subject alternate name (SAN) of the template
D. From Active Directory Users and Computers, configure Published Certificates for user account

Answer: C

Explanation:
Request a smart card certificate from the third-party CA.
Enroll for a certificate from the third-party CA that meets the stated requirements. The method for enrollment varies by the CA vendor.
The smart card certificate has specific format requirements:
* Subject Alternative Name = Other Name: Principal Name= (UPN). For example:
  UPN = user1@name.com
  The UPN OtherName OID is : "1.3.6.1.4.1.311.20.2.3"
  The UPN OtherName value: Must be ASN1-encoded UTF8 string
* Subject = Distinguished name of user.
* The CRL Distribution Point (CDP) location (where CRL is the Certification Revocation List) must be populated, online, and available.
* Key Usage.= Digital Signature
* Basic Constraints.[Subject Type=End Entity, Path Length Constraint=None] (Optional)
* Enhanced Key Usage

NEW QUESTION 19
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2008 R2.
You need to increase the amount of Active Directory diagnostic information logged to the Event Viewer on DC1.
What should you do?
A. Modify the properties of the objects in the Active Directory Diagnostics Data Collector Set (DCS).
B. Modify the properties of the System Log and the Application Log
C. Modify the flags attribute of DC1.
D. Modify the settings in the HKey_Local_Machine\SYSTEM\CurrentControlSet\services\NTDS\Diagnostics registry key

Answer: D

NEW QUESTION 20
Your network contains an Active Directory domain. The domain contains several domain controllers. All domain controllers run Windows Server 2008 R2.
You need to restore the Default Domain Policy Group Policy object (GPO) to the Windows Server 2008 R2 default settings.
What should you do?
A. Run dcgpofix.exe /target:d
B. Run dcgpofix.exe /target:domain
C. Delete the link for the Default Domain Controllers Policy, and then run gupdate.exe /forc
D. Delete the link for the Default Domain Controllers Policy, and then run gupdate.exe /syn

Answer: B

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