70-412 Dumps

Configuring Advanced Windows Server 2012 Services

https://www.certleader.com/70-412-dumps.html

NEW QUESTION 1
You have 30 servers that run Windows Server 2012 R2.
All of the servers are backed up daily by using Windows Azure Online Backup.
You need to perform an immediate backup of all the servers to Windows Azure Online Backup.
Which Windows PowerShell cmdlets should you run on each server?

A. Get-OBPolicy | StartOBBackup
B. Start-OBRegistration | StartOBBackup
C. Get-WBPolicy | Start-WBBackup
D. Get-WBBackupTarget | Start-WBBackup

Answer: A

Explanation: This example starts a backup job using a policy. Windows PowerShell
PS C:\> Get-OBPolicy | Start-OBBackup
Incorrect:
Not B. Registers the current computer to Windows Azure Backup. Not C. Not using Azure
Not D. Not using Azure
Reference: Start-OBBackup
http://technet.microsoft.com/en-us/library/hh770406(v=wps.620).aspx

NEW QUESTION 2
You have a virtual machine named VM1 that runs on a host named Host1.
You configure VM1 to replicate to another host named Host2. Host2 is located in the same physical location as Host1.
You need to add an additional replica of VM1. The replica will be located in a different physical site.
What should you do?

A. From VM1 on Host2, click Extend Replication.
B. On Host1, configure the Hyper-V settings.
C. From VM1 on Host1, click Extend Replication.
D. On Host2, configure the Hyper-V settings.

Answer: A

Explanation: Extend Replication through UI:
Before you Extend Replication to third site, you need to establish the replication between a primary server and replica server.
Once that is done, go to replica site and from Hyper-V UI manager select the VM for which you want to extend the replication. Right click on VM and select
"Replication->Extend Replication …". This will open Extend Replication Wizard which is similar to Enable Replication Wizard.
NOTE: You configure a server to receive replication with Hyper-V Manager, in this situation the replica site is assumed to be the Replica Server. Therefore you extend replication from VM1 on Host2.
Note 2: With Hyper-V Extend Replication feature in Windows Server 2012 R2, customers
can have multiple copies of data to protect them from different outage scenarios. For example, as a customer I might choose to keep my second DR site in the same campus or a few miles away while I want to keep my third copy of data across the continents to give added protection for my workloads. Hyper-V Replica Extend replication exactly addresses this problem by providing one more copy of workload at an extended site apart from replica site.
Reference: Hyper-V Replica: Extend Replication http://blogs.technet.com/b/virtualization/archive/2013/12/10/hyper-v-replica-extend-replication.aspx

NEW QUESTION 3
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.
Server1 and Server2 have the Network Load Balancing (NLB) feature installed. The servers are configured as nodes in an NLB cluster named Cluster1. Both servers connect to the same switch.
Cluster1 hosts a secure web Application named WebApp1. WebApp1 saves user state information in a central database.
You need to ensure that the connections to WebApp1 are distributed evenly between the nodes. The solution must minimize port flooding.
What should you configure? To answer, configure the appropriate affinity and the appropriate mode for Cluster1 in the answer area.

Affinity [▼]
Single
Client
Class C

Mode [▼]
Unicast
Multicast

Answer:

Explanation: The Affinity parameter is applicable only for the Multiple hosts filtering mode.
/ The Single option specifies that NLB should direct multiple requests from the same client IP address to the same cluster host.

NEW QUESTION 4
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the DHCP Server server role installed.
An administrator installs the IP Address Management (IPAM) Server feature on a server named Server2. The administrator configures IPAM by using Group Policy based provisioning and starts server discovery.
You plan to create Group Policies for IPAM provisioning.
You need to identify which Group Policy object (GPO) name prefix must be used for IPAM Group Policies.
What should you do on Server2?

A. From Server Manager, review the IPAM overview.
B. Run the ipamgc.exe tool.
C. From Task Scheduler, review the IPAM tasks.
D. Run the Get-IpamConfiguration cmdlet.

Answer: D

Explanation: Example:

```
PS C:\Users\Administrator> Get-IpamConfiguration

Version       Port       ProvisioningMethod       GpoPrefix       HmacKey
-------       ----       ------------------       ---------       -------
6.3.0.1       48885      Automatic                thisistheprefix System.Security.Secu...
```


NEW QUESTION 5
Your network contains two servers named Server1 and Server2 that run Windows Server 2012 R2.
Both servers have the Hyper-V server role installed. Server1 and Server2 are located in different offices. The offices connect to each other by using a high-latency WAN link.
Server2 hosts a virtual machine named VM1.
You need to ensure that you can start VM1 on Server1 if Server2 fails. The solution must minimize hardware costs.
What should you do?

A. On Server1, install the Multipath I/O (MPIO) featur
B. Modify the storage location of the VHDs for VM1.
C. From the Hyper-V Settings of Server2, modify the Replication Configuration setting
D. Enable replication for VM1.
E. On Server2, install the Multipath I/O (MPIO) featur
F. Modify the storage location of the VHDs for VM1.
G. From the Hyper-V Settings of Server1, modify the Replication Configuration setting
H. Enable replication for VM1.

Answer: D

Explanation: You first have to enable replication on the Replica server--Server1--by going to the server and modifying the "Replication Configuration" settings under Hyper-V settings. You then go to VM1--which presides on Server2-- and run the "Enable Replication" wizard on VM1.
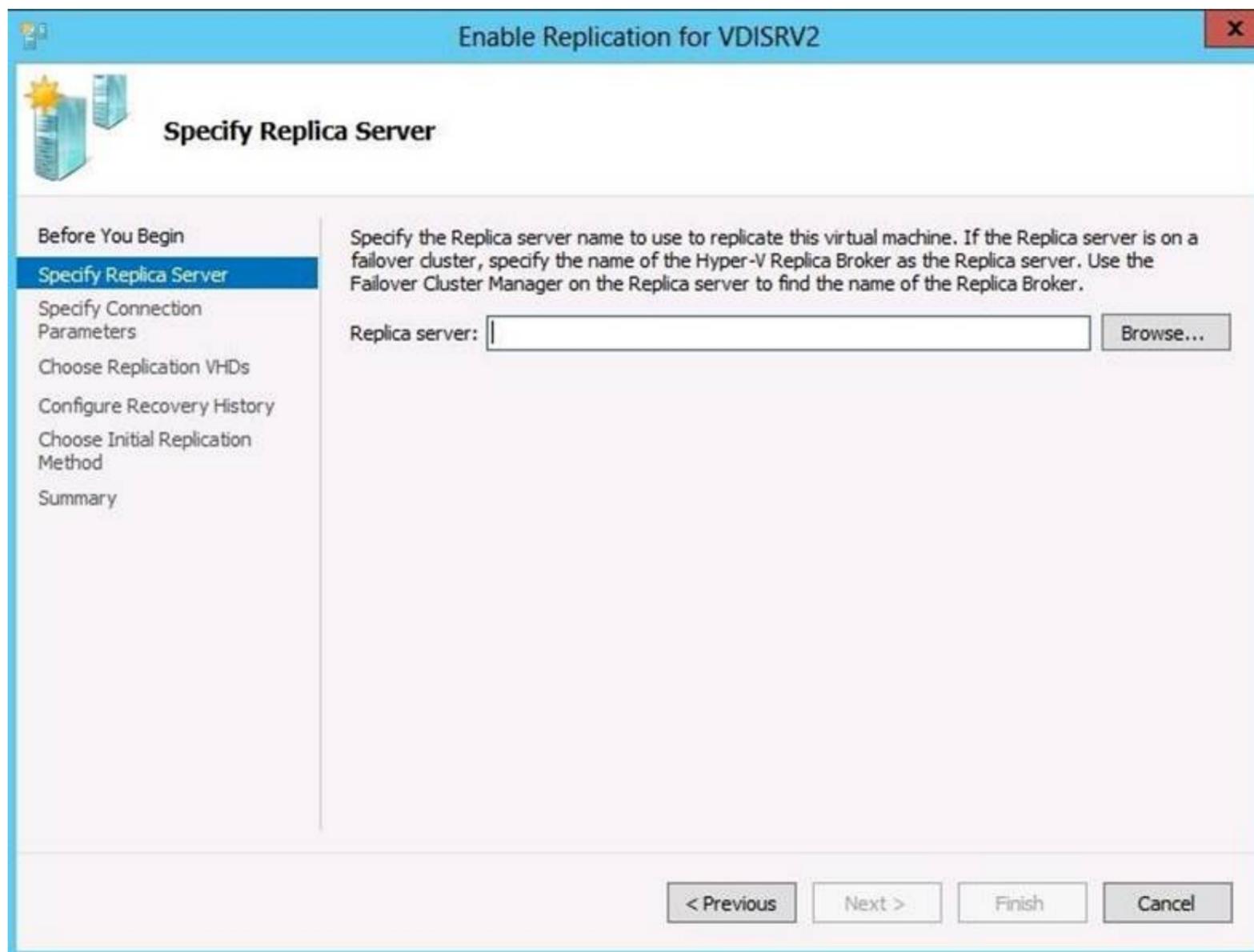
NEW QUESTION 6
Your network contains an Active directory forest named contoso.com. The forest contains two child domains named east.contoso.com and west.contoso.com.
You install an Active Directory Rights Management Services (AD RMS) cluster in each child domain.
You discover that all of the users in the contoso.com forest are directed to the AD RMS cluster in east.contoso.com.
You need to ensure that the users in west.contoso.com are directed to the AD RMS cluster in west.contoso.com and that the users in east.contoso.com are directed to the AD RMS cluster in east.contoso.com.
What should you do?

A. Modify the Service Connection Point (SCP).
B. Configure the Group Policy object (GPO) settings of the users in the west.contoso.com domain.
C. Configure the Group Policy object (GPO) settings of the users in the east.contoso.com domain.
D. Modify the properties of the AD RMS cluster in west.contoso.com.

Answer: B

Explanation: The west.contoso.com are the ones in trouble that need to be redirected to the west.contoso.com not the east.contoso.com.
Note: It is recommended that you use GPO to deploy AD RMS client settings and that you only deploy settings as needed.
Reference: AD RMS Best Practices Guide

NEW QUESTION 7
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. The system properties of Server1 are shown in the exhibit. (Click the Exhibit button.)
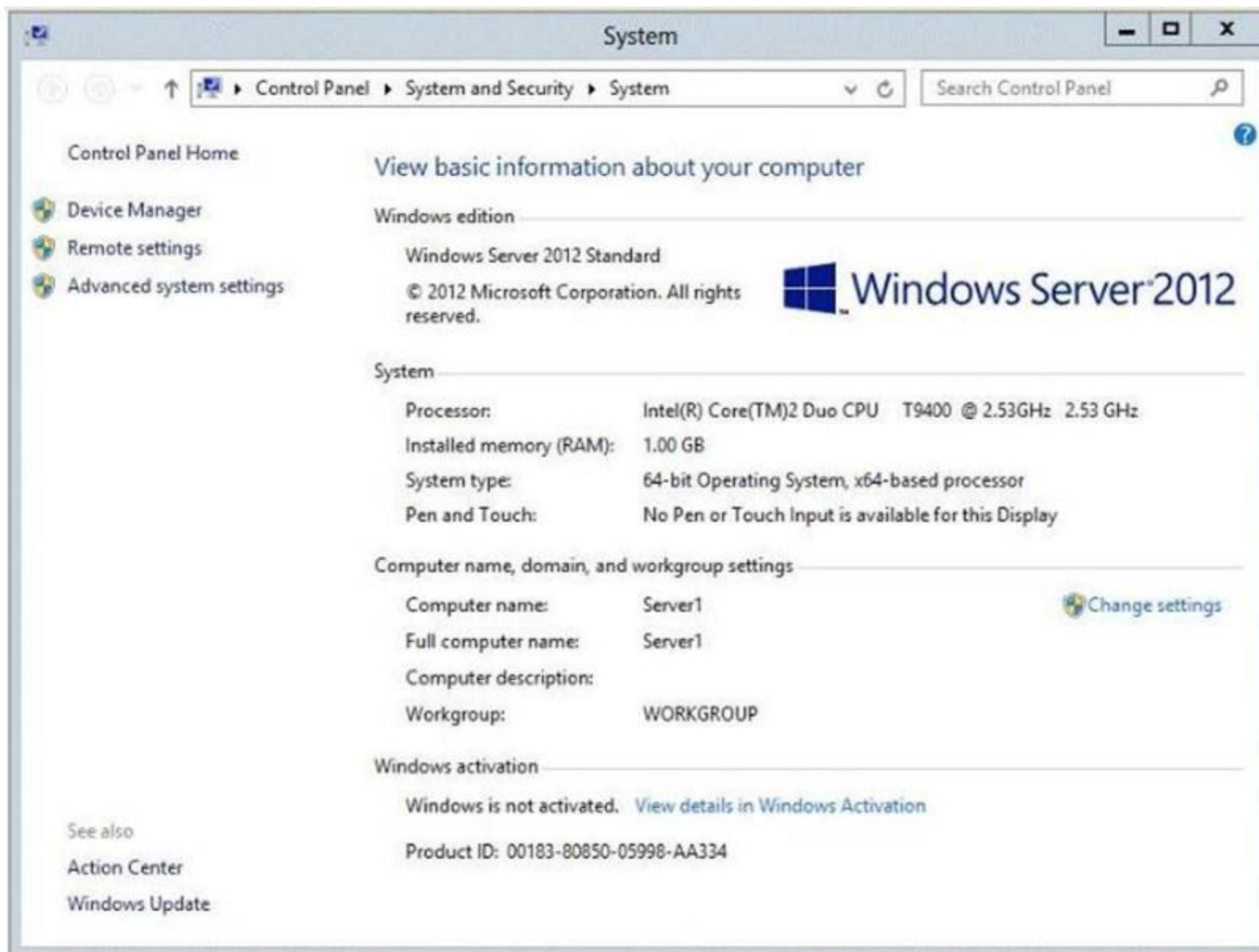
You need to configure Server1 as an enterprise subordinate certification authority (CA). What should you do first?

A. Add RAM to the server.
B. Set the Startup Type of the Certificate Propagation service to Automatic.
C. Install the Certification Authority Web Enrollment role service.
D. Join Server1 to the contoso.com domain.

Answer: D

Explanation: Enterprise CAs must be domain members. From the exhibit we see that it is only a Workgroup member.
Note:
A new CA can be the root CA of a new PKI or subordinate to another in an existing PKI.
Enterprise subordinate certification authority.
An enterprise subordinate CA must get a CA certificate from an enterprise root CA but can then issue certificates to all users and computers in the enterprise.
These types of CAs are often used for load balancing of an enterprise root CA.

AD CS Configuration

DESTINATION SERVER
DC1.home.local

Setup Type

Credentials
Role Services
Setup Type
CA Type
Private Key
  Cryptography
  CA Name
  Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

◉ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

< Previous   Next >   Configure   Cancel

Reference: Install a Subordinate Certification Authority

NEW QUESTION 8
DRAG DROP
Your network contains an Active Directory domain named contoso.com.
You need to ensure that third-party devices can use Workplace Join to access domain resources on the Internet.
Which four actions should you perform in sequence?
To answer, move the appropriate four actions from the list of actions to the answer area and arrange them in the correct order.

	Answer Area
Create a claims provider trust.	
Create an attribute store.	
Enable the Device Registration Service.	
Install a certificate obtained from a trusted third-party certification authority (CA).	
Install and configure Active Directory Federation Services (AD FS).	
Install and configure a Web Application Proxy.	

Answer:

Explanation: Note:
* Checklist: Deploying a Federation Server Farm include:
(Box 1) Enroll a Secure Socket Layer (SSL) certificate for AD FS. (Box 2) Install the AD FS role service.
(Box 3, box 4) Optional step: Configure a federation server with Device Registration Service (DRS).
Box 3: To enable Device Registration Service.
On your federation server, open a Windows PowerShell command window and type: Enable-AdfsDeviceRegistration
Repeat this step on each federation farm node in your AD FS farm.. Box 4: Update the Web Application Proxy configuration
The Device Registration Service will be available through the Web Application Proxy once it is enabled on a federation server. You may need to complete this

procedure to update the Web Application Proxy configuration if it was deployed prior to enabling the Device Registration Service.
* Workplace Join is made possible by the Device Registration Service (DRS) that is included with the Active Directory Federation Role in Windows Server 2012 R2. When a device is Workplace Joined, the DRS provisions a device object in Active Directory and sets a certificate on the consumer device that is used to represent the device identity. The DRS is meant to be both internal and external facing. Companies that deploy both DRS and the Web Application Proxy will be able to Workplace Join devices from any internet connected location.

NEW QUESTION 9
You have a server named Server1 that runs Windows Server 2012 R2.
From Server Manager, you install the Active Directory Certificate Services server role on Server1.
A domain administrator named Admin1 logs on to Server1.
When Admin1 runs the Certification Authority console, Admin1 receives the following error message.
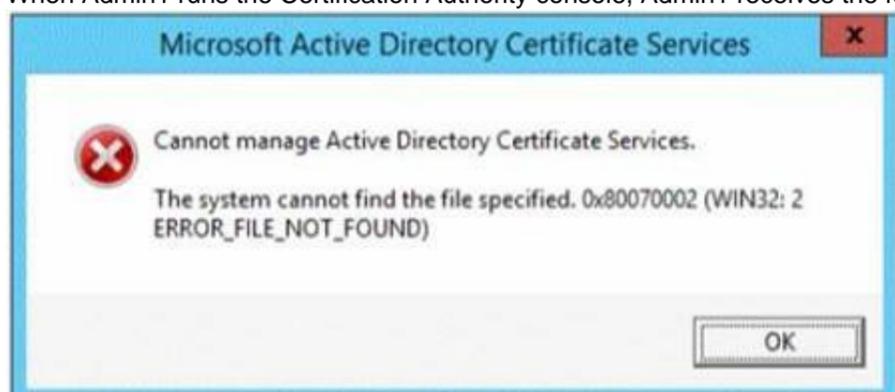
You need to ensure that when Admin1 opens the Certification Authority console on Server1, the error message does not appear.
What should you do?

A. Install the Active Directory Certificate Services (AD CS) tools.
B. Run the regsvr32.exe command.
C. Modify the PATH system variable.
D. Configure the Active Directory Certificate Services server role from Server Manager.

Answer: D

Explanation: The error message is related to missing role configuration.
* Cannot Manage Active Directory Certificate Services
Resolution: configure the two Certification Authority and Certification Authority Web Enrollment Roles:
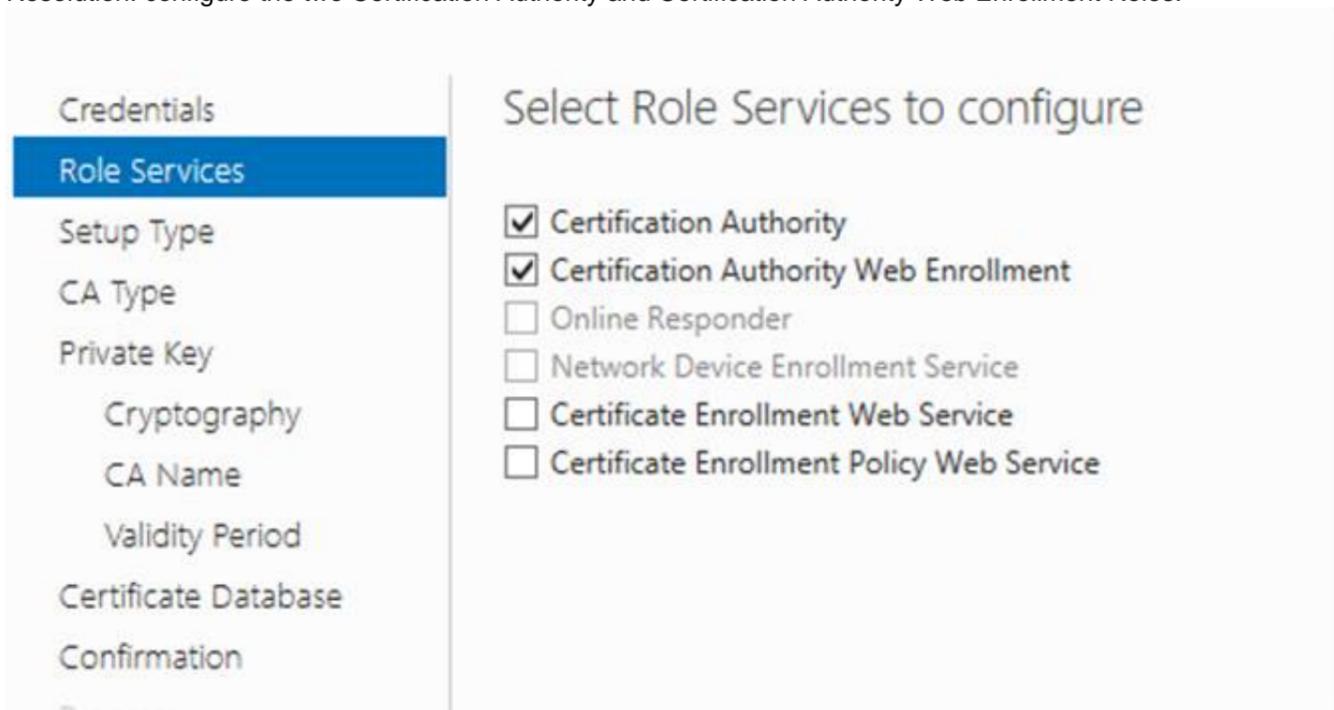
Reference: Cannot manage Active Directory Certificate Services in Server 2012 Error 0x800070002

NEW QUESTION 10
DRAG DROP
Your network contains an Active Directory domain named contoso.com. The domain contains four member servers named Server1, Server2, Servers, and Server4. All servers run Windows Server 2012 R2.
Server1 and Server2 are located in a site named Site1. Server3 and Server4 are located in a site named Site2. The servers are configured as nodes in a failover cluster named Cluster1.
Cluster1 is configured to use the Node Majority quorum configuration.
You need to ensure that Server1 is the only server in Site1 that can vote to maintain quorum.
What should you run from Windows PowerShell?
To answer, drag the appropriate commands to the correct location. Each command may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Commands		Answer Area	
Get-ClusterNode Server1		Command	Command
Get-ClusterNode Server2			
$_.NodeWeight = 0			
$_.NodeWeight = 1			
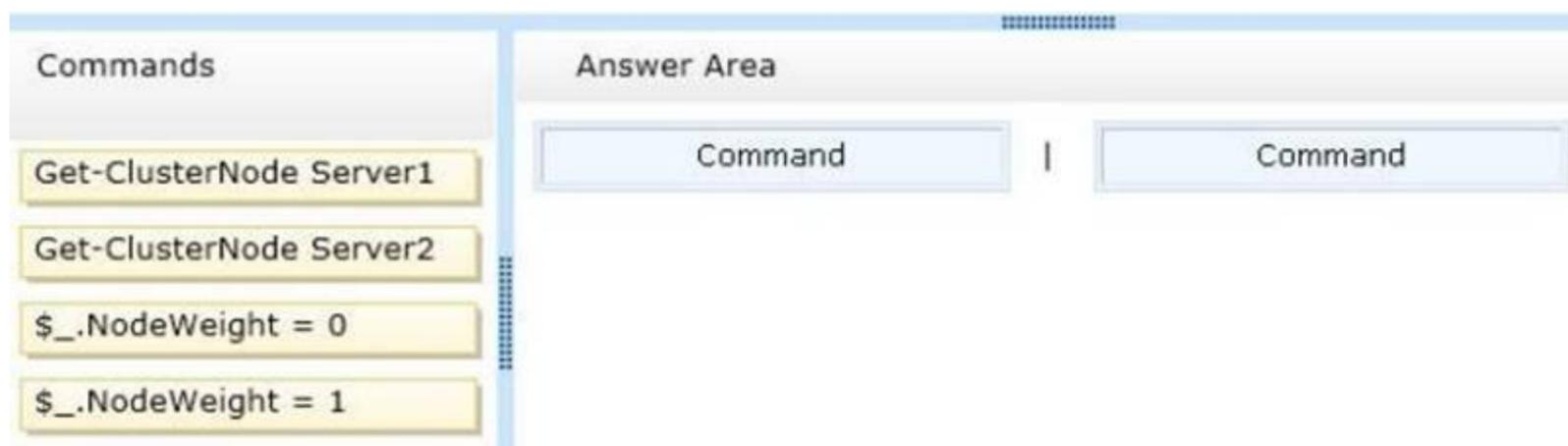
Answer:

Explanation: We remove Server2 from quorum vote by setting it's NodeWeight to 0.
NodeWeight settings are used during quorum voting to support disaster recovery and multi- subnet scenarios for AlwaysOn Availability Groups and SQL Server Failover Cluster Instances.
Example (Powershell)
The following example changes the NodeWeight setting to remove the quorum vote for the "AlwaysOnSrv1" node.
Import-Module FailoverClusters
$node = "AlwaysOnSrv1"
(Get-ClusterNode $node).NodeWeight = 0

NEW QUESTION 10
HOTSPOT
You have a file server named Server1 that runs Windows Server 2012 R2.
You need to ensure that you can use the NFS Share - Advanced option from the New Share Wizard in Server Manager.
Which two role services should you install?
To answer, select the appropriate two role services in the answer area.
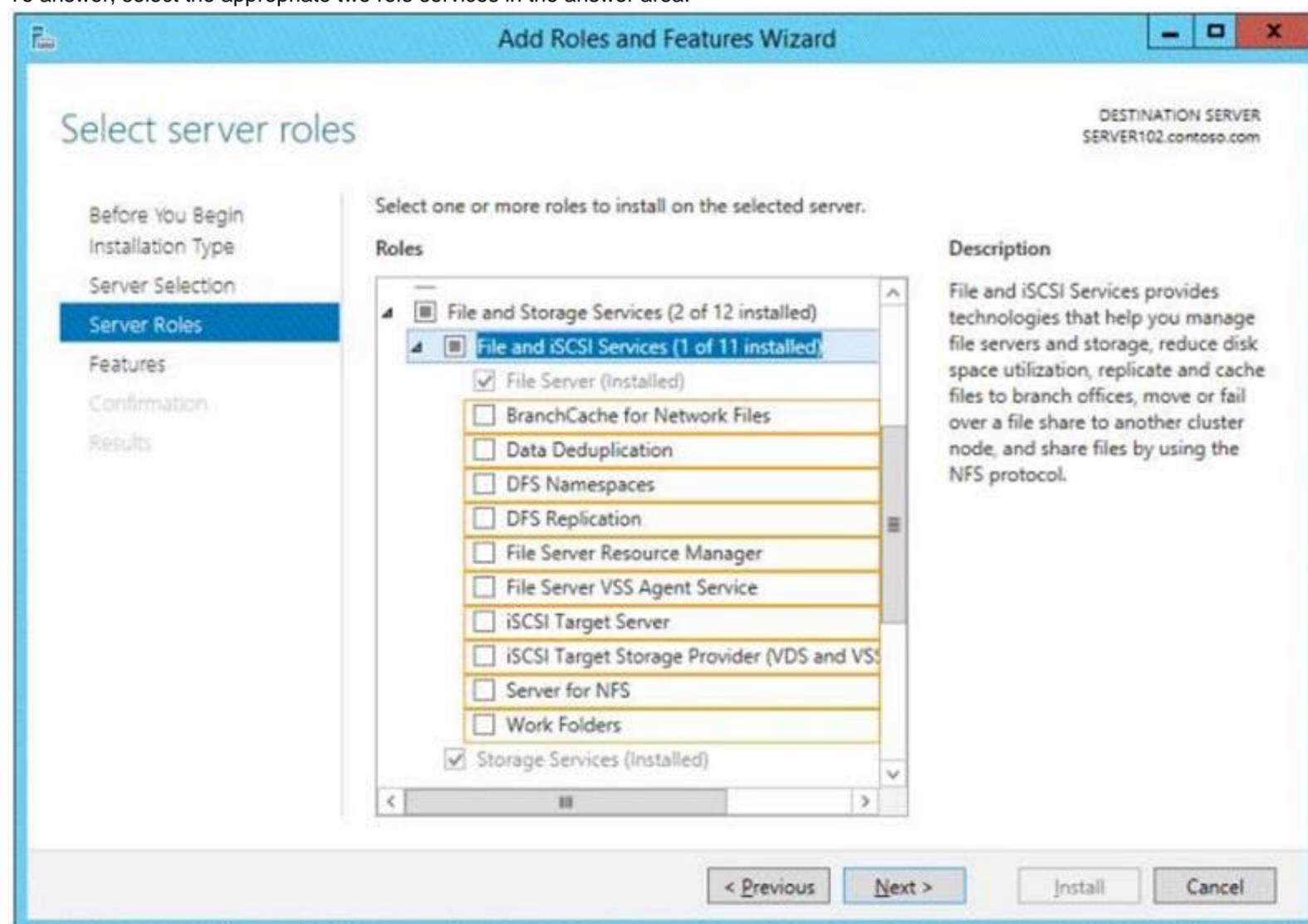
Answer:

Explanation: *File Server Resource Manager Role
File Server Resource Manager is a set of features that allow you to manage and classify data that is stored on file servers.
Note: NFS Share – Advanced
This advanced profile offers additional options to configure a NFS file share.
Set the folder owners for access-denied assistance
Configure default classification of data in the folder for management and access policies Enable quotas

NEW QUESTION 12
You create a new virtual disk in a storage pool by using the New Virtual Disk Wizard. You discover that the new virtual disk has a write-back cache of 1 GB.
You need to ensure that the virtual disk has a write-back cache of 5 GB. What should you do?

A. Detach the virtual disk, and then run the Resize-VirtualDisk cmdlet.
B. Detach the virtual disk, and then run the Set-VirtualDisk cmdlet.
C. Delete the virtual disk, and then run the New-StorageSubSystemVirtualDisk cmdlet.
D. Delete the virtual disk, and then run the New-VirtualDisk cmdlet.

Answer: D

Explanation: So what about changing the cache size? Well, you can't modify the cache size, but you can specify it at the time that you create a new virtual hard disk. In order to do so, you have to use Windows PowerShell.
New-VirtualDisk –StoragePoolFriendlyName "<storage pool name>" –FriendlyName "<v Reference: Using Windows Server 2012's SSD Write-Back Cache

NEW QUESTION 13
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2.
Server1 has the Active Directory Certificate Services server role installed and configured.
For all users, you are deploying smart cards for logon. You are using an enrollment agent
to enroll the smart card certificates for the users.
You need to configure the Contoso Smartcard Logon certificate template to support the use of the enrollment agent.
Which setting should you modify? To answer, select the appropriate setting in the answer area.
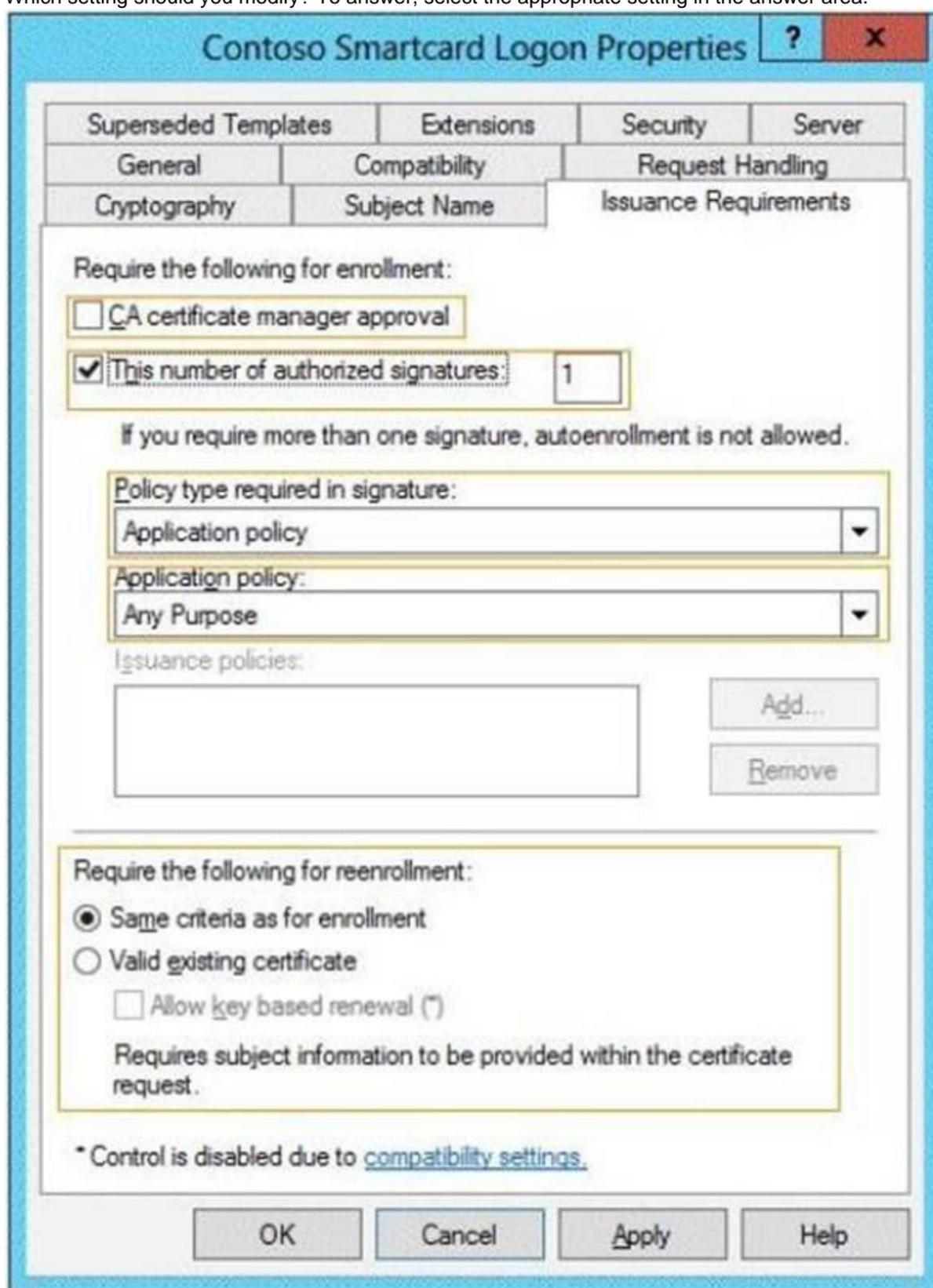
Answer:

Explanation: / In application policy drop-down list select Certificate Request Agent.
/ The Issuance Requirements Tab

* Application policy. This option specifies the application policy that must be included in the signing certificate used to sign the certificate request. It is enabled when Policy type required in signature is set to either Application policy or Both application and issuance policy.

NEW QUESTION 16
HOTSPOT
Your network contains an Active Directory domain named contoso.com.
You have a failover cluster named Cluster1 that contains two nodes named Server1 and Server2. Both servers run Windows Server 2012 R2 and have the Hyper-V server role installed.
You plan to create two virtual machines that will run an application named App1. App1 will store data on a virtual hard drive named App1data.vhdx. App1data.vhdx will be shared by both virtual machines.
The network contains the following shared folders:
? An SMB file share named Share1 that is hosted on a Scale-Out File Server.
? An SMB file share named Share2 that is hosted on a standalone file server.
? An NFS share named Share3 that is hosted on a standalone file server.
You need to ensure that both virtual machines can use App1data.vhdx simultaneously.
What should you do?
To answer, select the appropriate configurations in the answer area.

Answer Area

Location of App1data.vhdx: [▼]

App1data.vhdx disk type: [▼]

Location of App1data.vhdx: [▼]
                          Share1
                          Share2
                          Share3

App1data.vhdx disk type: [▼]
                         Differencing
   Dynamically expanding

Answer:

Explanation: * Simultaneous access to vhd can only be done by scale-out file server
* Create your VHDX data files to be shared as fixed-size or dynamically expanding, on the disk where you manually attached the Shared VHDX filter. Old VHD files are not allowed. Differencing disks are not allowed.

NEW QUESTION 21
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server3 that runs Windows Server 2012 R2 and has the DHCP Server server role installed.
DHCP is configured as shown in the exhibit. (Click the Exhibit button.)
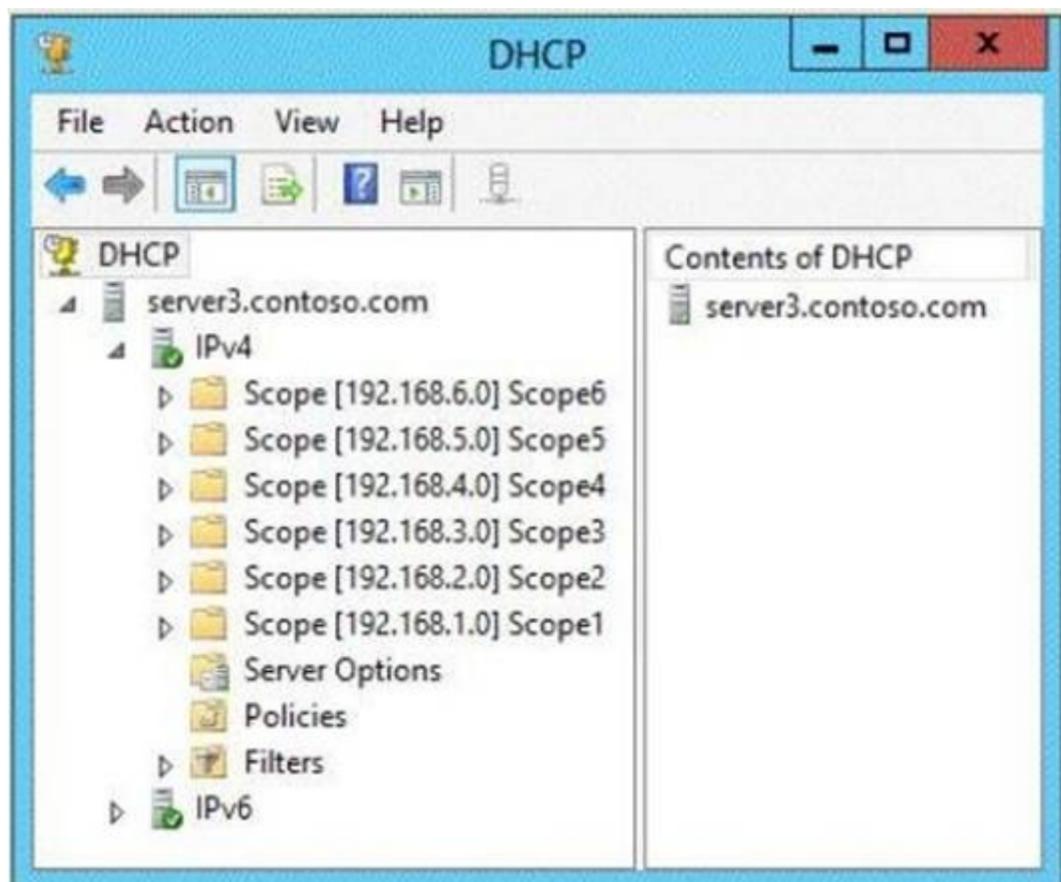
You need to ensure that only Scope1, Scope3, and Scope5 assign the same DNS servers to DHCP clients. The solution must minimize administrative effort.
What should you do?

A. Create a superscope and scope-level policies.
B. Configure the Scope Options.
C. Create a superscope and a filter.
D. Configure the Server Options.

Answer: B

Explanation: Any DHCP scope options can be configured for assignment to DHCP clients, such as DNS server.
Reference: Configuring a DHCP Scope. http://technet.microsoft.com/en-us/library/dd759218.aspx

NEW QUESTION 25
Your network contains 20 iSCSI storage appliances that will provide storage for 50 Hyper-V hosts running Windows Server 2012 R2.
You need to configure the storage for the Hyper-V hosts. The solution must minimize administrative effort.
What should you do first?

A. Install the iSCSI Target Server role service and configure iSCSI targets.
B. Install the iSNS Server service feature and create a Discovery Domain.
C. Start the Microsoft iSCSI Initiator Service and configure the iSCSI Initiator Properties.
D. Install the Multipath I/O (MPIO) feature and configure the MPIO Properties.

Answer: A

Explanation: Windows Server 2012 includes an iSCSI Target role that, along with Failover Clustering, allows it to become a cost-effective and highly-available iSCSI Storage Array.
We can connect from our Hyper-V host to the iSCSI target on the storage array with the following PowerShell command line:
New-IscsiTargetPortal –TargetPortalAddress <IP_Address or FQDN of storage array>
$target = Get-IscsiTarget
Connect-IscsiTarget –NodeAddress $target.NodeAddress Incorrect:
Not B. Discovery Domains in an iSCSI fabric, like zones in a Fibre Channel fabric, enable you to partition the storage resources in your storage area network (SAN). By creating and managing Discovery Domains, you can control the iSCSI targets that each iSCSI initiator can see and log on to.
Reference: Configure iSCSI Target Server Role on Windows Server 2012

NEW QUESTION 27
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run either Windows Server 2003, Windows Server 2008 R2, or Windows Server 2012 R2.
You plan to implement a new Active Directory forest. The new forest will be used for testing and will be isolated from the production network.
In the test network, you deploy a server named Server1 that runs Windows Server 2012 R2.
You need to configure Server1 as a new domain controller in a new forest named contoso.test.
The solution must meet the following requirements:
? The functional level of the forest and of the domain must be the same as that of contoso.com.
? Server1 must provide name resolution services for contoso.test.
What should you do?
To answer, configure the appropriate options in the answer area.

Active Directory Domain Services Configuration Wizard   — □ X

Domain Controller Options

TARGET SERVER
Server1

Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: [▼]

Domain functional level: [▼]

Specify domain controller capabilities

☐ Domain Name System (DNS) server
☑ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: [••••••••••••]

Confirm password: [••••••••••••]

More about domain controller options

[< Previous] [Next >]   [Install]   [Cancel]

Active Directory Domain Services Configuration Wizard   — □ X

Domain Controller Options

TARGET SERVER
Server1

Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: [▼]
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012

Domain functional level: [▼]
Windows Server 2003
Specify domain controller capabilities   Windows Server 2008
Windows Server 2008 R2
☐ Domain Name System (DNS) server   Windows Server 2012
☑ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: [••••••••••••]

Confirm password: [••••••••••••]

More about domain controller options

[< Previous] [Next >]   [Install]   [Cancel]

Answer:

Explanation: Set the forest function level and the Domain functional level both to Windows Server 2003. Also check Domain Name (DNS) server.
Note:
* When you deploy AD DS, set the domain and forest functional levels to the highest value that your environment can support. This way, you can use as many AD DS features as possible. For example, if you are sure that you will never add domain controllers that run Windows Server 2003 to the domain or forest, select the Windows Server 2008 functional level during the deployment process. However, if you might retain or add domain controllers that run Windows Server 2003, select the Windows Server 2003 functional level.
* You can set the domain functional level to a value that is higher than the forest functional level. For example, if the forest functional level is Windows Server 2003, you can set the domain functional level to Windows Server 2003or higher.

NEW QUESTION 29
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2.
Server1 has the Active Directory Certificate Services server role installed and is configured as an enterprise certification authority (CA).
You need to ensure that all of the users in the domain are issued a certificate that can be used for the following purposes:
? Email security
? Client authentication
? Encrypting File System (EFS)
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. From a Group Policy, configure the Certificate Services Client – Auto-Enrollmentsettings.
B. From a Group Policy, configure the Certificate Services Client – Certificate Enrollment Policy settings.
C. Modify the properties of the User certificate template, and then publish the template.
D. Duplicate the User certificate template, and then publish the template.
E. From a Group Policy, configure the Automatic Certificate Request Settings settings.

Answer: AD

Explanation: The default user template supports all of the requirements EXCEPT auto enroll as shown below:

| Permissions for Authenticated Users	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☐	☐
Enroll	☐	☐

For special permissions or advanced settings, click Advanced.

However a duplicated template from users has the ability to autoenroll:

Permissions for Authenticated Users	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☐	☐
Enroll	☐	☐
Autoenroll	☑	☐

The Automatic Certificate Request Settings GPO setting is only available to Computer, not user.
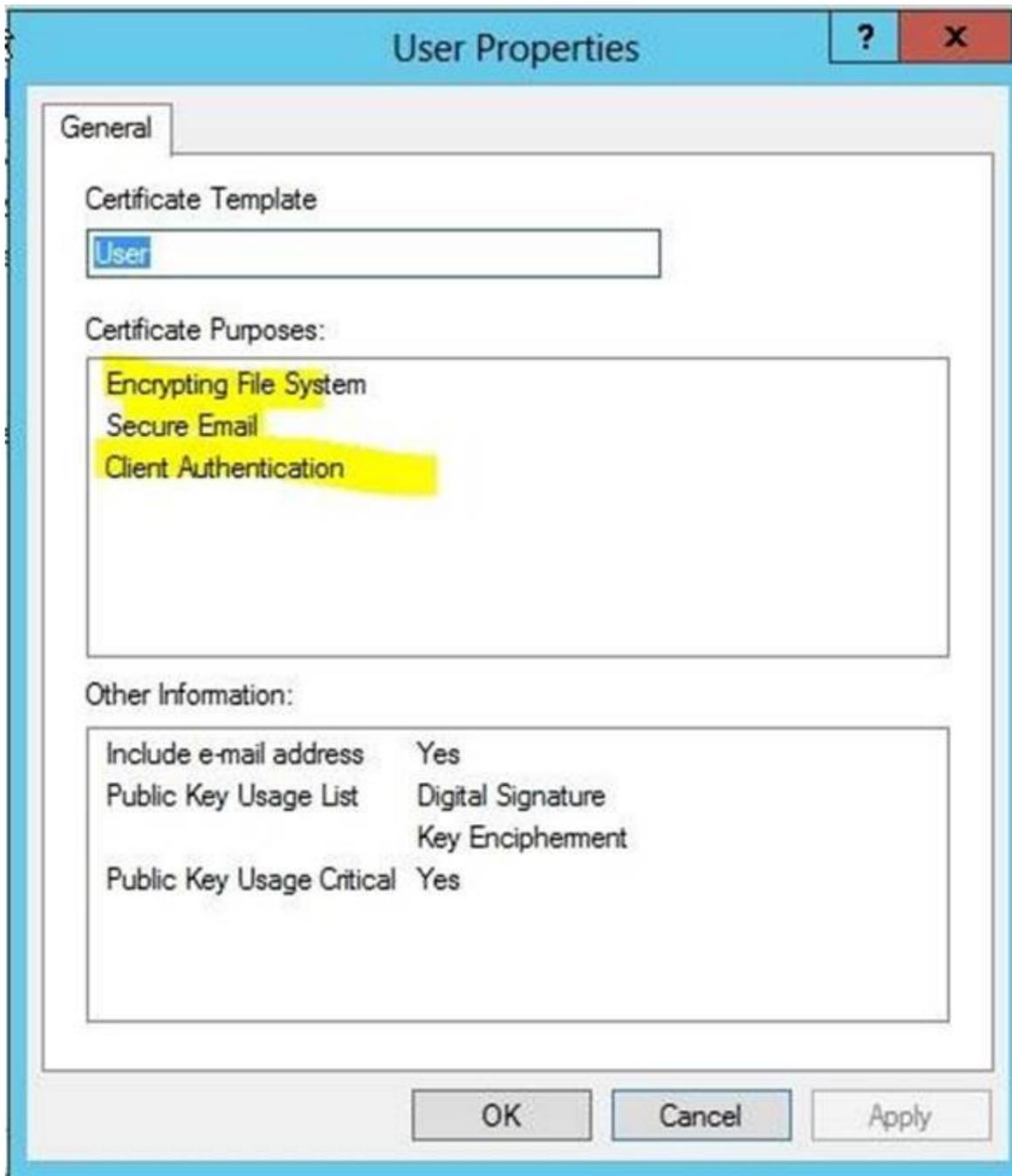
Reference: Manage Certificate Enrollment Policy by Using Group Policy. http://technet.microsoft.com/en-us/library/dd851772.aspx

NEW QUESTION 32
Your network contains two DNS servers named DNS1 and DNS2 that run Windows Server 2012 R2.
DNS1 has a primary zone named contoso.com. DNS2 has a secondary copy of the contoso.com zone.
You need to log the zone transfer packets sent between DNS1 and DNS2. What should you configure?

A. Monitoring from DNS Manager
B. Logging from Windows Firewall with Advanced Security
C. A Data Collector Set (DCS) from Performance Monitor
D. Debug logging from DNS Manager

Answer: D

Explanation: Debug logging allows you to log the packets sent and received by a DNS server. Debug logging is disabled by default, and because it is resource intensive, you should only activate it temporarily when you need more specific detailed information about server performance.
Reference: Active Directory 2008: DNS Debug Logging Facts.

NEW QUESTION 36
HOTSPOT
Your company has a primary data center and a disaster recovery data center.
The network contains an Active Directory domain named contoso.com. The domain contains a server named that runs Windows Server 2012 R2. Server1 is located in the primary data center.
Server1 has an enterprise root certification authority (CA) for contoso.com.
You deploy another server named Server2 to the disaster recovery data center.
You plan to configure Server2 as a secondary certificate revocation list (CRL) distribution point.
You need to configure Server2 as a CRL distribution point (CDP).
Which tab should you use to configure the required CDP entry? To answer, select the appropriate tab in the answer area.

contoso-Root-CA Properties

Extensions	Storage	Certificate Managers
Enrollment Agents	Auditing	Recovery Agents	Security
General	Policy Module	Exit Module

Certification authority (CA)

Name: contoso-Root-CA

CA certificates:

Certificate #0

[View Certificate]

Cryptographic settings

Provider: Microsoft Software Key Storage Provider

Hash algorithm: SHA1

[OK] [Cancel] [Apply] [Help]

Answer:

Explanation: To configure the CDP and AIA extensions on CA1
Etc.
uk.co.certification.simulator.questionpool.PList@cb55af0

NEW QUESTION 38
Your network contains an Active Directory forest named contoso.com. The forest contains two domains named contoso.com and childl.contoso.com. The domains contain three domain controllers.
The domain controllers are configured as shown in the following table.

Domain controller name	Operating system	Configuration
dc1.contoso.com	Windows Server 2008 R2	Schema master Domain naming master
dc10.child1.contoso.com	Windows Server 2012	PDC emulator
dc11.child1.contoso.com	Windows Server 2008 R2	RID master

You need to ensure that the KDC support for claims, compound authentication, and kerberos armoring setting is enforced in the child1.contoso.com domain.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Upgrade DC1 to Windows Server 2012 R2.
B. Upgrade DC11 to Windows Server 2012 R2.
C. Raise the domain functional level of childl.contoso.com.
D. Raise the domain functional level of contoso.com.
E. Raise the forest functional level of contoso.com.

Answer: AD

Explanation: The root domain in the forest must be at Windows Server 2012 level. First upgrade DC1 to this level (A), then raise the contoso.com domain functional level to Windows Server 2012 (D).

* (A) To support resources that use claims-based access control, the principal's domains will need to be running one of the following:
/ All Windows Server 2012 domain controllers
/ Sufficient Windows Server 2012 domain controllers to handle all the Windows 8 device authentication requests
/ Sufficient Windows Server 2012 domain controllers to handle all the Windows Server 2012 resource protocol transition requests to support non-Windows 8 devices.
Reference: What's New in Kerberos Authentication http://technet.microsoft.com/en-us/library/hh831747.aspx.

NEW QUESTION 39
You have a server named Server1 that runs Windows Server 2012 R2. Each day, Server1 is backed up fully to an external disk.
On Server1, the disk that contains the operating system fails. You replace the failed disk.
You need to perform a bare-metal recovery of Server1 by using the Windows Recovery Environment (Windows RE).
What should you do?

A. Run the Start-WBVolumeRecovery cmdlet and specify the -backupset parameter.
B. Run the Get-WBBareMetalRecovery cmdlet and specify the -policy parameter.
C. Run the wbadmin.exe start recovery command and specify the -recoverytarget parameter.
D. Run the wbadmin.exe start sysrecovery command and specify the -backuptarget parameter.

Answer: D

Explanation: Performs a system recovery (bare metal recovery). This subcommand can be run only from the Windows Recovery Environment.
* -backupTarget
Specifies the storage location that contains the backup or backups that you want to recover. This parameter is useful when the storage location is different from where backups of this computer are usually stored.
Reference: Wbadmin start sysrecovery http://technet.microsoft.com/en-us/library/cc742118.aspx

NEW QUESTION 41
Your network contains an Active Directory forest named contoso.com. The forest contains three domains. All domain controllers run Windows Server 2012 R2.
The forest has a two-way realm trust to a Kerberos realm named adatum.com.
You discover that users in adatum.com can only access resources in the root domain of contoso.com.
You need to ensure that the adatum.com users can access the resources in all of the domains in the forest.
What should you do in the forest?

A. Delete the realm trust and create a forest trust.
B. Delete the realm trust and create three external trusts.
C. Modify the incoming realm trust.
D. Modify the outgoing realm trust.

Answer: D

Explanation: * A one-way, outgoing realm trust allows resources in your Windows Server domain (the domain that you are logged on to at the time that you run the New Trust Wizard) to be accessed by users in the Kerberos realm.
* You can establish a realm trust between any non-Windows Kerberos version 5 (V5) realm and an Active Directory domain. This trust relationship allows cross-platform interoperability with security services that are based on other versions of the Kerberos V5 protocol, for example, UNIX and MIT implementations. Realm trusts can switch from nontransitive to transitive and back. Realm trusts can also be either one-way or two-way.
Reference: Create a One-Way, Outgoing, Realm Trust

NEW QUESTION 46
You have 20 servers that run Windows Server 2012 R2.
You need to create a Windows PowerShell script that registers each server in Windows Azure Backup and sets an encryption passphrase.
Which two PowerShell cmdlets should you run in the script? (Each correct answer presents part of the solution. Choose two.)

A. New-OBPolicy
B. New-OBRetentionPolicy
C. Add-OBFileSpec
D. Start-OBRegistration
E. Set OBMachineSetting

Answer: DE

Explanation: D. Start-OBRegistration
Registers the current computer with Windows Azure Online Backup using the credentials (username and password) created during enrollment.
E. The Set-OBMachineSetting cmdlet sets a OBMachineSetting object for the server that includes proxy server settings for accessing the internet, network bandwidth throttling settings, and the encryption passphrase that is required to decrypt the files during recovery to another server.
Incorrect:
Not C. TheAdd-OBFileSpeccmdlet adds theOBFileSpecobject, which specifies the items to include or exclude from a backup, to the backup policy (OBPolicyobject). TheOBFileSpecobject can include or exclude multiple files, folders, or volumes.
Reference: Start-OBRegistration; Set OBMachineSetting
http://technet.microsoft.com/en-us/library/hh770398.aspx http://technet.microsoft.com/en-us/library/hh770409.aspx

NEW QUESTION 50
You have a server named SCI that runs a Server Core Installation of Windows Server 2012 R2. Shadow copies are enabled on all volumes.
You need to delete a specific shadow copy. The solution must minimize server downtime. Which tool should you use?

A. Shadow

B. Diskshadow
C. Wbadmin
D. Diskpart

Answer: B

Explanation: DiskShadow.exe is a tool that exposes the functionality offered by the Volume Shadow Copy Service (VSS).
The diskshadow command delete shadows deletes shadow copies.

Parameter	Description
all	Deletes all shadow copies.
volume <Volume>	Deletes all shadow copies of the given volume.
oldest <Volume>	Deletes the oldest shadow copy of the given volume.
set <SetID>	Deletes the shadow copies in the Shadow Copy Set of the given ID. You can specify an alias alias exists in the current environment.
id <ShadowID>	Deletes a shadow copy of the given ID. You can specify an alias by using the % symbol if th environment.
exposed {<Drive> | <MountPoint>}	Deletes the shadow copy exposed at the specified drive letter or mount point. Specify mou by the drive letter such as p:.

Reference: Technet, Diskshadow

NEW QUESTION 52
Your network contains an Active Directory forest named contoso.com.
Users frequently access the website of an external partner company. The URL of the website is http://partners.adatum.com.
The partner company informs you that it will perform maintenance on its Web server and that the IP addresses of the Web server will change.
After the change is complete, the users on your internal network report that they fail to access the website. However, some users who work from home report that they can access the website.
You need to ensure that your DNS servers can resolve partners.adatum.com to the correct IP address immediately.
What should you do?

A. Run dnscmd and specify the CacheLockingPercent parameter.
B. Run Set-DnsServerGlobalQueryBlockList.
C. Run ipconfig and specify the Renew parameter.
D. Run Set-DnsServerCache.

Answer: D

Explanation: The Set-DnsServerCache cmdlet modifies cache settings for a Domain Name System (DNS) server.
Run Set-DnsServerCache with the -LockingPercent switch.
/ -LockingPercent<UInt32>
Specifies a percentage of the original Time to Live (TTL) value that caching can consume. Cache locking is configured as a percent value. For example, if the cache locking value is set to 50, the DNS server does not overwrite a cached entry for half of the duration of the TTL. By default, the cache locking percent value is 100. This value means that the DNS server will not overwrite cached entries for the entire duration of the TTL.
Note. A better way would be clear the DNS cache on the DNS server with either Dnscmd
/ClearCache (from command prompt), or Clear-DnsServerCache (from Windows PowerShell).
Reference: Set-DnsServerCache http://technet.microsoft.com/en-us/library/jj649852.aspx
Incorrect:
Not A. You need to use the /config parameter as well:
You can change this value if you like by using the dnscmd command: dnscmd /Config /CacheLockingPercent<percent>

NEW QUESTION 55
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1 that has the Active Directory Federation Services server role installed. All servers run Windows Server 2012.
You complete the Active Directory Federation Services Configuration Wizard on Server1. You need to ensure that client devices on the internal network can use Workplace Join. Which two actions should you perform on Server1? (Each correct answer presents part of the solution. Choose two.)

A. Run Enable-AdfsDeviceRegistration -PrepareActiveDirectory.
B. Edit the multi-factor authentication global authentication policy settings.
C. Run Enable-AdfsDeviceRegistration.
D. Run Set-AdfsProxyProperties HttpPort 80.
E. Edit the primary authentication global authentication policy settings.

Answer: CE

Explanation: C. To enable Device Registration Service
On your federation server, open a Windows PowerShell command window and type: Enable-AdfsDeviceRegistration

Repeat this step on each federation farm node in your AD FS farm.
E. Enable seamless second factor authentication
Seamless second factor authentication is an enhancement in AD FS that provides an added level of access protection to corporate resources and applications from external devices that are trying to access them. When a personal device is Workplace Joined, it becomes a 'known' device and administrators can use this information to drive conditional access and gate access to resources.
To enable seamless second factor authentication, persistent single sign-on (SSO) and conditional access for Workplace Joined devices.
In the AD FS Management console, navigate to Authentication Policies. Select Edit Global Primary Authentication. Select the check box next to Enable Device Authentication, and then click OK.
Reference: Configure a federation server with Device Registration Service.

NEW QUESTION 59
Your network contains two Web servers named Server1 and Server2. Both servers run Windows Server 2012 R2.
Server1 and Server2 are nodes in a Network Load Balancing (NLB) cluster. The NLB cluster contains an application named App1 that is accessed by using the URLhttp://app1.contoso.com.
You plan to perform maintenance on Server1.
You need to ensure that all new connections to App1 are directed to Server2. The solution must not disconnect the existing connections to Server1.
What should you run?

A. The Set-NlbCluster cmdlet
B. The Set-NlbClusterNode cmdlet
C. The Stop-NlbCluster cmdlet
D. The Stop-NlbClusterNode cmdlet

Answer: D

Explanation: The Stop-NlbClusterNode cmdlet stops a node in an NLB cluster. When you use the stop the nodes in the cluster, client connections that are already in progress are interrupted. To avoid interrupting active connections, consider using the -drain parameter, which allows the node to continue servicing active connections but disables all new traffic to that node.
-Drain <SwitchParameter>
Drains existing traffic before stopping the cluster node. If this parameter is omitted, existing traffic will be dropped.
Reference: Stop-NlbClusterNode

NEW QUESTION 62
Your network contains an Active Directory domain named contoso.com.
A previous administrator implemented a Proof of Concept installation of Active Directory Rights Management Services (AD RMS).
After the proof of concept was complete, the Active Directory Rights Management Services server role was removed.
You attempt to deploy AD RMS.
During the configuration of AD RMS, you receive an error message indicating that an existing AD RMS Service Connection Point (SCP) was found.
You need to remove the existing AD RMS SCP. Which tool should you use?

A. Active Directory Users and Computers
B. Authorization Manager
C. Active Directory Domains and Trusts
D. Active Directory Sites and Services
E. Active Directory Rights Management Services

Answer: E

Explanation: ADRMS will registered the Service Connection Point (SCP) in Active Directory and you will need to unregister first before you remove the ADRMS server role.
If your ADRMS server is still alive, you can easily manually remove the SCP by below:
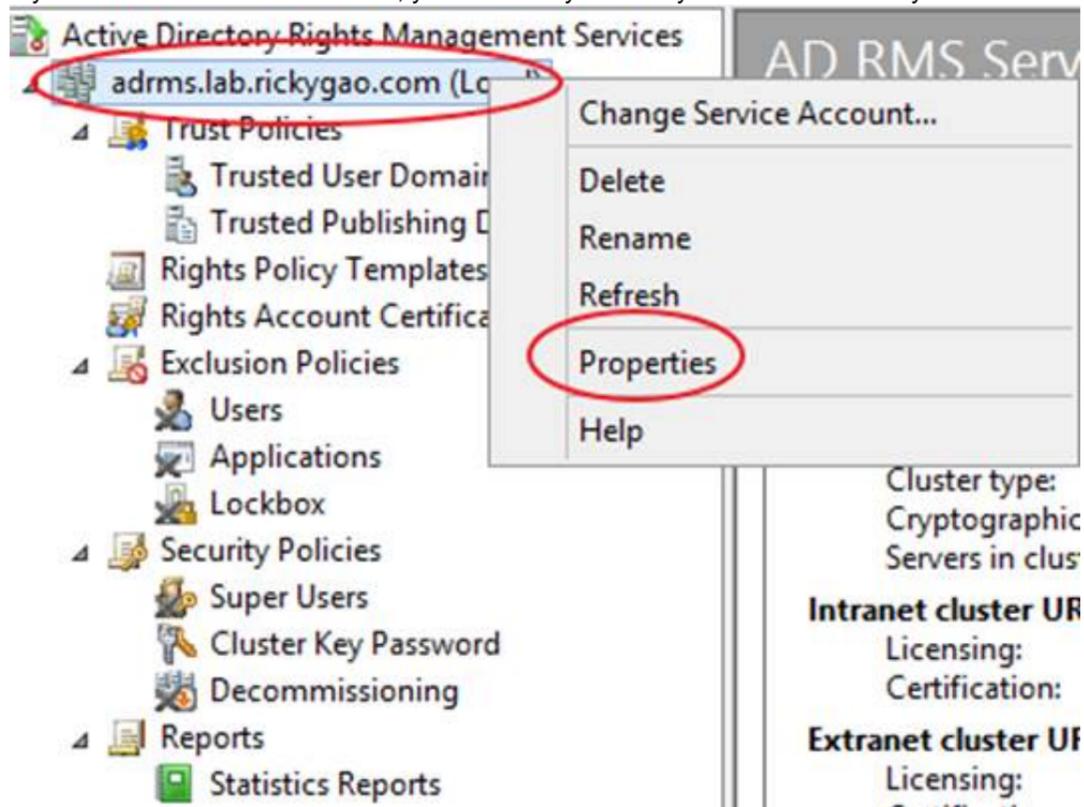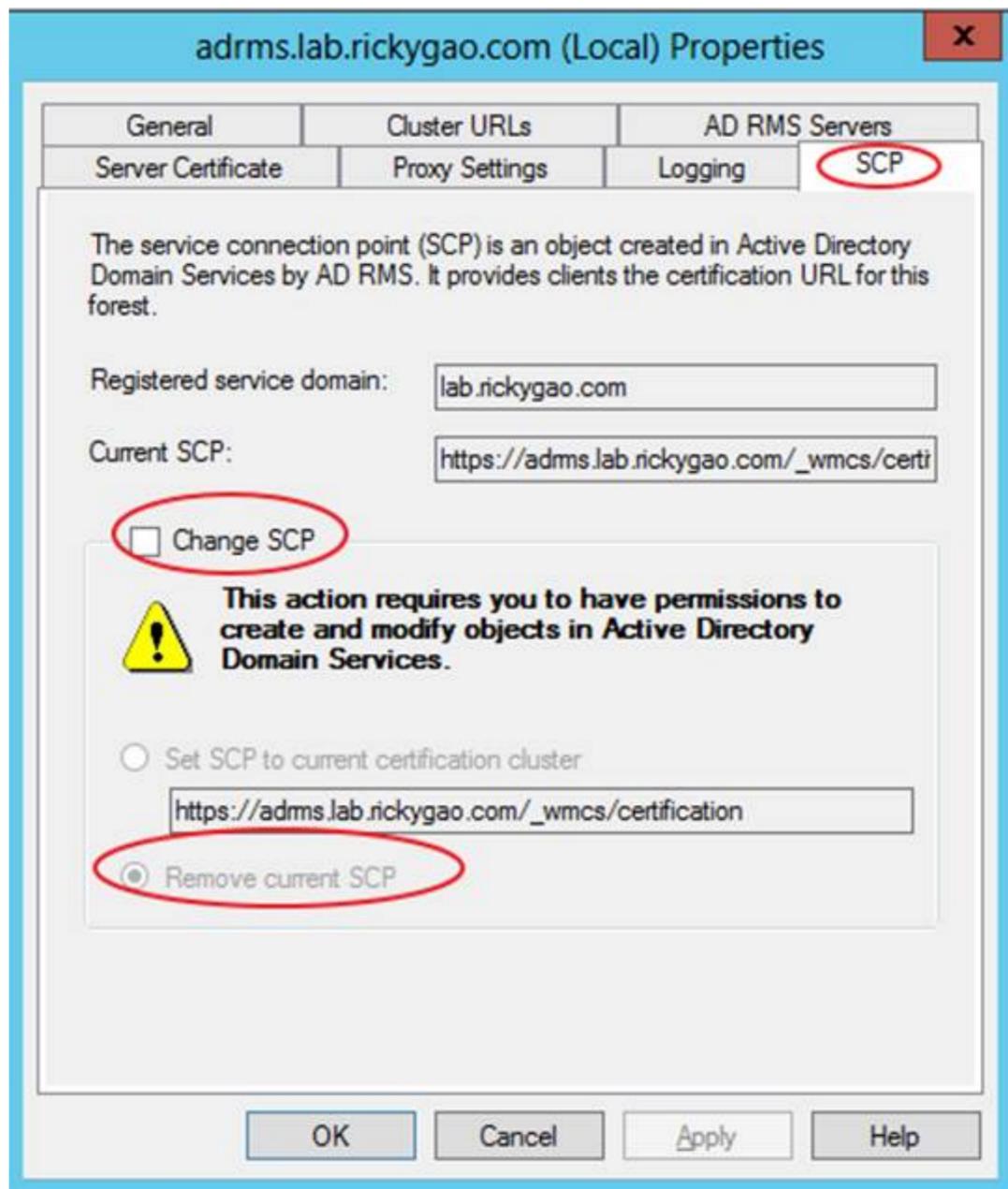
http://www.rickygao.com/wp-content/uploads/2013/08/080513_1308_Howtomanual2.png Reference: How to manually remove or reinstall ADRMS

NEW QUESTION 66
HOTSPOT
Your company has a main office and a branch office. An Active Directory site exists for each office.
The network contains an Active Directory forest named contoso.com. The contoso.com domain contains three member servers named Server1, Server2, and Server3. All servers run Windows Server 2012 R2.
In the main office, you configure Server1 as a file server that uses BranchCache.
In the branch office, you configure Server2 and Server3 as BranchCache hosted cache servers.
You are creating a Group Policy for the branch office site. Which two Group Policy settings should you configure?
To answer, select the appropriate two settings in the answer area.
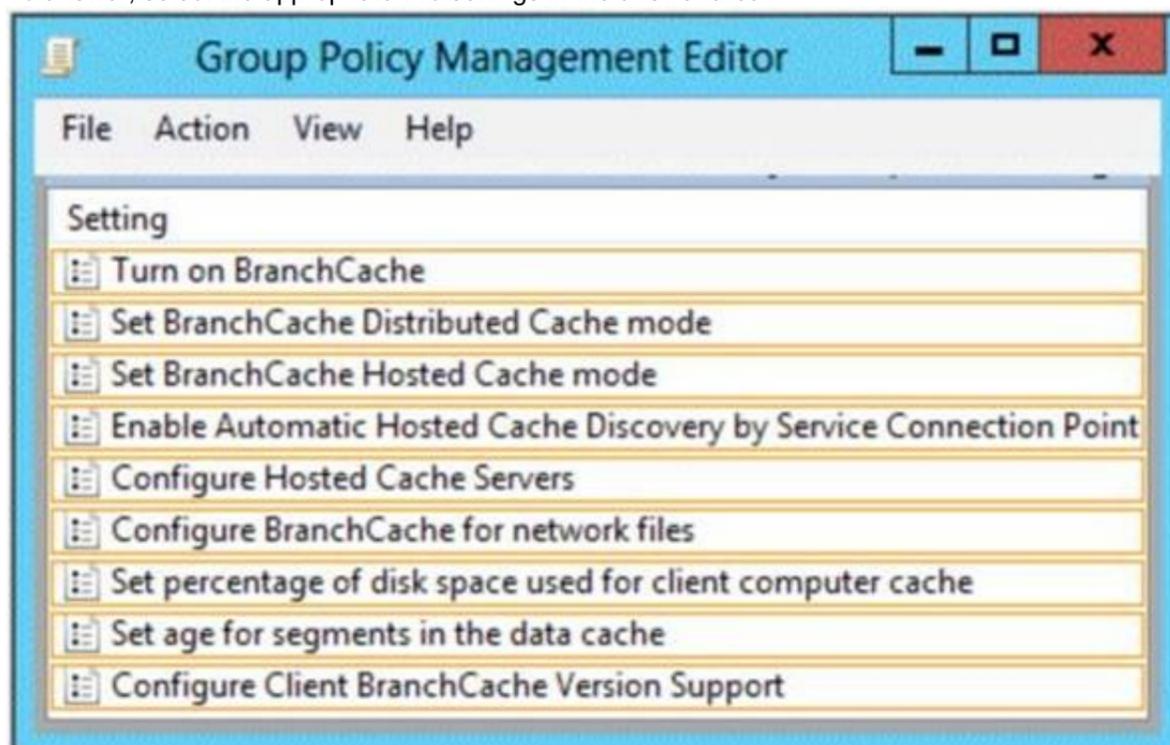
Answer:

Explanation: To use Group Policy to configure clients for hosted cache mode
Step x: In the Turn on BranchCache dialog box, click Enabled, and then click OK.
Step x+1: In the Group Policy Management Editor console, ensure that BranchCache is still selected, and then in the details pane double-click Set BranchCache

Hosted Cache mode. The Set BranchCache Hosted Cache mode dialog box opens.

NEW QUESTION 68
Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.
Server1 and Server2 have the Failover Clustering feature installed. The servers are configured as nodes in a failover cluster named Cluster1. Cluster1 contains a Clustered Shared Volume (CSV).
A developer creates an application named App1. App1 is NOT a cluster-aware application. App1 stores data in the file system.
You need to ensure that App1 runs in Cluster1. The solution must minimize development effort.
Which cmdlet should you run?

A. Add-ClusterServerRole
B. Add-ClusterGenericServiceRole
C. Add ClusterScaleOutFileServerRole
D. Add ClusterGenericApplicationRole

Answer: D

Explanation: Add-ClusterGenericApplicationRole
Configure high availability for an application that was not originally designed to run in a failover cluster.
If you run an application as a Generic Application, the cluster software will start the application, then periodically query the operating system to see whether the application appears to be running. If so, it is presumed to be online, and will not be restarted or failed over.
EXAMPLE 1.
Command Prompt: C:\PS>
Add-ClusterGenericApplicationRole -CommandLine NewApplication.exe Name OwnerNode State
---- --------- -----
cluster1GenApp node2 Online Description

This command configures NewApplication.exe as a generic clustered application. A default name will be used for client access and this application requires no storage.
Reference: Add-ClusterGenericApplicationRole http://technet.microsoft.com/en-us/library/ee460976.aspx

NEW QUESTION 73
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.
The domain contains a domain controller named DC1 that is configured as an enterprise root certification authority (CA).
All users in the domain are issued a smart card and are required to log on to their domain- joined client computer by using their smart card.
A user named User1 resigned and started to work for a competing company.
You need to prevent User1 immediately from logging on to any computer in the domain. The solution must not prevent other users from logging on to the domain.
Which tool should you use?

A. Active Directory Administrative Center
B. Certificate Templates
C. The Security Configuration Wizard
D. The Certificates snap-in

Answer: A

Explanation: To disable or enable a user account using Active Directory Administrative Center
1. To open Active Directory Administrative Center, clickStart, clickAdministrative Tools, and then clickActive Directory Administrative Center.
To open Active Directory Users and Computers in Windows Server 2012, clickStart, typedsac.exe.
2. In the navigation pane, select the node that contains the user account whose status you want to change.
3. In the management list, right-click the user whose status you want to change.
4. Depending on the status of the user account, do one of the following:
uk.co.certification.simulator.questionpool.PList@d5b8510
Reference: Disable or Enable a User Account

NEW QUESTION 76
You have a datacenter that contains six servers. Each server has the Hyper-V server role installed and runs Windows Server 2012 R2. The servers are configured as shown in the following table.

Host name	Processor manufacturer	Storage type
Host1	Intel	Local disk
Host2	AMD	iSCSI disk
Host3	Intel	iSCSI disk
Host4	Intel	Cluster Shared Volume (CSV)
Host5	Intel	Cluster Shared Volume (CSV)
Host6	AMD	iSCSI disk

Host4 and Host5 are part of a cluster named Cluster1. Cluster1 hosts a virtual machine named VM1.
You need to move VM1 to another Hyper-V host. The solution must minimize the downtime of VM1.
To which server and by which method should you move VM1?

A. To Host3 by using a storage migration

B. To Host6 by using a storage migration
C. To Host2 by using a live migration
D. To Host1 by using a quick migration

Answer: A

Explanation: With Hyper-V live migration, you can move running VMs from one Hyper-V physical host to another without any disruption of service or perceived downtime.
Host3 has an Intel processer, as does Host4 and Host5 in Cluster1, so the migration will work fine.
Incorrect:
Not B, not C. The migration of a virtual machine between physical computers is only supported on computers that have the same processor steppings or are from the same vendor. Therefore you cannot move a virtual machine from a Hyper-V host on an Intel- based server to a Hyper-V Host on an AMD-based server.
Not D. Quick Migration saves, moves and restores VMs, which results in some downtime. Reference: Hyper-V Migration Guide
http://technet.microsoft.com/en-us/library/ee849855(v=WS.10).aspx
Reference: Virtual Machine Storage Migration Overview http://technet.microsoft.com/en-us/library/hh831656.aspx
Reference: Windows Server 2008 R2 & Microsoft Hyper-V Server 2008 R2 - Hyper-V Live Migration Overview & Architecture (http://www.microsoft.com/en-us/download/details.aspx?id=12601)

NEW QUESTION 81
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. The functional level of the forest is Windows Server 2003.
You have a domain outside the forest named adatum.com.
You need to configure an access solution to meet the following requirements:
* Users in adatum.com must be able to access resources in contoso.com.
* Users in adatum.com must be prevented from accessing resources in fabrikam.com.
* Users in both contoso.com and fabrikam.com must be prevented from accessing resources in adatum.com.
What should you create?

A. a one-way realm trust from contoso.com to adatum.com
B. a one-way realm trust from adatum.com to contoso.com
C. a one-way external trust from contoso.com to adatum.com
D. a one-way external trust from adatum.com to contoso.com

Answer: C

Explanation: The contoso domain must trust the adatum domain.
Note: In a One-way: incoming trust, users in your (trusted) domain can be authenticated in the other (trusting) domain. Users in the other domain cannot be authenticated in your domain.
Incorrect:
Not A, not B. Use realm trusts to form a trust relationship between a non-Windows Kerberos realm and a Windows Server domain.
Not D. The resources that are to be shared are in the contoso domain. Reference: Trust types

NEW QUESTION 84
Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.
Server1 and Server2 have the Failover Clustering feature installed. The servers are configured as nodes in a failover cluster named Cluster1.
Cluster1 hosts an Application named App1.
You need to ensure that Server2 handles all of the client requests to the cluster for App1. The solution must ensure that if Server2 fails, Server1 becomes the active node for App1.
What should you configure?

A. Affinity-None
B. Affinity-Single
C. The cluster quorum settings
D. The failover settings
E. A file server for general use
F. The Handling priority
G. The host priority
H. Live migration
I. The possible owner
J. The preferred owner
K. Quick migration
L. the Scale-Out File Server

Answer: J

Explanation: The preferred owner in a two-server cluster will always be the active node unless it is down.
Reference: Preferred Owners in a Cluster http://blogs.msdn.com/b/clustering/archive/2008/10/14/9000092.aspx

NEW QUESTION 85
You have a server named Server1 that runs Windows Server 2012 R2. Server1 is located in the perimeter network and has the DNS Server server role installed.
Server1 has a zone named contoso.com. You App1y a security template to Server1.
After you App1y the template, users report that they can no longer resolve names from contoso.com.
On Server1, you open DNS Manager as shown in the DNS exhibit. (Click the Exhibit button.)

On Server1, you open Windows Firewall with Advanced Security as shown in the Firewall exhibit. (Click the Exhibit button.)
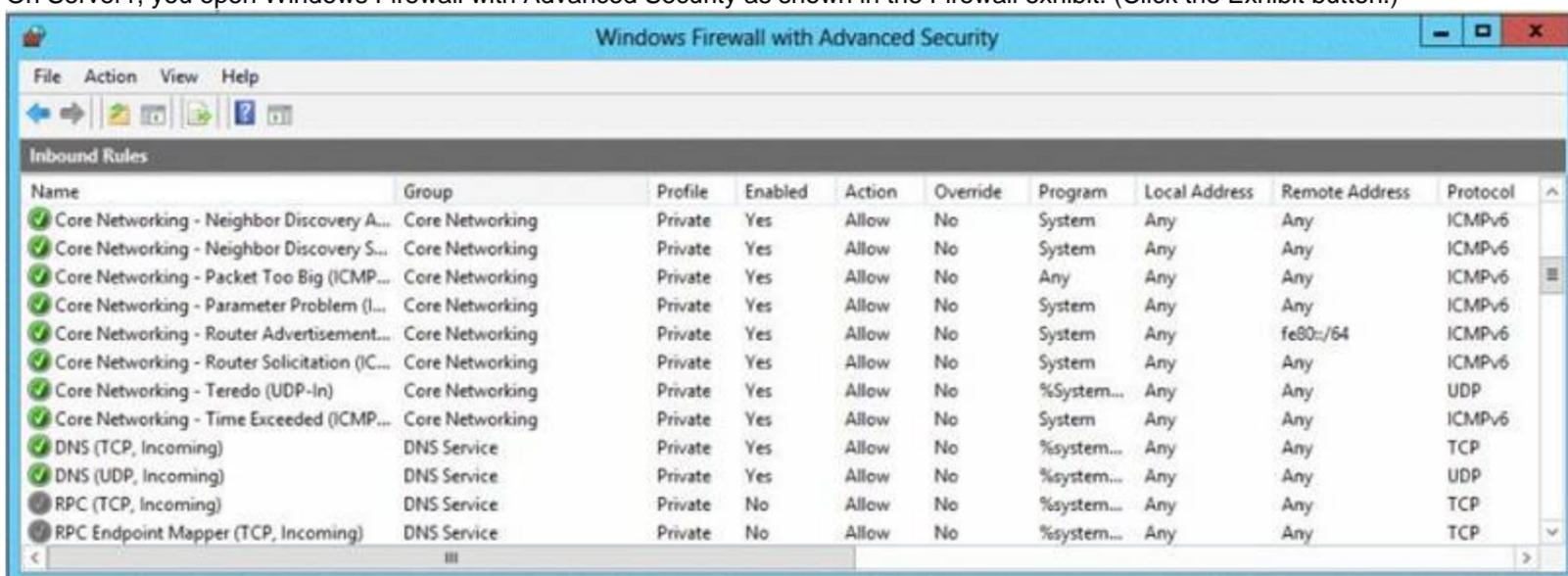
You need to ensure that users can resolve contoso.com names. What should you do?

A. From Windows Firewall with Advanced Security, disable the DNS (TCP, Incoming) rule and the DNS (UDP, Incoming) rule.
B. From DNS Manager, modify the Zone Transfers settings of the contoso.com zone.
C. From DNS Manager, unsign the contoso.com zone.
D. From DNS Manager, modify the Start of Authority (SOA) of the contoso.com zone.
E. From Windows Firewall with Advanced Security, modify the profiles of the DNS (TCP, Incoming) rule and the DNS (UDP, Incoming) rule.

Answer: E

Explanation: To configure Windows Firewall on a managed DNS server
? On the Server Manager menu, clickToolsand then clickWindows Firewall with Advanced Security.
? Right-clickInbound Rules, and then clickNew Rule. TheNew Inbound Rule Wizardwill launch.
? InRule Type, selectPredefined, chooseDNS Servicefrom the list, and then clickNext.
? InPredefined Rules, underRules, select the checkboxes next to the following rules:
? ClickNext, chooseAllow the connection, and then clickFinish.
? Right-clickInbound Rules, and then clickNew Rule. TheNew Inbound Rule Wizardwill launch.
etc.
Reference: Manually Configure DNS Access Settings

NEW QUESTION 87
Your network contains two servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 and Server2 are configured as shown in the following table.

Server name	Installed component
Server1	iSCSI Target Server
Server2	iSNS server service

You need to ensure that when new targets are added to Server1, the targets are registered on Server2 automatically.
What should you do on Server1?

A. Configure the Discovery settings of the iSCSI initiator.
B. Configure the security settings of the iSCSI target.
C. Run the Set-WmiInstance cmdlet.
D. Run the Set-IscsiServerTarget cmdlet.

Answer: C

Explanation: Explanation/Reference:
Manage iSNS server registration
The iSNS server registration can be done using the following cmdlets, which manages the WMI objects.
To add an iSNS server:
Set-WmiInstance -Namespace root\wmi -Class WT_iSNSServer –Arguments
@{ServerName="ISNSservername"}
Note: The Set-WmiInstance cmdlet creates or updates an instance of an existing WMI class. The created or updated instance is written to the WMI repository.
Reference: iSCSI Target cmdlet reference http://blogs.technet.com/b/filecab/archive/2012/06/08/iscsi-target-cmdlet-reference.aspx

NEW QUESTION 90
You deploy an Active Directory Federation Services (AD FS) 2.1 infrastructure. The infrastructure uses Active Directory as the attribute store.
Some users report that they fail to authenticate to the AD FS infrastructure.
You discover that only users who run third-party web browsers experience issues. You need to ensure that all of the users can authenticate to the AD FS infrastructure
successfully.
Which Windows PowerShell command should you run?

A. Set-ADFSProperties -ProxyTrustTokenLifetime 1:00:00
B. Set-ADFSProperties -AddProxyAuthenticationRules None
C. Set-ADFSProperties -SSOLifetime 1:00:00
D. Set-ADFSProperties -ExtendedProtectionTokenCheck None

Answer: D

Explanation:
Certain client browser software, such as Firefox, Chrome, and Safari, do not support the Extended Protection for Authentication capabilities that can be used across the Windows platform to protect against man-in-the-middle attacks. To prevent this type of attack from occurring over secure AD FS communications, AD FS 2.0 enforces (by default) that all communications use a channel binding token (CBT) to mitigate against this threat.
Note: Disable the extended Protection for authentication
To disable the Extended Protection for Authentication feature in AD FS 2.0
? On a federation server, login using the Administrator account, open the Windows PowerShell command prompt, and then type the following command:
Set-ADFSProperties –ExtendedProtectionTokenCheck None
? Repeat this step on each federation server in the farm.
Reference: Configuring Advanced Options for AD FS 2.0

NEW QUESTION 92
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. The forest contains three Active Directory sites named SiteA, SiteB, and SiteC. The sites contain four domain controllers. The domain controllers are configured as shown in the following table.

Site name	Domain controller name
SiteA	DC1, DC2
SiteB	DC3, DC4
SiteC	None

An IP site link exits between each site.
You discover that the users in SiteC are authenticated by the domain controllers in SiteA and SiteB.
You need to ensure that the SiteC users are authenticated by the domain controllers in SiteB, unless all of the domain controllers in SiteB are unavailable.
What should you do?

A. Create an SMTP site link between SiteB and SiteC.
B. Create additional connection objects for DC3 and DC4.
C. Decrease the cost of the site link between SiteB and SiteC.
D. Create additional connection objects for DC1 and DC2.

Answer: C

Explanation: By decreasing the site link cost between SiteB and SiteC the SiteC users would be authenticated by SiteB rather than by SiteA.

NEW QUESTION 93
HOTSPOT
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
The network has the physical sites and TCP/IP subnets configured as shown in the following table.

Site name	Network subnet
Site1	192.168.1.0/24
Site2	192.168.2.0/24
Site3	192.168.3.0/24

You have a web application named App1 that is hosted on six separate Web servers. DNS has the host names and IP addresses registered as shown in the following table.

Host name	Network address
App1.contoso.com	192.168.1.70
App1.contoso.com	192.168.1.71
App1.contoso.com	192.168.2.140
App1.contoso.com	192.168.2.141
App1.contoso.com	192.168.3.210
App1.contoso.com	192.168.3.211

You discover that when users connect to appl.contoso.com, they are connected frequently to a server that is not on their local subnet.
You need to ensure that when the users connect to appl.contoso.com, they connect to a server on their local subnet. The connections must be distributed across the servers that host appl.contoso.com on their subnet.
Which two settings should you configure?
To answer, select the appropriate two settings in the answer area.

DC1 Properties

? X

Debug Logging	Event Logging	Monitoring	Security
Interfaces	Forwarders	Advanced	Root Hints

Server version number:

6.3 9431 (0x24d7)

Server options:

☐ Disable recursion (also disables forwarders)
☐ Enable BIND secondaries
☐ Fail on load if bad zone data
☐ Enable round robin
☐ Enable netmask ordering
☐ Secure cache against pollution
☐ Enable DNSSEC validation for remote responses

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 7 days

Reset to Default

OK   Cancel   Apply   Help

Answer:

Explanation: DNS Round Robin is a mechanism for choosing an IP address from the list returned by a DNS server so that all clients won't get the same IP address every time. Netmask ordering is a mechanism for further optimizing which IP address is used by attempting to determine the closest result.

NEW QUESTION 98
Your network contains an Active Directory forest. The forest contains one domain named adatum.com. The domain contains three domain controllers. The domain controllers are
configured as shown in the following table.

Domain controller name	Operating system
DC1	Windows Server 2003
DC2	Windows Server 2008 R2
DC3	Windows Server 2008 R2
DC4	Windows Server 2012 R2

DC2 has all of the domain-wide operations master roles. DC3 has all of the forest-wide operation master roles.
You need to ensure that you can use Password Settings objects (PSOs) in the domain. What should you do first?

A. Uninstall Active Directory from DC1.
B. Change the domain functional level.

C. Transfer the domain-wide operations master roles.
D. Transfer the forest-wide operations master roles.

Answer: A

Explanation: In Windows Server 2008 and later, you can use fine-grained password policies to specify multiple password policies and apply different password restrictions and account lockout policies to different sets of users within a single domain.
Note: In Microsoft Windows 2000 and Windows Server 2003 Active Directory domains, you could apply only one password and account lockout policy, which is specified in the domain's Default Domain Policy, to all users in the domain. As a result, if you wanted different password and account lockout settings for different sets of users, you had to either create a password filter or deploy multiple domains. Both options were costly for different reasons.
Reference: AD DS Fine-Grained Password and Account Lockout Policy Step-by-Step Guide

NEW QUESTION 102
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server3 that runs Windows Server 2012 R2 and has the DHCP Server server role installed.
DHCP is configured as shown in the exhibit. (Click the Exhibit button.)
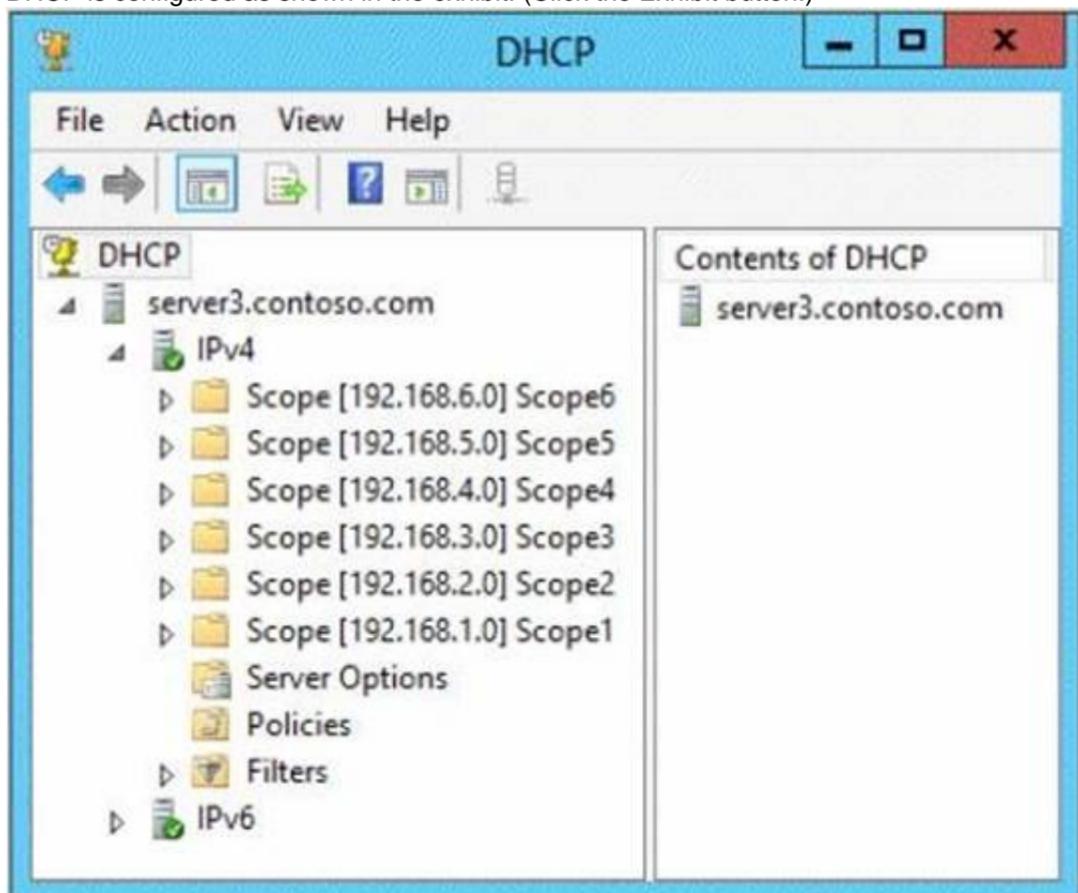
Scope1, Scope2, and Scope3 are configured to assign the IP addresses of two DNS servers to DHCP clients. The remaining scopes are NOT configured to assign IP addresses of DNS servers to DHCP clients.
You need to ensure that only Scope1, Scope3, and Scopes assign the IP addresses of the DNS servers to the DHCP clients. The solution must minimize administrative effort.
What should you do?

A. Create a superscope and a filter.
B. Create a superscope and scope-level policies.
C. Configure the Server Options.
D. Configure the Scope Options.

Answer: D

Explanation: Scope options are applied to any clients that obtain a lease within that particular scope. Active scope option types always apply to all computers obtaining a lease in a given scope unless they are overridden by class or reserved client settings for the option type.
Incorrect:
Not A, not B. A superscope allows a DHCP server to provide leases from more than one scope to clients on a single physical network. It is not applicable here.
Not C. If we configure the Server Options and set the DNS Servers then all DHCP clients would be assigned a DNS server.
Reference: Managing DHCP Options https://technet.microsoft.com/en-us/library/cc958929.aspx

NEW QUESTION 104
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2012 R2.
The domain contains four servers. The servers are configured as shown in the following table.

Server name	Configuration
DC1	• Domain controller
DC2	• Domain controller • DNS server • DHCP server
DC3	• Domain controller • DHCP server
Server1	• Windows Server Updates Services (WSUS) server

You need to deploy IP Address Management (IPAM) to manage DNS and DHCP. On which server should you install IPAM?

A. DC1
B. DC2
C. DC3
D. Server1

Answer: D

Explanation:
IPAM cannot be installed on Domain Controllers. All servers, except Server1, have the DC role
Reference: IP Address Management (IPAM) Overview http://technet.microsoft.com/en-us/library/hh831353.aspx

NEW QUESTION 107
HOTSPOT
Your network contains two Web servers named Server1 and Server2. Both servers run Windows Server 2012 R2.
Server1 and Server2 are nodes in a Network Load Balancing (NLB) cluster. The NLB cluster contains an application named App1 that is accessed by using the URL http://app1.contoso.com.
You deploy a new server named Server3 that runs Windows Server 2012 R2. The contoso.com DNS zone contains the records shown in the following table.

Record name	Record type	Address
App1	Host (A)	192.168.1.100
Server1	Host (A)	192.168.1.101
Server2	Host (A)	192.168.1.102
Server3	Host (A)	192.168.1.103

You need to add Server3 to the NLB cluster. What command should you run?
To answer, select the appropriate options in the answer area.

Answer Area

[▼] [▼] |

[▼] –NewNodeName Server3 –NewNodeInterface EtherNet

Answer Area

[▼] [▼] |
Get-NlbClusterNode   App1
Get-NlbClusterNodeDip   Server1
Get-NlbClusterVip   Server3

[▼] –NewNodeName Server3 –NewNodeInterface EtherNet
Add-NlbClusterNode
Add-NlbClusterNodeDip
Add-NlbClusterVip
Set-NlbClusterNodeDip

Answer:

Explanation: * The Add-NlbClusterNode cmdlet adds a new node to the NLB cluster. Once the new node settings are circulated through all of the NLB cluster node, the new cluster node will be in a running state in the cluster.
* The Get-NlbClusterNode cmdlet retrieves information about a node in the NLB cluster.
* EXAMPLE: This command adds host node2 to the cluster on node1. C:\PS>
Get-NlbCluster node1 | Add-NlbClusterNode -NewNodeName node2 -NewNodeInterface vlan-3
Name State Interface HostID
---- ----- --------- ------

node2 Converged vlan-3 2

NEW QUESTION 111
Your network contains two Active Directory forests named contoso.com and adatum.com. Each forest contains one domain. Contoso.com has a two-way forest trust to adatum.com. Selective authentication is enabled on the forest trust.
Contoso contains 10 servers that have the File Server role service installed. Users successfully access shared folders on the file servers by using permissions granted to the Authenticated Users group.
You migrate the file servers to adatum.com.
Contoso users report that after the migration, they are unable to access shared folders on the file servers.
You need to ensure that the Contoso users can access the shared folders on the file servers.
What should you do?

A. Disable selective authentication on the existing forest trust.
B. Disable SID filtering on the existing forest trust.
C. Run netdom and specify the /quarantine attribute.
D. Replace the existing forest trust with an external trust.

Answer: B

Explanation: Although it is not recommended, you can use this procedure to disable security identifier (SID) filter quarantining for an external trust with the Netdom.exe tool. You should consider disabling SID filter quarantining only in the following situations:
* Users have been migrated to the trusted domain with their SID histories preserved, and you want to grant those users access to resources in the trusting domain (the former domain of the migrated users) based on the sIDHistory attribute.
Etc.
Reference: Disabling SID filter quarantining http://technet.microsoft.com/en-us/library/cc794713(v=ws.10).aspx

NEW QUESTION 114
Your network contains three servers named Server1, Server2, and Server3. All servers run Windows Server 2012 R2.
You need to ensure that Server1 can provide iSCSI storage for Server2 and Server3. What should you do on Server1?

A. Start the Microsoft iSCSI Initiator Service and configure the iSCSI Initiator Properties.
B. Install the iSNS Server service feature and create a Discovery Domain.
C. Install the Multipath I/O (MPIO) feature and configure the MPIO Properties.
D. Install the iSCSI Target Server role service and configure iSCSI targets.

Answer: D

Explanation: iSCSI Target Server: The server runs the iSCSI Target. It is also the iSCSI Target role name in Windows Server 2012.
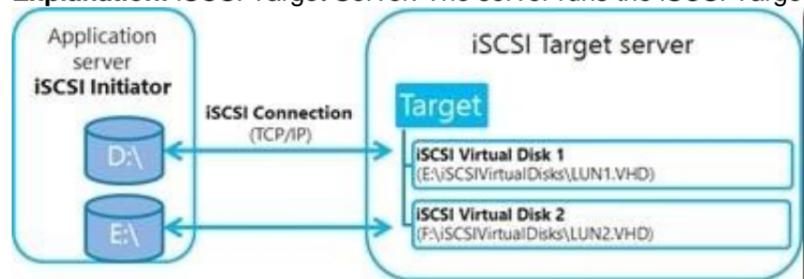
Note:
iSCSI: it is an industry standard protocol allow sharing block storage over the Ethernet. The server shares the storage is called iSCSI Target. The server (machine) consumes the storage is called iSCSI initiator. Typically, the iSCSI initiator is an application server. For example, iSCSI Target provides storage to a SQL server, the SQL server will be the iSCSI initiator in this deployment.
Target: It is an object which allows the iSCSI initiator to make a connection. The Target keeps track of the initiators which are allowed to be connected to it. The Target also keeps track of the iSCSI virtual disks which are associated with it. Once the initiator establishes the connection to the Target, all the iSCSI virtual disks associated with the Target will be accessible by the initiator.

NEW QUESTION 118
HOTSPOT
You have a file server named Server1 that runs Windows Server 2012 R2.
Server1 contains a file share that must be accessed by only a limited number of users.
You need to ensure that if an unauthorized user attempts to access the file share, a custom access-denied message appears, which contains a link to request access to the share. The message must not appear when the unauthorized user attempts to access other shares.
Which two nodes should you configure in File Server Resource Manager? To answer, select the appropriate two nodes in the answer area.
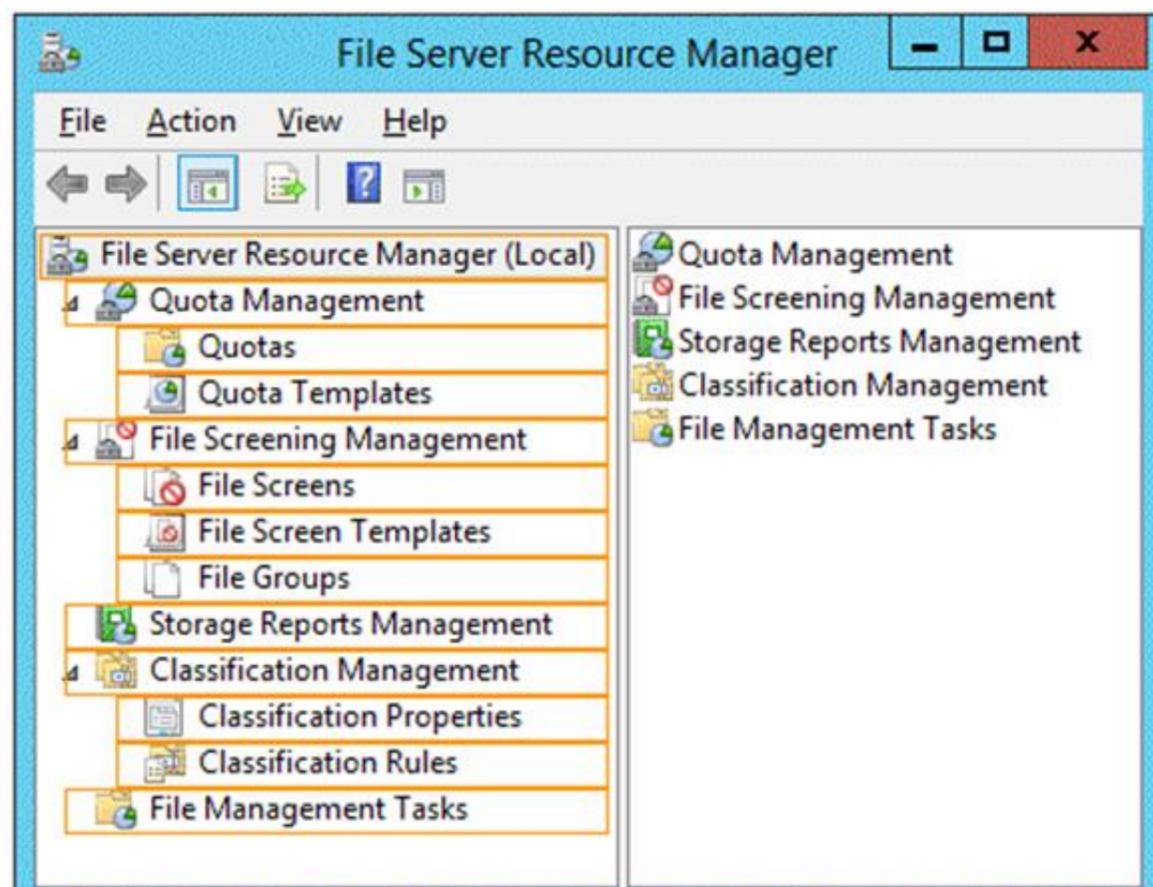
Answer:

Explanation: * Configure access-denied assistance
To configure access-denied assistance by using File Server Resource Manager
\1. Open File Server Resource Manager. In Server Manager, click Tools, and then click File Server Resource Manager.
\2. Right-click File Server Resource Manager (Local), and then click Configure Options. etc.
* To specify a separate access-denied message for a shared folder by using File Server Resource Manager
\1. Open File Server Resource Manager. In Server Manager, click Tools, and then click File Server Resource Manager.
\2. Expand File Server Resource Manager (Local), and then click Classification Management.
\3. Right-click Classification Properties, and then click Set Folder Management Properties. Etc

NEW QUESTION 119
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. The forest functional level is Windows Server 2012 R2.
You have a domain controller named DC1.
On DC1, you create a new Group Policy object (GPO) named GPO1. You need to verify that GPO1 was replicated to all of the domain controllers.
Which tool should you use?

A. Group Policy Management
B. Active Directory Sites and Services
C. DFS Management
D. Active Directory Administrative Center

Answer: A

Explanation: In Windows Server 2012, the Group Policy Management Console (GPMC) was enhanced to provide a report for the overall health state of the Group Policy infrastructure for a domain, or to scope the health view to a single GPO.
Reference: Check Group Policy Infrastructure Status http://technet.microsoft.com/en-us/library/jj134176.aspx

NEW QUESTION 122
Your company recently deployed a new Active Directory forest named contoso.com. The forest contains two Active Directory sites named Site1 and Site2. The first domain controller in the forest runs Windows Server 2012 R2.
You need to force the replication of the SYSVOL folder from Site1 to Site2. Which tool should you use?

A. Active Directory Sites and Services
B. DFS Management
C. Repadmin
D. Dfsrdiag

Answer: D

Explanation: In Windows Server 2012 R2, Windows Server 2008 R2, or Windows Server 2008, you can force replication immediately by using DFS Management, as described in Edit Replication Schedules. You can also force replication by using the Dfsrdiag SyncNow command. You can force polling by using the Dfsrdiag PollAD command.
Reference: DFS Replication: Frequently Asked Questions (FAQ) http://technet.microsoft.com/en-us/library/cc773238(v=ws.10).aspx#BKMK_072

NEW QUESTION 126

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 is a file server that has the Hyper-V server role installed.
Server1 hosts several virtual machines. The virtual machine configuration files are stored on drive D and the VHD files are stored on drive E.
You plan to replace drive E with a larger volume.
You need to ensure that the virtual machines on Server1 remain available while drive E is being replaced.
What should you do?

A. Perform a quick migration.
B. Add Server1 and Server2 as nodes in a failover cluster.
C. Perform a live migration.
D. Perform a storage migration.

Answer: D

Explanation: Hyper-V in Windows Server 2012 R2 introduces support for moving virtual machine storage without downtime by making it possible to move the storage while the virtual machine remains running.
Reference: Virtual Machine Storage Migration Overview http://technet.microsoft.com/en-us/library/hh831656.aspx

NEW QUESTION 127
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.
The domain contains a domain controller named DC1 that is configured as an enterprise root certification authority (CA).
All users in the domain are issued a smart card and are required to log on to their domain- joined client computer by using their smart card.
A user named User1 resigned and started to work for a competing company.
You need to prevent User1 immediately from logging on to any computer in the domain. The solution must not prevent other users from logging on to the domain.
Which tool should you use?

A. Active Directory Users and Computers
B. Server Manager
C. The Certificates snap-in
D. Active Directory Administrative Center

Answer: D

Explanation: To disable or enable a user account using Active Directory Administrative Center
\1. To open Active Directory Administrative Center, clickStart, clickAdministrative Tools, and then clickActive Directory Administrative Center.
To open Active Directory Users and Computers in Windows Server 2012, clickStart, typedsac.exe.
\2. In the navigation pane, select the node that contains the user account whose status you want to change.
\3. In the management list, right-click the user whose status you want to change.
\4. Depending on the status of the user account, do one of the following:
uk.co.certification.simulator.questionpool.PList@da803f0
Reference: Disable or Enable a User Account

NEW QUESTION 130
Your network contains four Active Directory forests. Each forest contains an Active Directory Rights Management Services (AD RMS) root cluster.
All of the users in all of the forests must be able to access protected content from any of the forests.
You need to identify the minimum number of AD RMS trusts required. How many trusts should you identify?

A. 3
B. 6
C. 12
D. 16

Answer: C

Explanation: The number of AD RMS trusts required to interact between all AD RMS forests can be defined by using the following formula: N*(N-1).
Here N=4, so the number of trust is 12 (4*3).
Reference: AD RMS Prerequisites, Important considerations for installing AD RMS in a multi-forest environment

NEW QUESTION 133
You have a server named Server1 that runs Windows Server 2012 R2.
Server1 has a single volume that is encrypted by using BitLocker Drive Encryption (BitLocker).
BitLocker is configured to save encryption keys to a Trusted Platform Module (TPM). Server1 is configured to perform a daily system image backup.
The motherboard on Server1 is upgraded.
After the upgrade, Windows Server 2012 R2 on Server1 fails to start. You need to start the operating system on Server1 as soon as possible. What should you do?

A. Start Server1 from the installation medi
B. Run startrec.exe.
C. Move the disk to a server that has a model of the old motherboar
D. Start the server from the installation medi
E. Run bcdboot.exe.
F. Move the disk to a server that has a model of the old motherboar
G. Start the serve
H. Run tpm.msc.
I. Start Server1 from the installation medi
J. Perform a system image recovery.

Answer: C

Explanation: By moving the hard drive to server with that has a model of the old motherboard the system would be able to start. As BitLocker was configured to save encryption keys to a Trusted Platform Module (TPM), we can use tpm.msc to access the TPM settings.
Note: After you replaced the motherboard, you need to repopulate the TPM with new information regarding the encryption of the hard disk.
We use these commands to repopulate the information in the TPM (without PIN): manage-bde –delete -protectors C: -type TPM
manage-bde –protectors –add C: -tpm
Incorrect:
Not D. After the system image recovery you would still have the new motherboard installed. The problem would return.
Reference: BitLocker - New motherboard replacement

NEW QUESTION 137
Your network contains an Active Directory domain named contoso.com. The domain contains servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 has the Active Directory Federation Services server role installed. Server2 is a file server.
Your company introduces a Bring Your Own Device (BYOD) policy.
You need to ensure that users can use a personal device to access domain resources by using Single Sign-On (SSO) while they are connected to the internal network.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Enable the Device Registration Service in Active Directory.
B. Publish the Device Registration Service by using a Web Application Proxy.
C. Configure Active Directory Federation Services (AD FS) for the Device Registration Service.
D. Create and configure a sync share on Server2.
E. Install the Work Folders role service on Server2.

Answer: AC

Explanation: * Workplace Join leverages a feature included in the Active Directory Federation Services (AD FS) Role in Windows Server 2012 R2, called Device Registration Service (DRS). DRS provisions a device object in Active Directory when a device is Workplace Joined. Once the device object is in Active Directory, attributes of that object can be retrieved and used to provide conditional access to resources and applications. The device identity is
represented by a certificate which is set on the personal device by DRS when the device is Workplace Joined.
* In Windows Server 2012 R2, AD FS and Active Directory Domain Services have been extended to comprehend the most popular mobile devices and provide conditional access to enterprise resourcesbased on user+device combinations and access policies. With these policies in place, you can control access based on users, devices, locations, and access times.
Reference: BYOD Basics: Enabling the use of Consumer Devices using Active Directory in Windows Server 2012 R2

NEW QUESTION 141
DRAG DROP
Your network contains an Active Directory domain named contoso.com. The domain contains four member servers named Server1, Server2, Server3, and Server4. All servers run Windows Server 2012 R2.
Server1 and Server3 are located in a site named Site1. Server2 and Server4 are located in a site named Site2. The servers are configured as nodes in a failover cluster named Cluster1.
Dynamic quorum management is disabled.
Cluster1 is configured to use the Node Majority quorum configuration.
You need to ensure that users in Site2 can access Cluster1 if the network connection between the two sites becomes unavailable.
What should you run from Windows PowerShell?
To answer, drag the appropriate commands to the correct location. Each command may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer:

Explanation: NodeWeight settings are used during quorum voting to support disaster recovery and multi- subnet scenarios for AlwaysOn Availability Groups and SQL Server Failover Cluster Instances.
Example (Powershell)
The following example changes the NodeWeight setting to remove the quorum vote for the "AlwaysOnSrv1" node.
Import-Module FailoverClusters
$node = "AlwaysOnSrv1"
(Get-ClusterNode $node).NodeWeight = 0

NEW QUESTION 143
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the DHCP Server server role installed. Server1 has an IPv6 scope named Scope1.

You implement an additional DHCP server named Server2 that runs Windows Server 2012 R2.
You need to provide high availability for Scope1. The solution must minimize administrative effort.
What should you do?

A. Install and configure Network Load Balancing (NLB) on Server1 and Server2.
B. Create a scope on Server2.
C. Configure DHCP failover on Server1.
D. Install and configure Failover Clustering on Server1 and Server2.

Answer: C

Explanation: Overview: Configure DHCP failover using the DHCP console
To configure DHCP failover using the DHCP console, right-click a DHCP scope or right- click IPv4 and then click Configure Failover.
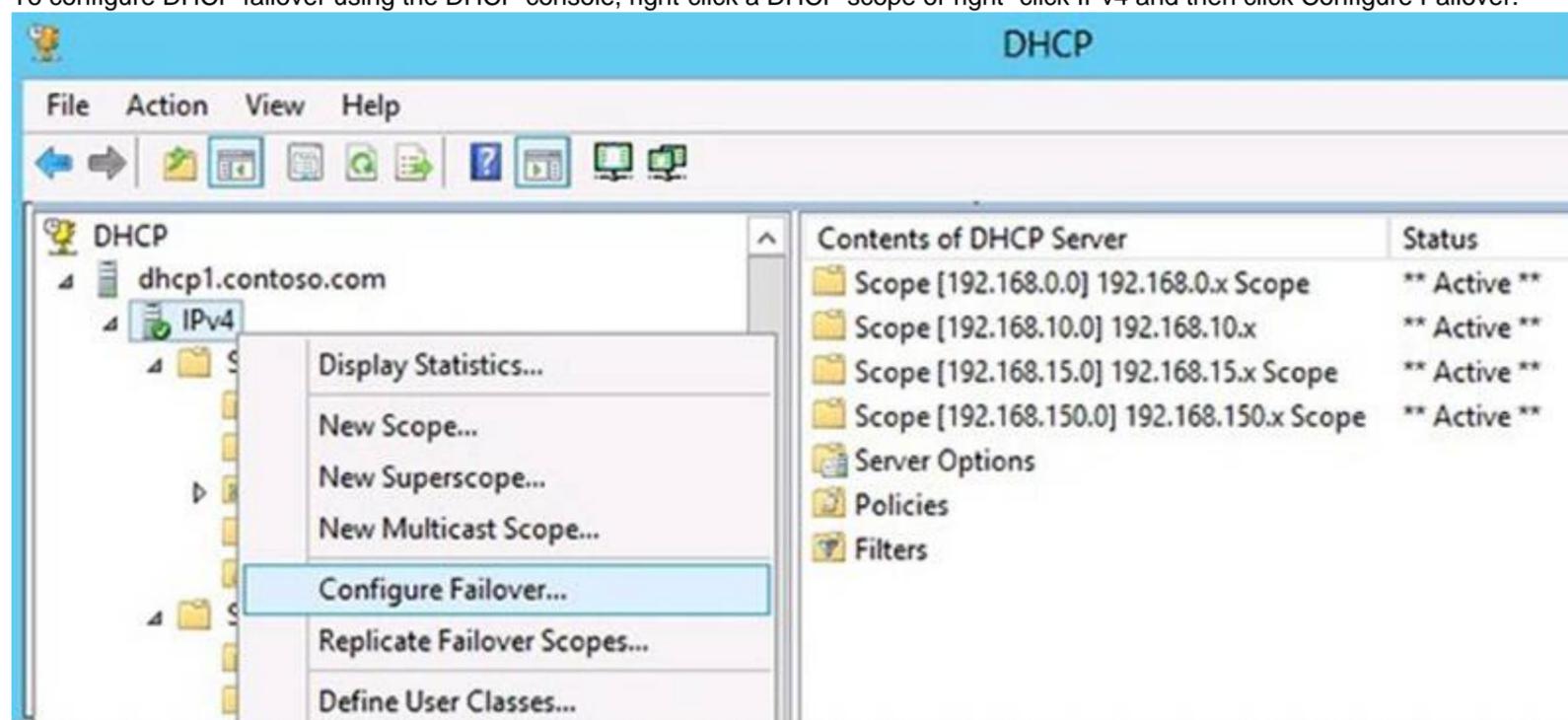
Configure Failover
TheConfigure Failoverwizard guides you through configuring DHCP failover on the selected scope.
Note: The DHCP server failover feature, available in Windows Server 2012 and later, provides the ability to have two DHCP servers provide IP addresses and option configuration to the same subnet or scope, providing for continuous availability of DHCP service to clients.
Incorrect:
Not A. NLB is not related to DHCP scope availability. Not B. DHCP failover requirements include:
DHCP Scopes requirement:
At least one IPv4 DHCP scope must be configured on the primary DHCP server.
The same DHCP scope ID, or an overlapping scope, must not be configured on the failover partner.
Not D. Failover clustering is possibly, but would not minimize administration. Reference: Deploy DHCP Failover

NEW QUESTION 146
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.
DC1 has the DNS Server server role installed.
The network contains client computers that run either Linux, Windows 7, or Windows 8. You have a zone named adatum.com as shown in the exhibit. (Click the Exhibit button.)
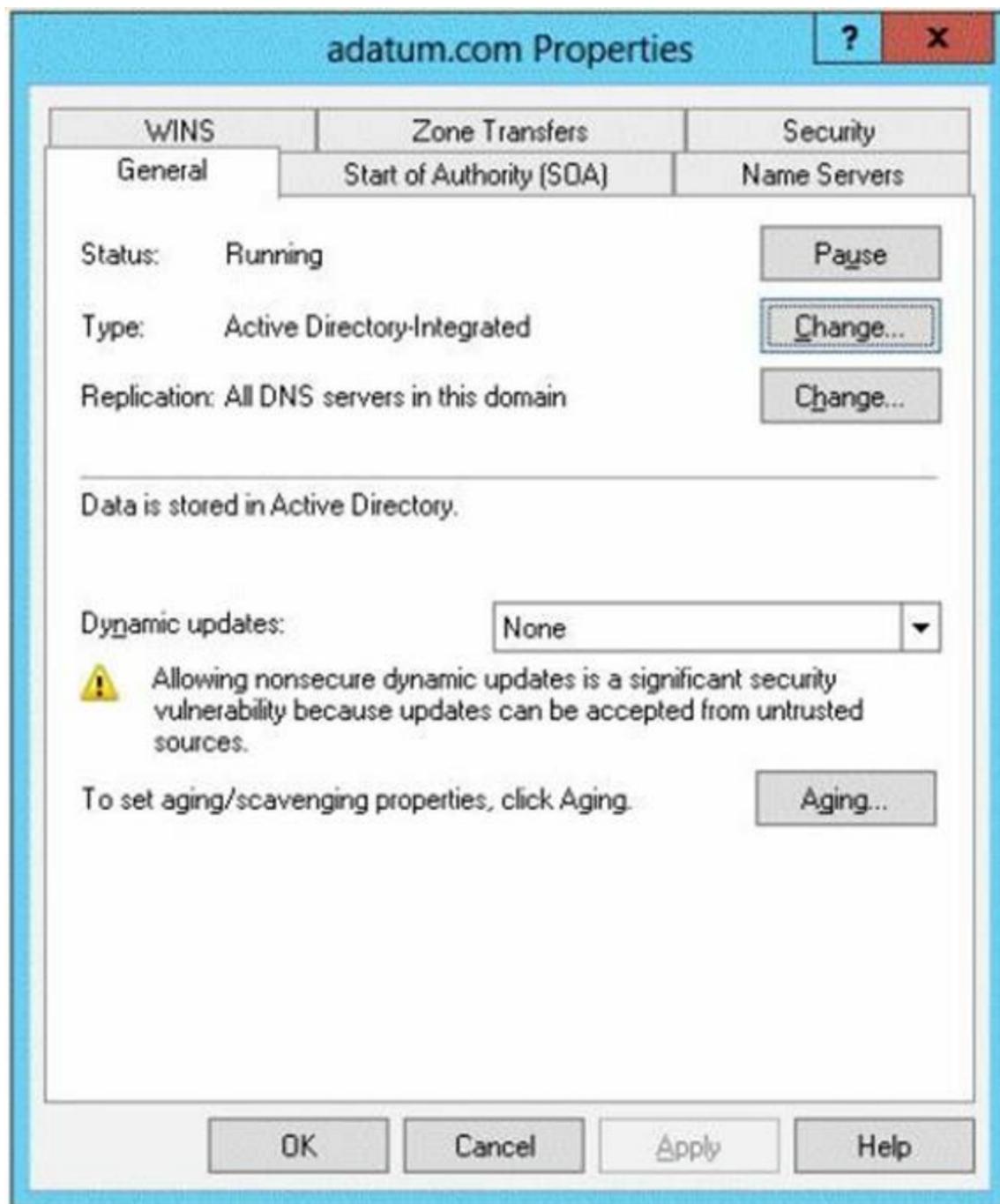
You plan to configure Name Protection on all of the DHCP servers.
You need to configure the adatum.com zone to support Name Protection.
What should you do?

A. Change the zone type.
B. Sign the zone.
C. Add a DNSKEY record.
D. Configure Dynamic updates.

Answer: D

Explanation: Name protection requires secure update to work. Without name protection DNS names may be hijacked.
You can use the following procedures to allow only secure dynamic updates for a zone. Secure dynamic update is supported only for Active Directory–integrated zones. If the zone type is configured differently, you must change the zone type and directory-integrate the zone before securing it for Domain Name System (DNS) dynamic updates.
Enable secure dynamic updates:
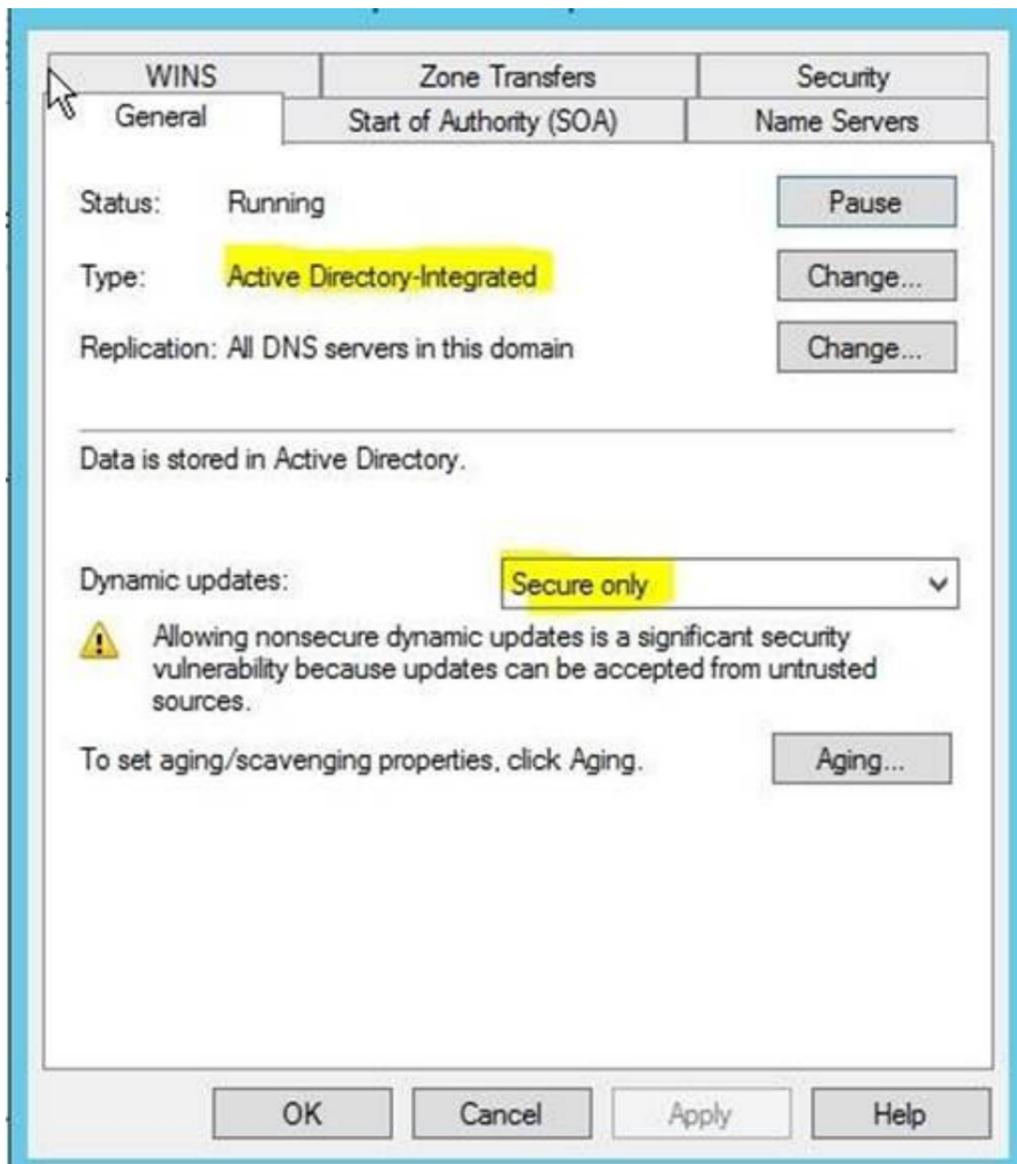
Reference: DHCP: Secure DNS updates should be configured if Name Protection is enabled on any IPv4 scope
http://technet.microsoft.com/en-us/library/ee941152(v=ws.10).aspx

NEW QUESTION 148
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named File1 that runs a Server Core Installation of
Windows Server 2012 R2.
File1 has a volume named D that contains home folders. File1 creates a shadow copy of volume D twice a day.
You discover that volume D is almost full. You add a new volume named H to File1.
You need to ensure that the shadow copies of volume D are stored on volume H. Which command should you run?

A. The Set-Volume cmdlet with the -driveletter parameter
B. The vssadmin.exe create shadow command
C. The Set-Volume cmdlet with the -path parameter
D. The vssadmin.exe add shadowstorage command

Answer: D

Explanation: Add ShadowStorage
Adds a shadow copy storage association for a specified volume.
Incorrect:
Not A. Sets or changes the file system label of an existing volume. -DriveLetter Specifies a letter used to identify a drive or volume in the system.
Not B. Create Shadow
Creates a new shadow copy of a specified volume.
Not C. Sets or changes the file system label of an existing volume -Path Contains valid path information.
Reference: Vssadmin; Set-Volume
http://technet.microsoft.com/en-us/library/cc754968(v=ws.10).aspx http://technet.microsoft.com/en-us/library/hh848673(v=wps.620).aspx

NEW QUESTION 151
Your network contains two servers that run Windows Server 2012 R2 named Server1 and Server2. Both servers have the File Server role service installed.
On Server2, you create a share named Backups.
From Windows Server Backup on Server1, you schedule a full backup to run every night. You set the backup destination to \\Server2 \Backups.
After several weeks, you discover that \\Server2\Backups only contains the last backup that completed on Server1.
You need to ensure that multiple backups of Server1 are maintained. What should you do?

A. Modify the Volume Shadow Copy Service (VSS) settings.
B. Modify the properties of the Windows Store Service (WSService) service.
C. Change the backup destination.
D. Configure the permission of the Backups share.

Answer: C

Explanation:
The destination in the exhibit shows a network share is used. If a network share is being used only the latest copy will be saved.

Reference: Where should I save my backup?
http://windows.microsoft.com/en-us/windows7/where-should-i-save-my-backup

NEW QUESTION 155
Your network contains an Active Directory forest named contoso.com. The forest contains two domains named contoso.com and childl.contoso.com. The domains contain three domain controllers. The domain controllers are configured as shown in the following table.

Domain controller name	Operating system	Configuration
dc1.contoso.com	Windows Server 2008 R2	Schema master Domain naming master
dc10.child1.contoso.com	Windows Server 2012 R2	PDC emulator
dc11.child1.contoso.com	Windows Server 2008 R2	RID master

You need to ensure that the KDC support for claims, compound authentication, and kerberos armoring setting is enforced in both domains.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Raise the domain functional level of contoso.com.
B. Raise the domain functional level ofchildl.contoso.com.
C. Raise the forest functional level of contoso.com.
D. Upgrade DC11 to Windows Server 2012 R2.
E. Upgrade DC1 to Windows Server 2012 R2.

Answer: AE

Explanation: The root domain in the forest must be at Windows Server 2012 level. First upgrade DC1 to this level (E), then raise the contoso.com domain functional level to Windows Server 2012 (A).
* (E) To support resources that use claims-based access control, the principal's domains will need to be running one of the following:
/ All Windows Server 2012 domain controllers.
/ Sufficient Windows Server 2012 domain controllers to handle all the Windows 8 device authentication requests.
/ Sufficient Windows Server 2012 domain controllers to handle all the Windows Server 2012 resource protocol transition requests to support non-Windows 8 devices.
Reference: What's New in Kerberos Authentication http://technet.microsoft.com/en-us/library/hh831747.aspx.

NEW QUESTION 160
DRAG DROP
Your network contains two Active Directory forests named contoso.com and adatum.com. Each forest contains an Active Directory Rights Management Services (AD RMS) root cluster. All servers run Windows Server 2012 R2.
You need to ensure that the rights account certificates issued in adatum.com are accepted by the AD RMS root cluster in contoso.com.
What should you do in each forest?
To answer, drag the appropriate actions to the correct forests. Each action may be used once, more than once, or not at all. You may need to drag the split bar

between panes or scroll to view content.

Actions	Answer Area	
Add a trusted user domain.	Adatum.com:	Action
Add a rights policy template.	Contoso.com:	Action
Export the client licensor certificate.		
Export the server licensor certificate.		
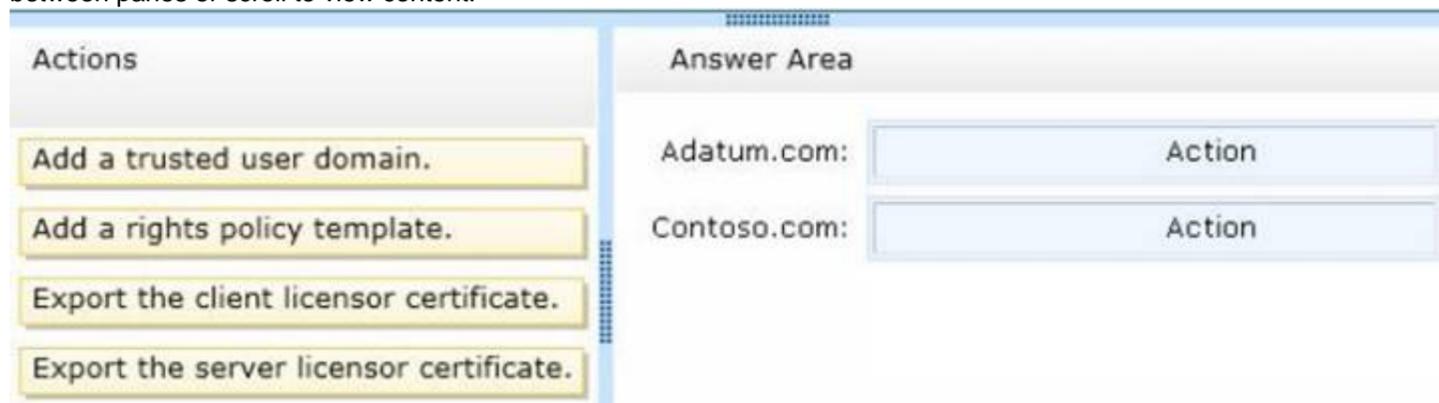
Answer:

Explanation: A trusted user domain, often referred as a TUD, is a trust between AD RMS clusters that instructs a licensing server to accept rights account certificates (the certificates identifying users) from another AD RMS server in a different Active Directory forest. An AD RMS trust is not the same as an Active Directory trust, but it is similar in that it refers to the ability of one environment to accept identities from another environment as valid subjects.
Illustration:
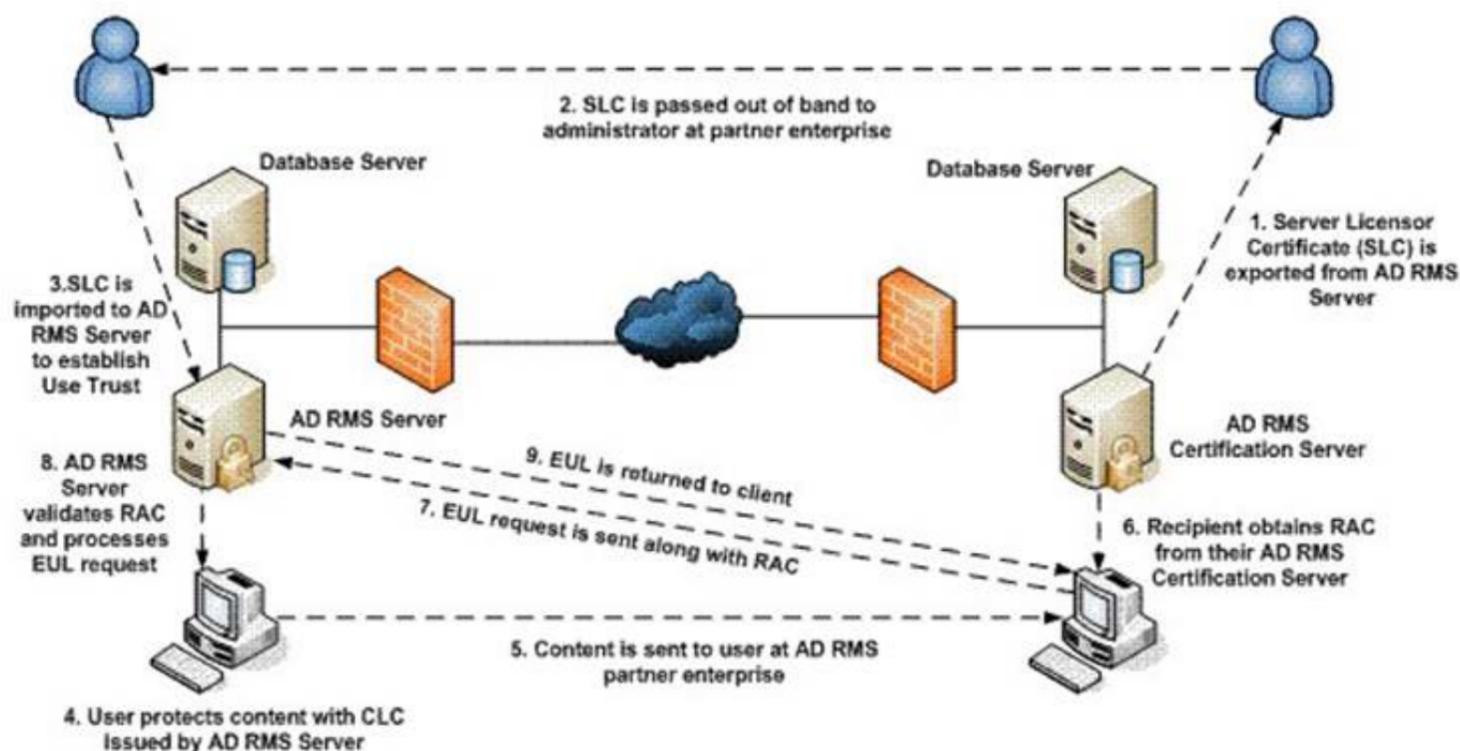
NEW QUESTION 164
Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.
Server1 and Server2 have the Failover Clustering feature installed. The servers are configured as nodes in a failover cluster named Cluster1.
You configure File Services and DHCP as clustered resources for Cluster1. Server1 is the active node for both clustered resources.
You need to ensure that if two consecutive heartbeat messages are missed between Server1 and Server2, Server2 will begin responding to DHCP requests. The solution must ensure that Server1 remains the active node for the File Services clustered resource for up to five missed heartbeat messages.
What should you configure?

A. Affinity-None
B. Affinity-Single
C. The cluster quorum settings
D. The failover settings
E. A file server for general use
F. The Handling priority
G. The host priority
H. Live migration
I. The possible owner
J. The preferred owner
K. Quick migration
L. the Scale-Out File Server

Answer: D

Explanation: The number of heartbeats that can be missed before failover occurs is known as the heartbeat threshold. Heartbeat threshold is failover clustering setting.
Reference: Tuning Failover Cluster Network Thresholds http://technet.microsoft.com/en-us/library/dn265972.aspx
http://technet.microsoft.com/en-us/library/dd197562(v=ws.10).aspx http://blogs.msdn.com/b/clustering/archive/2012/11/21/10370765.aspx

NEW QUESTION 168
HOTSPOT

You have a server named Server1 that runs Windows Server 2012 R2. You are configuring a storage space on Server1.
You need to ensure that the storage space supports tiered storage.
Which settings should you configure?
To answer, select the appropriate options in the answer area.

Answer Area

Disk allocation: [▼]

Volume provisioning type: [▼]

Answer Area

Disk allocation: [▼]
- Automatic
- Hot Spare
- Manual

Volume provisioning type: [▼]
- Fixed
- Thin

Answer:

Explanation: Disk Allocation: Automatic

New Storage Pool Wizard — Select physical disks for the storage pool

Slot	Name	Capacity	Bus	RPM	Model	Allocation	Chassis	Media Type
	PhysicalDisk3 (...	224 GB	SATA			Automatic ▼		SSD
	PhysicalDisk1 (...	224 GB	SATA			Automatic ▼		SSD
	PhysicalDisk2 (...	224 GB	SATA			Automatic ▼		SSD
	PhysicalDisk4 (...	224 GB	SATA			Automatic ▼		SSD
	PhysicalDisk5 (...	932 GB	RAID		Volume A	Automatic ▼		Unknown
	PhysicalDisk6 (...	932 GB	RAID		Volume B	Automatic ▼		Unknown
	PhysicalDisk7 (...	932 GB	RAID		Volume C	Automatic ▼		Unknown
	PhysicalDisk8 (...	932 GB	RAID		Volume D	Hot Spare ▼		Unknown
	PhysicalDisk9 (...	932 GB	RAID		Volume E	Automatic ▼		Unknown
	PhysicalDisk10...	932 GB	RAID		Volume F	Automatic ▼		Unknown
	PhysicalDisk11...	932 GB	RAID		Volume G	Automatic ▼		Unknown
	PhysicalDisk12...	932 GB	RAID		Volume H	Automatic ▼		Unknown
	PhysicalDisk13...	932 GB	RAID		Volume I	Hot Spare ▼		Unknown

Total selected capacity: 9.06 TB
Selecting these disks will create a local pool.

* When using tiers, you must fixed provisioning.
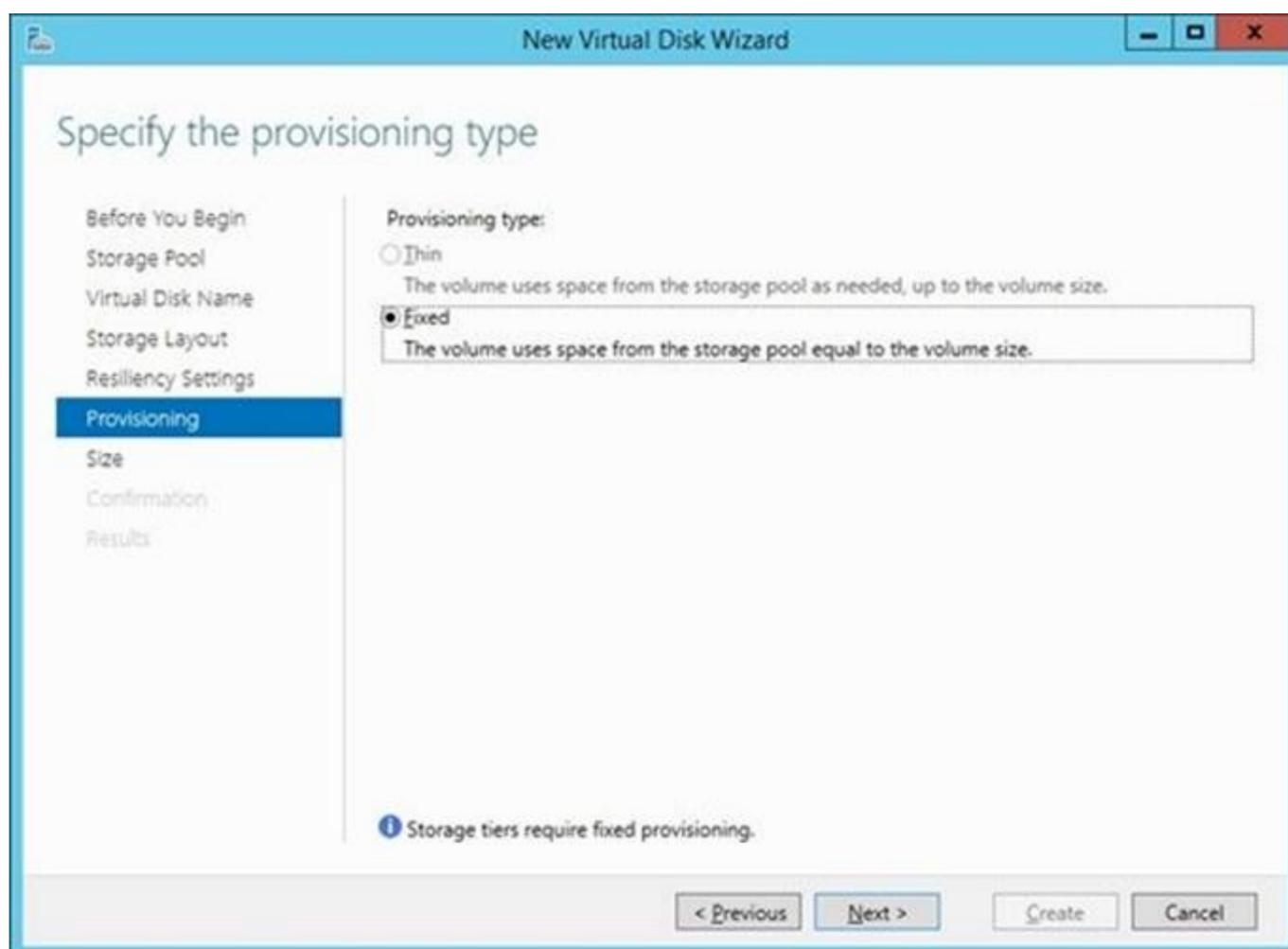
http://blogs.technet.com/resized-image.ashx/ size/550x0/ key/communityserver-blogs-components-weblogfiles/00-00-00-91-74/3201.Figure17.jpg

NEW QUESTION 172
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers have the IP Address Management (IPAM) Server feature installed.
You have a support technician named Tech1. Tech1 is a member of the IPAM Administrators group on Server1 and Server2.
You need to ensure that Tech1 can use Server Manager on Server1 to manage IPAM on Server2.
To which group on Server2 should you add Tech1?

A. IPAM MSM Administrators
B. IPAM Administrators
C. winRMRemoteWMIUsers_
D. Remote Management Users

Answer: C

Explanation: If you are accessing the IPAM server remotely using Server Manager IPAM client RSAT, then you must be a member of the WinRMRemoteWMIUsers group on the IPAM server, in addition to being a member of the appropriate IPAM security group (or local Administrators group).
Reference: IPAM Deployment Planning, IPAM specifications

NEW QUESTION 174
Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.
Server1 and Server2 have the Failover Clustering feature installed. The servers are configured as nodes in a failover cluster named Guster1. Cluster1 contains a file server role named FS1 and a generic service role named SVC1. Server1 is the preferred node for FS1. Server 2 is the preferred node for SVC1.
You plan to run a disk maintenance tool on the physical disk used by FS1.
You need to ensure that running the disk maintenance tool does not cause a failover to occur.
What should you do before you run the tool?

A. Run Suspend-ClusterResource.
B. Run Suspend-GusterNode.
C. Run cluster.exe and specify the pause parameter.
D. Run cluster.exe and specify the offline parameter.

Answer: D

NEW QUESTION 177
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 has the IP Address Management (IPAM) Server feature installed.
A technician performs maintenance on Server1.
After the maintenance is complete, you discover that you cannot connect to the IPAM
server on Server1.
You open the Services console as shown in the exhibit. (Click the Exhibit button.)

Name ▲	Status
Windows Color System	
Windows Connection Manager	Running
Windows Driver Foundation - User-mode Driver Framework	
Windows Encryption Provider Host Service	
Windows Error Reporting Service	
Windows Event Collector	
Windows Event Log	
Windows Firewall	Running
Windows Font Cache Service	Running
Windows Installer	
Windows Internal Database	
Windows Internal Database VSS Writer	
Windows Management Instrumentation	Running
Windows Modules Installer	
Windows Process Activation Service	
Windows Remote Management (WS-Management)	Running
Windows Store Service (WSService)	
Windows Time	Running
Windows Update	
WinHTTP Web Proxy Auto-Discovery Service	
Wired AutoConfig	
WMI Performance Adapter	
Workstation	Running

You need to ensure that you can connect to the IPAM server. Which service should you start?

A. Windows Process Activation Service
B. Windows Event Collector
C. Windows Internal Database
D. Windows Store Service (WSService)

Answer: C

Explanation:
Windows Internal Database
Windows Internal Database is a relational data store that can be used only by Windows roles and features.
IPAM does not support external databases. Only a Windows Internal Database is supported.
IPAM stores 3 years of forensics data (IP address leases, host MAC addresses, user login/logoff information) for 100,000 users in a Windows Internal Database.
There is no database purge policy provided, and the administrator must purge data manually as needed.
Incorrect:
Not A. IPAM works even if the Windows Process Activation Service is not running.
Not B. IPAM does not require the Windows Event Collector Service. It need to be running on the managed DC/DNS/DHCP computers.
Not D. IPAM does not require the Windows Store Service. It provides infrastructure support for Windows Store.This service is started on demand and if disabled applications bought using Windows Store will not behave correctly.
Reference: IPAM Deployment Planning

NEW QUESTION 180
Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2 that run Windows Server 2012 R2. Both servers have the Hyper-V server role installed.
The network contains an enterprise certification authority (CA). All servers are enrolled automatically for a certificate-based on the Computer certificate template.
On Server1, you have a virtual machine named VM1. VM1 is replicated to Server2. You need to encrypt the replication of VM1.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. On Server1, modify the Hyper-V Settings.
B. On Server2, modify the settings of VM1.
C. On Server2, modify the Hyper-V Settings.
D. On Server1, modify the settings of VM1.
E. On Server1, modify the settings of the virtual switch to which VM1 is connected.
F. On Server2, modify the settings of the virtual switch to which VM1 is connected.

Answer: BC

Explanation: \B. Each virtual machine that is to be replicated must be enabled for replication (on the replica server – Server2).
\C.To configure the Replica server(here Server2)
? In Hyper-V Manager, clickHyper-V Settingsin theActionspane.
? In theHyper-V Settingsdialog, clickReplication Configuration.
? In the Details pane, selectEnable this computer as a Replica server.
? In theAuthentication and portssection, select the authentication method. For either authentication method, specify the port to be used (the default ports are 80 for
Etc
Kerberos over HTTP and 443 for certificate-based authentication over HTTPS).
? If you are using certificate-based authentication, clickSelect Certificateand provide the request certificate information.
Reference: Deploy Hyper-V Replica Step 2: Enable Replication

NEW QUESTION 184
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.
Server1 and Server2 have the Hyper-V server role installed. The servers are configured as shown in the following table.

Node name	Node architecture	Virtual machine name
Server1	AMD	VM1 VM2 VM3
Server2	Intel	VM4 VM5 VM6

You add a third server named Server3 to the network. Server3 has Intel processors.
You need to move VM3 and VM6 to Server3. The solution must minimize downtime on the virtual machines.
Which method should you use to move each virtual machine?
To answer, select the appropriate method for each virtual machine in the answer area.

VM3 [▼]
VM6 [▼]
VM3 [▼]
    export and import
    live migration
    quick migration
    storage migration
VM6 [▼]
    export and import
    live migration
    quick migration
    storage migration

Answer:

Explanation: VM3: export/import is the only option due to different processor manufacturers VM6: Live migration can be used as both have Intel CPU's Live Storage Migration requires same processor manufacturers Live migration requires same processor manufacturers
Incorrect:
Quick migration has downtime

NEW QUESTION 186
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2.
Server1 has the Remote Desktop Session Host role service installed. The computer account of Server1 resides in an organizational unit (OU) named OU1.
You create and link a Group Policy object (GPO) named GPO1 to OU1. GPO1 is configured as shown in the exhibit. . (Click the Exhibit button.)
Exhibit is Missing
You need to prevent GPO1 from applying to your user account when you log on to Server1. GPO1 must apply to every other user who logs on to Server1.
What should you configure?

A. Security Filtering
B. VMI Filtering
C. Block Inheritance
D. Item-level targeting

Answer: A

Explanation: Security filtering is a way of refining which users and computers will receive and apply the settings in a Group Policy object (GPO). Using security filtering, you can specify that only certain security principals within a container where the GPO is linked apply the GPO. Security group filtering determines whether the GPO as a whole applies to groups, users, or computers; it cannot be used selectively on different settings within a GPO.
Incorrect:
Not B: Windows Management Instrumentation (WMI) filters allow you to dynamically determine the scope of Group Policy objects (GPOs) based on attributes of the target computer.
Reference: Security filtering using GPMC https://technet.microsoft.com/sv-se/library/Cc781988(v=WS.10).aspx

NEW QUESTION 189
HOTSPOT
Your network contains one Active Directory forest named contoso.com. The forest contains the domain controllers configured as shown in the following table.

Name	Domain	Site	Global catalog
DC1	Contoso.com	Site1	Yes
DC2	Contoso.com	Site2	Yes
DC3	Contoso.com	Site2	No
DC4	Na.contoso.com	Site2	No
DC5	Na.contoso.com	Site1	No
DC6	Na.contoso.com	Site1	No

You perform the following actions:
? Create a file named File1.txt in the SYSVOL folder on DC1.
? Create a user named User1 on DC4.
You need to identify on which domain controller or controllers a copy of each object is stored.
What should you identify? To answer, select the appropriate options in the answer area.

Answer Area

Domain controller	File1.txt	User1
DC3	☐	☐
DC4	☐	☐
DC5	☐	☐
DC6	☐	☐

Answer:

Explanation:

Answer Area

Domain controller	File1.txt	User1
DC3	☑	☐
DC4	☐	☑
DC5	☐	☐
DC6	☐	☐

NEW QUESTION 193
HOTSPOT
Your network contains two DHCP servers named Server1 and Server2. Server1 fails. You discover that DHCP clients can no longer receive IP address leases.
You need to ensure that the DHCP clients receive IP addresses immediately.
What should you configure from the View/Edit Failover Relationship settings? To answer, select the appropriate setting in the answer area.

View/Edit Failover Relationship

Edit parameters related to the failover relationship:

Relationship name: server1.contoso.com-server2.contoso.cc

State of this server: Lost contact with partner

[Change to partner down]

State of partner server: Not available

☐ Enable Message Authentication

Shared Secret:

○ Load Balance Mode

Local Server: 0 %

Partner Server: 0 %

◉ Hot Standby Mode

Role of this server: Standby

Addresses reserved for standby server: 5 %

[OK] [Cancel]

Answer:

Explanation: A manual failover will have to occur by clicking on the Change to partner down button (the partner has to actually be unavailable to click this button).
Note: You can manually change the state of a server which is running in communication interrupted to partner down using DHCP MMC or DHCP PowerShell.
In MMC, go to IPv4->Properties, go to Failover tab, select the specific failover relationship and click edit. You will see "Change to partner down" button on the edit page. This button is enabled when the server is running in communication interrupted state.

NEW QUESTION 196
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains the two servers.
The servers are configured as shown in the following table.

Server name	Role
Server1	Issuing certification authority (CA)
Server2	Web server

You investigate a report about the potential compromise of a private key for a certificate issued to Server2.
You need to revoke the certificate issued to Server2. The solution must ensure that the revocation can be reverted.
Which reason code should you select?
To answer, select the appropriate reason code in the answer area.

Answer:

Explanation: If you specify "Certificate Hold" as the reason for revoking the certificate, it typically means that you may want to unrevoke the certificate at a future time. Only certificates that have been revoked with the reason of "Certificate Hold" can be unrevoked.

NEW QUESTION 200
Your network contains an Active Directory forest named contoso.com.
Users frequently access the website of an external partner company. The URL of the website is http://partners.adatum.com.
The partner company informs you that it will perform maintenance on its Web server and that the IP addresses of the Web server will change.
After the change is complete, the users on your internal network report that they fail to access the website. However, some users who work from home report that they can access the website.
You need to ensure that your DNS servers can resolve partners.adatum.com to the correct IP address immediately.
What should you do?

A. Run ipconfig and specify the FlushDns parameter.
B. Run ipconfig and specify the Renew parameter.
C. Run dnscmd and specify the ClearCache parameter.
D. Run Set-DnsServerResourceRecordAging.

Answer: C

Explanation: We cane clear the DNS cache on the DNS server with either Dnscmd
/ClearCache (from command prompt) or Clear-DnsServerCache (from Windows PowerShell).
Reference: Technet, Dnscmd https://technet.microsoft.com/en-us/library/cc772069.aspx

NEW QUESTION 201
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. The forest contains three Active Directory sites named SiteA, SiteB, and SiteC. The sites contain four domain controllers. The domain controllers are configured as shown in the following table.

Site name	Domain controller name
SiteA	DC1, DC2
SiteB	DC3, DC4
SiteC	None

An IP site link exits between each site.
You discover that the users in SiteC are authenticated by the domain controllers in SiteA and SiteB.
You need to ensure that the SiteC users are authenticated by the domain controllers in SiteB, unless all of the domain controllers in SiteB are unavailable.
What should you do?

A. Create an SMTP site link between SiteB and SiteC.
B. Crate additional connection objects for DC1 and DC2.
C. Decrease the cost of the site link between SiteB and SiteC.
D. Create additional connection objects for DC3 and DC4.

Answer: C

Explanation: By decreasing the site link cost between SiteB and SiteC the SiteC users would be authenticated by SiteB rather than by SiteA.

NEW QUESTION 204

DRAG DROP
Your network contains four servers that run Windows Server 2012 R2.
Each server has the Failover Clustering feature installed. Each server has three network adapters installed. An iSCSI SAN is available on the network.
You create a failover cluster named Cluster1. You add the servers to the cluster.
You plan to configure the network settings of each server node as shown in the following table.

Network card name	Network ID	Cluster network	Network communication
NIC1	192.168.1.0/24	Cluster Network 1	Client traffic, Management traffic, and Heartbeat traffic
NIC2	192.168.2.0/24	Cluster Network 2	Heartbeat traffic only
NIC3	192.168.3.0/24	Cluster Network 3	iSCSI SAN traffic only

You need to configure the network settings for Cluster1. What should you do?
To answer, drag the appropriate network communication setting to the correct cluster network. Each network communication setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Network Communication Settings

Allow cluster network communication on this network

Do not allow cluster network communication on this network

Answer Area

Cluster Network 1	Network communication setting
Cluster Network 2	Network communication setting
Cluster Network 3	Network communication setting
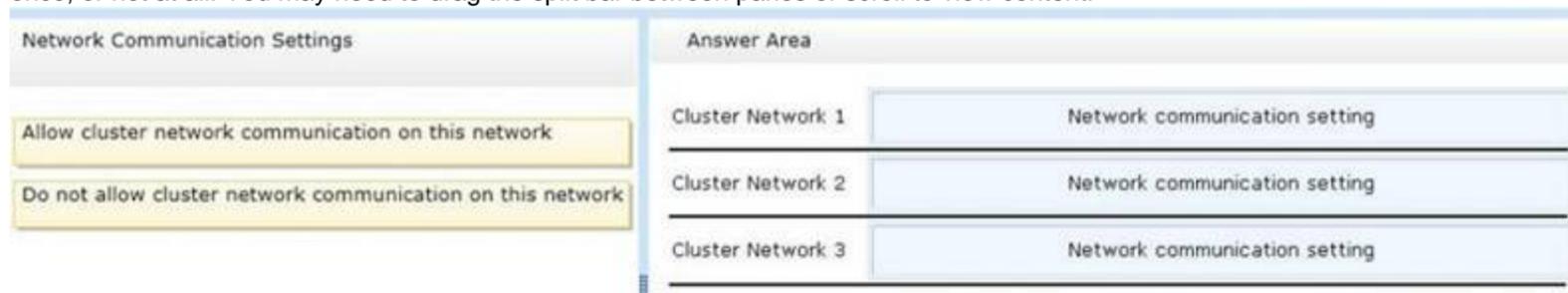
Answer:

Explanation: Allow cluster network communication for heartbeats.
Note: Heartbeats
The Cluster service, running on each node of the cluster, keeps track of the current state of the nodes within a cluster and determines when a group and its resources fail over to an alternate node. This communication takes the form of messages that are sent regularly between each node's Cluster service. These messages are called heartbeats.

NEW QUESTION 206
Your network contains one Active Directory domain named contoso.com. The domain contains an IP Address Management (IPAM)
Server named Server1. Server1 manages several DHCP and DNS servers. From server Manager on Server1, you create a custom role for IPAM.
You need to assign the role to a group named IP_Admins.
What should you do?

A. From Windows PowerShell, run theAdd-Membercmdlet.
B. From Server Manager, create an access policy.
C. From Windows PowerShell, run theSet-IpamConfigurationcmdlet.
D. From Server Manager, create an access scope.

Answer: B

Explanation: A role is a collection of IPAM operations. You can associate a role with a user or group in Windows using an access policy. Several built-in roles are provided, but you can also create customized roles to meet your business requirements.
Reference: Manage IPAM, Access Control https://technet.microsoft.com/en-us/library/dn741281.aspx

NEW QUESTION 207
You have a group Managed Service Account named Service01. Three servers named Server01, Server02, and Server03 currently use the Service01 service account.
You plan to decommission Server01.
You need to remove the cached password of the Service01 service account from Server01. The solution must ensure that Server02 and Server03 continue to use Service01.
Which cmdlet should you run?

A. Set-ADServiceAccount
B. Reset-ADServiceAccountPassword
C. Remove-ADServiceAccount
D. Uninstall-ADServiceAccount

Answer: B

Explanation: We reset the password for the service.
The Reset-ADServiceAccountPassword cmdlet resets the service account password for
the local computer. This cmdlet needs to be run on the computer where the service account is installed.

Incorrect:
Not A: The Set-ADServiceAccount cmdlet cannot modify the password of the service.
Reference: Reset-ADServiceAccountPassword https://technet.microsoft.com/en-us/library/ee617201.aspx

NEW QUESTION 210
Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.
The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.
You need to identify whether deleted objects can be recovered from the Active Directory Recycle Bin.
Which cmdlet should you use?

A. Get-ADGroupMember
B. Get-ADDomainControllerPasswordReplicationPolicy
C. Get-ADDomainControllerPasswordReplicationPolicyUsage
D. Get-ADDomain
E. Get-ADOptionalFeature

Answer: E

Explanation: The Get-ADOptionalFeature cmdlet gets an optional feature or performs a search to retrieve multiple optional features from an Active Directory.
Example: Get a specified optional feature
This command gets the optional feature with the name Recycle Bin Feature. Windows PowerShell
PS C:\> Get-ADOptionalFeature -Identity 'Recycle Bin Feature'
Reference: Get-ADOptionalFeature
https://technet.microsoft.com/en-us/library/hh852212(v=wps.630).aspx

NEW QUESTION 213
Your network contains an Active Directory domain named adatum.com. The domain contains a file server named FS1 that runs Windows Server 2012 R2 and has the File Server Resource Manager role service installed. All client computers run Windows 8.
File classification and Access-Denied Assistance are enabled on FS1.
You need to ensure that if users receive an Access Denied message, they can request assistance by email from the Access Denied dialog box.
What should you configure?

A. A file management task
B. A classification property
C. The File Server Resource Manager Options
D. A report task

Answer: C

Explanation: You can configure access-denied assistance individually on each file server by using the File Server Resource Manager console.
Note:
To configure access-denied assistance by using File Server Resource Manager
? Open File Server Resource Manager. In Server Manager, clickTools, and then clickFile Server Resource Manager.
? Right-clickFile Server Resource Manager (Local), and then clickConfigure Options.
? Click theAccess-Denied Assistancetab.
? Select theEnable access-denied assistancecheck box.
? In theDisplay the following message to users who are denied access to a folder or filebox, type a message that users will see when they are denied access to a file or folder.
You can add macros to the message that will insert customized text.
? ClickConfigure email requests, select theEnable users to request assistancecheck box, and then clickOK.
? ClickPreviewif you want to see how the error message will look to the user.
? ClickOK.
Reference: Deploy Access-Denied Assistance (Demonstration Steps)

NEW QUESTION 214
You have a server named Server1 that runs Windows Server 2012 R2. Windows Server 2012 R2 is installed on volume C.
You need to ensure that Safe Mode with Networking loads the next time Server1 restarts. Which tool should you use?

A. The Msconfig command
B. The Bootcfg command
C. The Restart-Computer cmdlet
D. The Restart-Server cmdlet

Answer: A

Explanation: Use system config (Msconfig) to configure boot options.
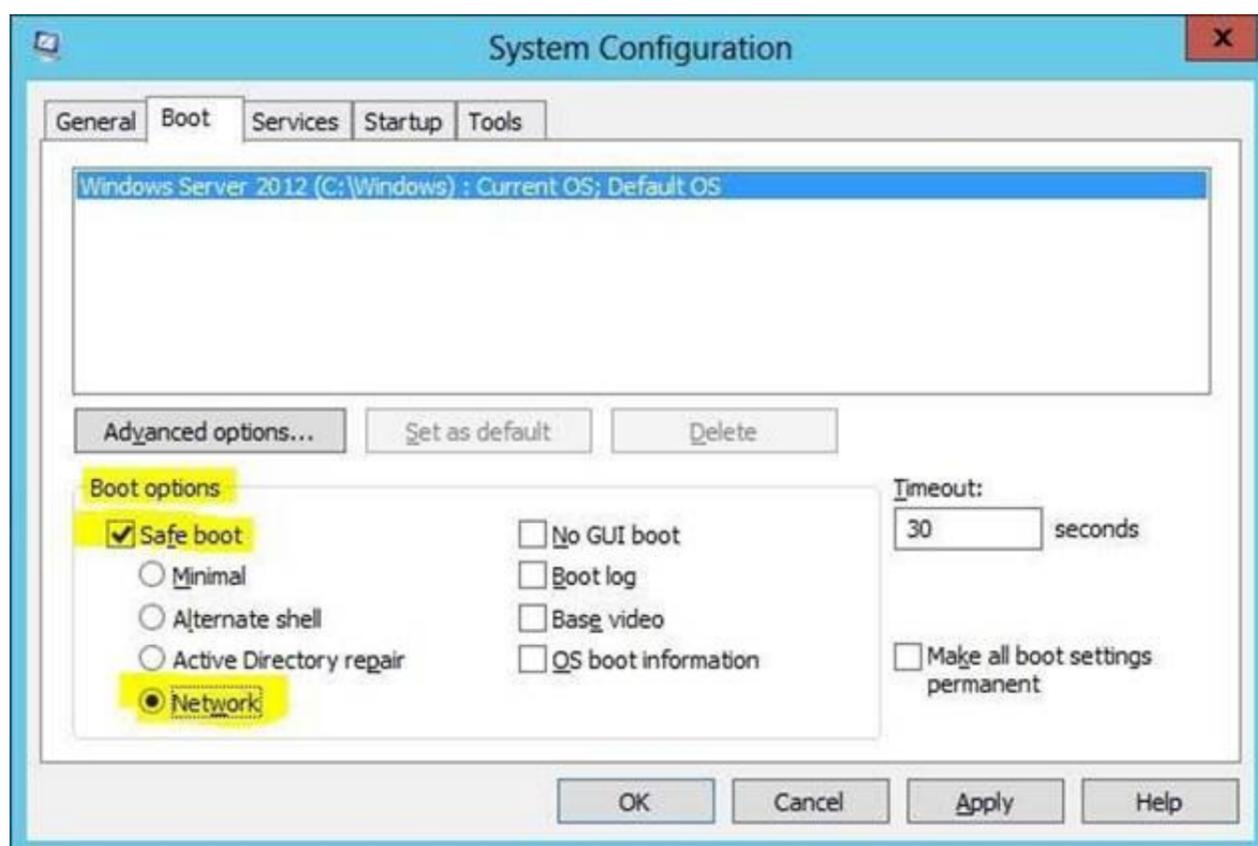
Reference: System Configuration – aka MSCONFIG.

NEW QUESTION 217
You have a failover cluster named Cluster1 that contains four nodes. All of the nodes run Windows Server 2012 R2.
You need to force every node in Cluster1 to contact immediately the Windows Server Update Services (WSUS) server on your network for updates.
Which tool should you use?

A. The Add-CauClusterRole cmdlet
B. The Wuauclt command
C. The Wusa command
D. The Invoke-CauScan cmdlet

Answer: A

Explanation: The Add-CauClusterRole cmdlet adds the Cluster-Aware Updating (CAU) clustered role that provides the self-updating functionality to the specified cluster. When the CAU clustered role has been added to a cluster, the failover cluster can update itself on the schedule that is specified by the user, without requiring an external computer to coordinate the cluster updating process.
Incorrect:
Not B. The wuauclt utility allows you some control over the functioning of the Windows Update Agent. It is updated as part of Windows Update.
The following are the command line for wuauclt.
OptionDescription
/a /ResetAuthorization
Initiates an asynchronous background search for applicable updates. If Automatic Updates is disabled, this option has no effect.
/r /ReportNow
Sends all queued reporting events to the server asynchronously.
/? /h /help
Shows this help information.
Not D.
The Invoke-CauScan cmdlet performs a scan of cluster nodes for applicable updates and returns a list of the initial set of updates that would be applied to each node in a specified cluster.
Note: The Invoke-CauRun cmdlet performs a scan of cluster nodes for applicable updates and installs those updates via an Updating Run on the specified cluster.
Reference: Add-CauClusterRole
http://technet.microsoft.com/en-us/library/hh847235(v=wps.620).aspx

NEW QUESTION 221
DRAG DROP
Your network contains an Active Directory forest. The forest contains a single domain named contoso.com.
The forest contains two Active Directory sites named Main and Branch1. The sites connect to each other by using a site link named Main-Branch1. There are no other site links.
Each site contains several domain controllers. All domain controllers run Windows Server 2012 R2. Your company plans to open a new branch site named Branch2. The new site will have a WAN link that connects to the Main site only. The site will contain two domain controllers that run Windows Server 2012 R2.
You need to create a new site and a new site link for Branch2. The solution must ensure that the domain controllers in Branch2 only replicate to the domain controllers in Branch1 if all of the domain controllers in Main are unavailable.
Which three actions should you perform?
To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Disable site link bridging.	
Add Branch2 to the Main-Branch1 site link.	
Remove Branch2 from the Main-Branch1 site link.	
Create a new site link bridge named Main-Branch2.	
Create a new site link object named Main-Branch2.	
Create a new site object named Branch2.	

Answer:

Explanation: SO...the first part of this answer is:
\1. Create a new site object named Branch2
*When you create the new site Branch2 you will be prompted to associate it with a site link...right now we only have one site link (Main-Branch1). Hit Finish
\2. Remove Branch2 site from the Main-Branch1 Site Link
*In order to move a site into a new site link, you must first remove them from their previous site link....In this case Branch2 was put in Main-Branch1 when we create the new site because we didn't have another site link to associate the new site with at the time we created it.
\3. Create a new site link object named Main-Branch2
*When you create the site link object you will be asked to place the appropriate sites in this link...choose Main and Branch 2
Because we are using Interstice topology replication, ISTG (similar to KCC with Intrasite) will build a logical transitive connection path between all site links because site link bridge is enabled by default and is a Microsoft best practice to leave this default.
By default a site link has a default cost of 100 so the Main-Branch1 site cost 100. Since we
do not have a site link established from Branch2 - Branch1, ISTG will create a logical patch that travels along the Main-Branch2 site link (cost 100) and through Main-Branch1 site link(cost 100) to establish replication connection in the event the least cost path goes down. Since the logical path =200, Branch2 will only replicate with Branch1 if the site link to the Main Site goes down.

NEW QUESTION 225
You have a DHCP server named Server1 that runs Windows Server 2012 R2.
Server1 has two scopes named Production and Development. Currently, all DHCP clients register their host name in a DNS zone named contoso.com.
You need to ensure that only the clients that obtain an IP address from the Development scope, register their host name in a DNS zone named dev.contoso.com.
What should you do?

A. Run the Set-DHCPServerv4Binding cmdlet.
B. Modify the Advanced settings of the Development scope.
C. Modify the Advanced settings of the DHCP server.
D. Create a DHCP policy for the Development scope.

Answer: D

Explanation: DHCP policies can be defined server wide or for a specific scope. Any DNS registration behavior of the DHCP server which can be configured server wide or on a per scope basis
– for example, turn on/off the DNS registration (and deregistration) or DNS name protection
– can be configured on a per policy basis.
Reference: DHCP Policies in Windows Server 2012 http://blogs.technet.com/b/teamdhcp/archive/2012/08/22/granular-dhcp-server-administration-using-dhcp-policies-in-windows-server-2012.aspx

NEW QUESTION 226
HOTSPOT
Your network contains an Active Directory domain named contoso.com.
You install the IP Address Management (IPAM) Server feature on a server named Server1 and select Manual as the provisioning method.
The IPAM database is located on a server named SQL1.
You need to configure IPAM to use Group Policy Based provisioning. What command should you run first?
To answer, select the appropriate options in the answer area.

Answer Area

▼	▼	▼

Answer Area

Invoke-IpamGpoProvisioning		─ComputerName		Automatic
Remove-IpamServerInventory		─DatabaseServer		Contoso.com
Set-IpamConfiguration		─Name		Ipam
Uninstall-WindowsFeature		─ProvisioningMethod		Sql1
Update-IpamServer				
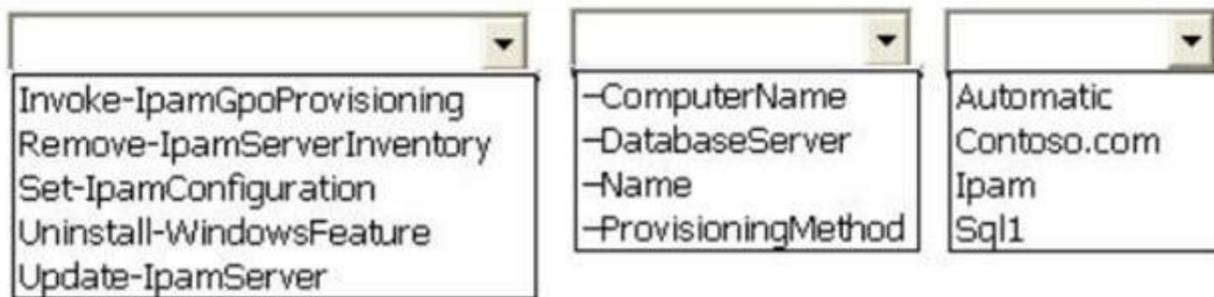
Answer:

Explanation: The choice of a provisioning method is permanent for the current installation of IPAM Server. To change the provisioning method, you must uninstall and reinstall IPAM Server.

NEW QUESTION 229
HOTSPOT
Your network contains one Active Directory domain named contoso.com. The domain contains 10 file servers that run Windows Server 2012 R2.
You plan to enable BitLocker Drive Encryption (BitLocker) for the for the operating system drives of the file servers.
You need to configure BitLocker policies for the file servers to meet the following requirements:
? Ensure that all of the servers use a startup PIN for operating system drives encrypted with BitLocker.
? Ensure that the BitLocker recovery key and recovery password are stored in Active
Directory.
Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.

Local Group Policy Editor			
File Action View Help			

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Not configured	No
Require additional authentication at startup (Windows Serve...	Not configured	No
Disallow standard users from changing the PIN or password	Not configured	No
Enable use of BitLocker authentication requiring preboot ke...	Not configured	No
Allow enhanced PINs for startup	Not configured	No
Configure minimum PIN length for startup	Not configured	No
Configure use of hardware-based encryption for operating s...	Not configured	No
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives ca...	Not configured	No
Configure TPM platform validation profile for BIOS-based fi...	Not configured	No
Configure TPM platform validation profile (Windows Vista, ...	Not configured	No
Configure TPM platform validation profile for native UEFI fir...	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

Windows Components
  ActiveX Installer Service
  Add features to Windows 8.1
  App Package Deployment
  App runtime
  Application Compatibility
  AutoPlay Policies
  Biometrics
  BitLocker Drive Encryption
    Fixed Data Drives
    Operating System Drives
    Removable Data Drives
  Credential User Interface
  Desktop Gadgets
  Desktop Window Manager
  Device and Driver Compatibilit
  Digital Locker
  Edge UI
  Event Forwarding
  Event Log Service
  Event Viewer

Extended / Standard

17 setting(s)

Answer:

Explanation: Choice 1: Require additional authentication at startup
Choice 2: Choose how BitLocker-protected operating system drives can be recovered
* Choice 1: Require additional authentication at startup
This policy setting is used to control which unlock options are available for operating system drives.
You can set this option to Require startup PIN with TPM
Choice 2: Choose how BitLocker-protected operating system drives can be recovered This policy setting is used to configure recovery methods for operating system drives.
In Save BitLocker recovery information to Active Directory Domain Services, choose which BitLocker recovery information to store in Active Directory Domain Services (AD DS) for operating system drives. If you select Store recovery password and key packages, the BitLocker recovery password and the key package are stored in AD DS. Storing the key package supports recovering data from a drive that is physically corrupted. If you select Store recovery password only, only the recovery password is stored in AD DS.

NEW QUESTION 230
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.
DC1 has the DHCP Server server role installed.
DHCP is configured as shown in the exhibit. (Click the Exhibit button.)
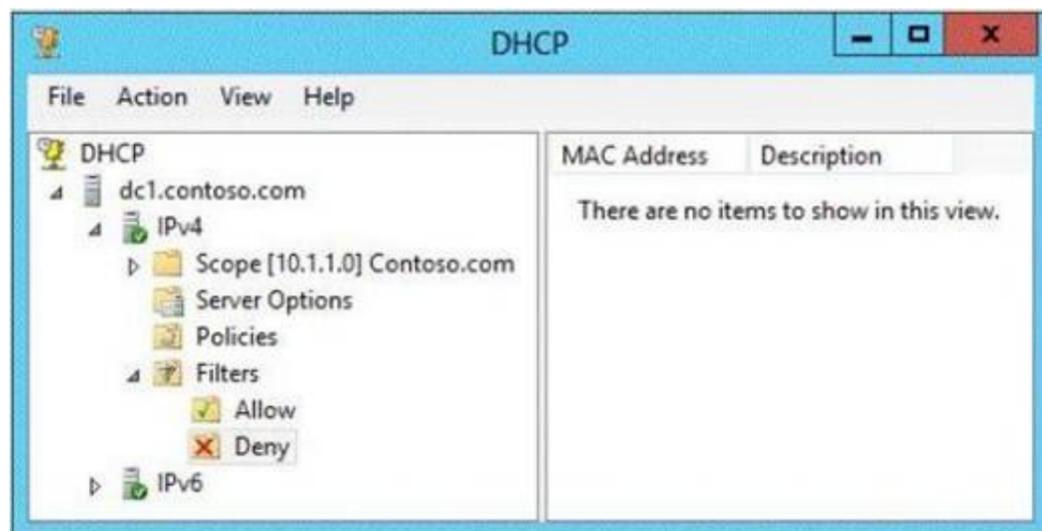
You discover that client computers cannot obtain IPv4 addresses from DC1.
You need to ensure that the client computers can obtain IPv4 addresses from DC1. What should you do?

A. Activate the scope.
B. Authorize DC1.
C. Disable the Allow filters.
D. Disable the Deny filters.

Answer: C

Explanation: You have enabled the Allow list but haven't entered any MAC addresses, thus everyone is denied. Either Disable the Allow filters or start adding MAC addresses to the Allow filter.
Note: MAC address based filtering allows specific control over which clients have access to DHCP addresses. You can create a list of computers that are allowed to obtain DHCP addresses from the server by adding the client MAC address to the list of allowed client computers. By enabling the allow list, you automatically deny access to the DHCP server addresses to any client computer not on the list.
Reference: DHCP: If the allow list is enabled, MAC address filtering should be populated https://technet.microsoft.com/en-us/library/ee956897(v=ws.10)

NEW QUESTION 231
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2.
Server1 has the Active Directory Rights Management Services server role installed.
Your company works with a partner organization that does not have its own Active Directory Rights Management Services (AD RMS) implementation.
You need to create a trust policy for the partner organization.
The solution must meet the following requirements:
? Grant users in the partner organization access to protected content.
? Provide users in the partner organization with the ability to create protected content.
Which type of trust policy should you create?

A. A federated trust
B. Windows Live ID
C. A trusted publishing domain
D. A trusted user domain

Answer: A

Explanation: In AD RMS rights can be assigned to users who have a federated trust with Active Directory Federation Services (AD FS). This enables an organization to share access to rights-protected content with another organization without having to establish a separate Active Directory trust or Active Directory Rights Management Services (AD RMS) infrastructure.
Incorrect:
Not C. Trusted publishing domains allow one AD RMS server to issue use licenses that correspond with a publishing license issued by another AD RMS server, but in this scenario the partner organization does not have any Active Directory.
Not D. A trusted user domain, often referred as a TUD, is a trust between AD RMS clusters, but in this scenario the partner organization does not have any Active Directory.
Reference: AD RMS and AD FS Considerations http://technet.microsoft.com/en-us/library/dd772651(v=WS.10).aspx

NEW QUESTION 235
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 70-412 Exam with Our Prep Materials Via below:

https://www.certleader.com/70-412-dumps.html