Version: 34.0

Question: 1

Your company recently deployed a new Active Directory forest named contoso.com. The first domain controller in the forest runs Windows Server 2012 R2.
You need to identify the time-to-live (TTL) value for domain referrals to the NETLOGON and SYSVOL shared folders.
Which tool should you use?

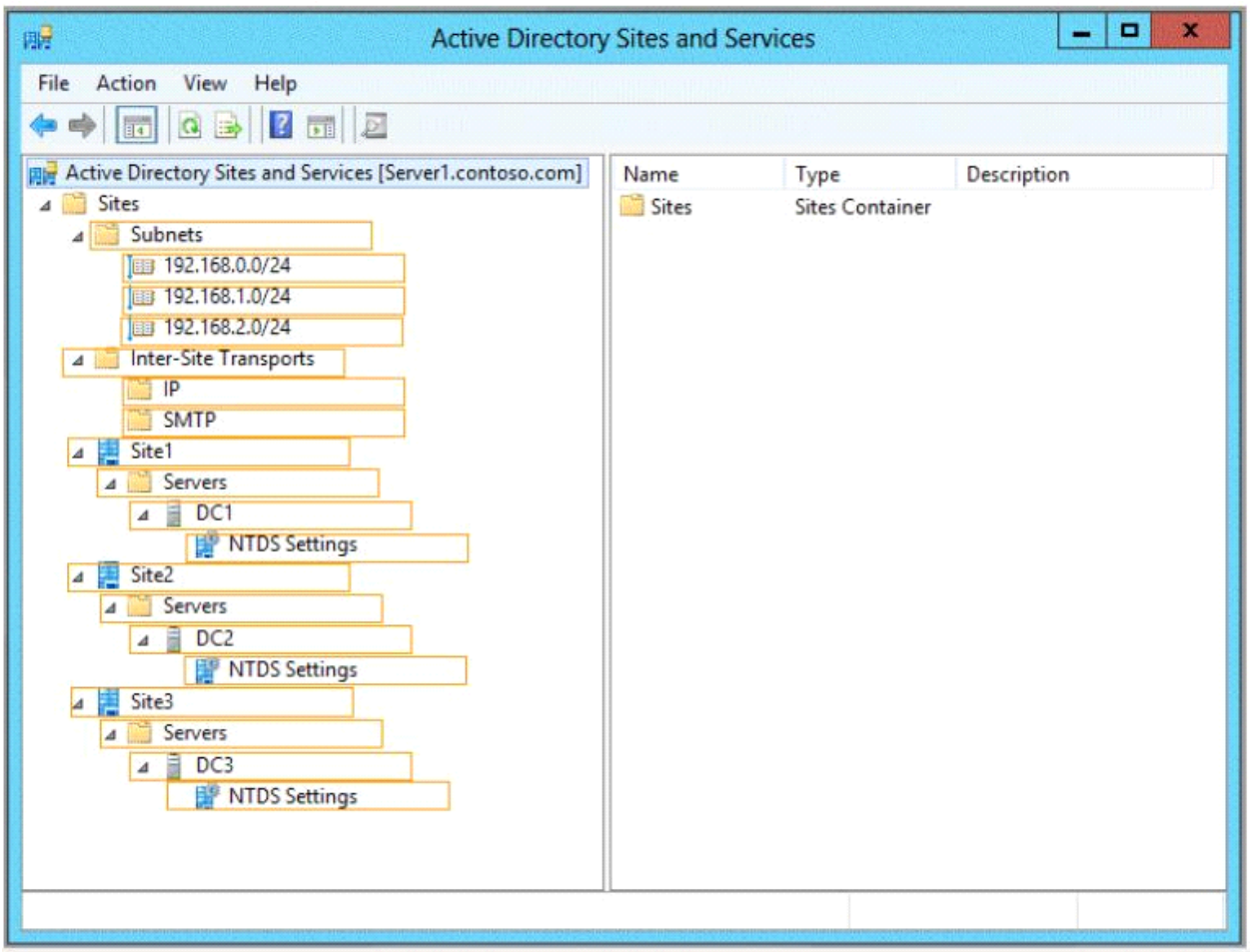
A. Ultrasound
B. Replmon
C. Dfsdiag
D. Frsutil

Answer: C

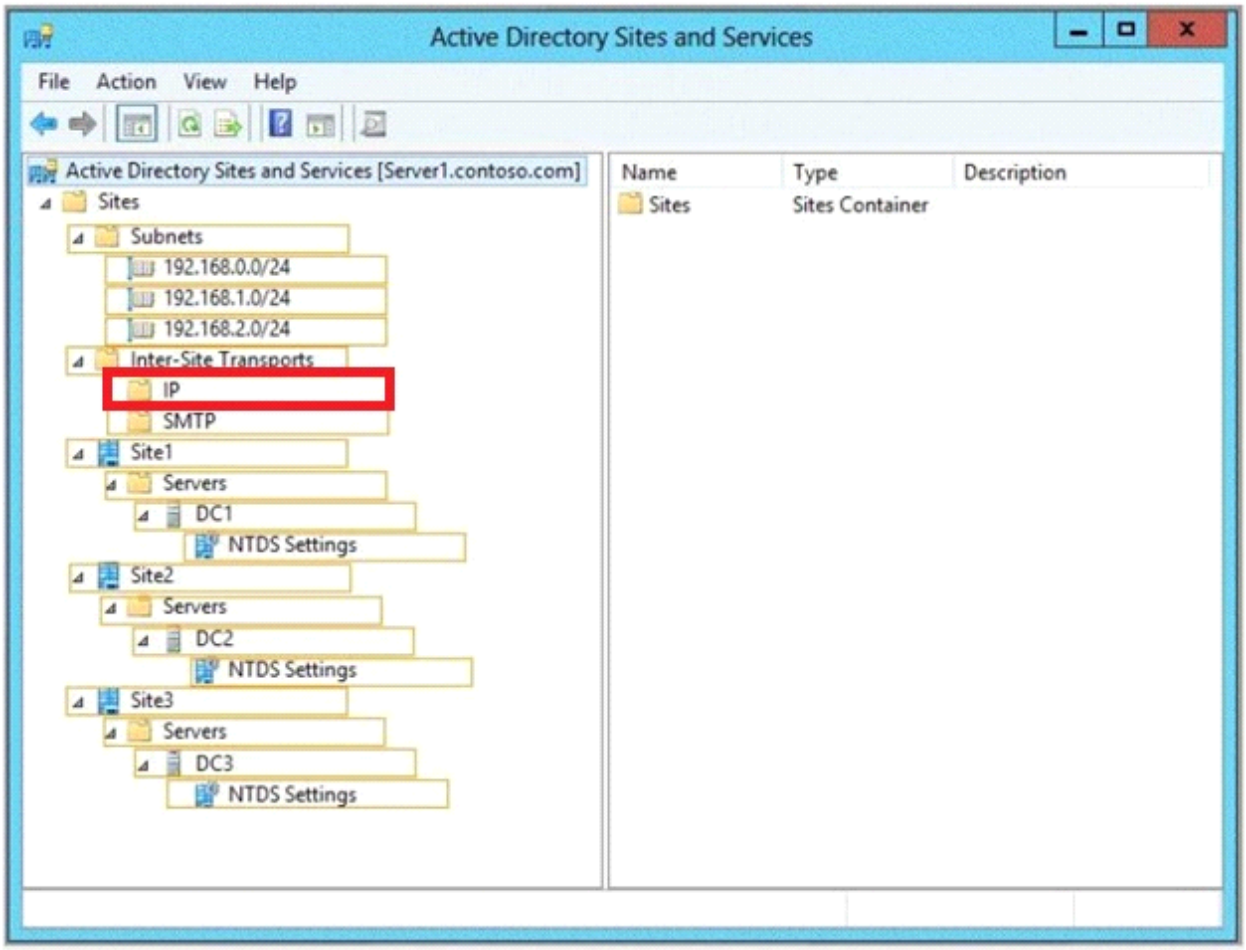
Explanation:
DFSDIAG can check your configuration in five different ways:
Checking referral responses (DFSDIAG /TestReferral)
Checking domain controller configuration
Checking site associations
Checking namespace server configuration
Checking individual namespace configuration and integrity
Reference: Five ways to check your DFS-Namespaces (DFS-N) configuration with the DFSDIAG.EXE tool

Question: 2

HOTSPOT
Your network contains an Active Directory forest named contoso.com that contains a single domain. The forest contains three sites named Site1, Site2, and Site3.
Domain controllers run either Windows Server 2008 R2 or Windows Server 2012 R2.
Each site contains two domain controllers. Site1 and Site2 contain a global catalog server.
You need to create a new site link between Site1 and Site2. The solution must ensure that the site link supports the replication of all the naming contexts.
From which node should you create the site link?
To answer, select the appropriate node in the answer area.


Active Directory Sites and Services
File Action View Help
Active Directory Sites and Services [Server1.contoso.com]
Sites
Subnets
192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
Inter-Site Transports
IP
SMTP
Site1
Servers
DC1
NTDS Settings
Site2
Servers
DC2
NTDS Settings
Site3
Servers
DC3
NTDS Settings
Name
Type
Description
Sites
Sites Container

Answer:



Explanation:

Create a Site Link

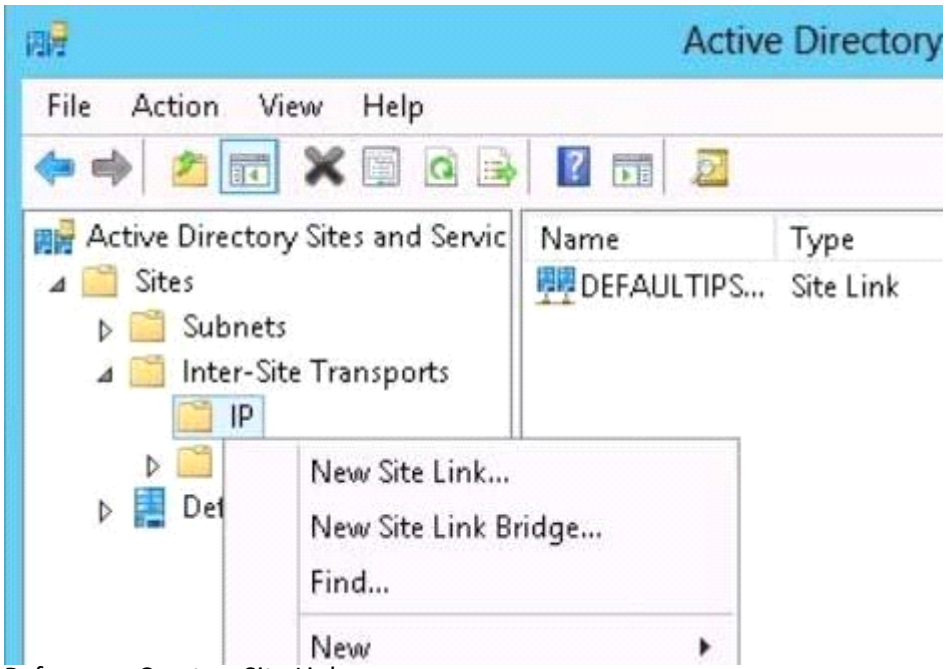
To create a site link

Open Active Directory Sites and Services. To open Active Directory Sites and Services, click Start, click Administrative Tools, and then click Active Directory Sites and Services.

To open Active Directory Sites and Services in Windows Server® 2012, click Start, type dssite.msc.

In the console tree, right-click the intersite transport protocol that you want the site link to use.

Use the IP intersite transport unless your network has remote sites where network connectivity is intermittent or end-to-end IP connectivity is not available. Simple Mail Transfer Protocol (SMTP) replication has restrictions that do not apply to IP replication.



Reference: Create a Site Link
http://technet.microsoft.com/en-us/library/cc731294.aspx

Question: 3

Your network contains two Active Directory forests named contoso.com and adatum.com.
Contoso.com contains one domain. Adatum.com contains a child domain named child.adatum.com.
Contoso.com has a one-way forest trust to adatum.com. Selective authentication is enabled on the forest trust.
Several user accounts are migrated from child.adatum.com to adatum.com.
Users report that after the migration, they fail to access resources in contoso.com. The users successfully accessed the resources in contoso.com before the accounts were migrated.
You need to ensure that the migrated users can access the resources in contoso.com.
What should you do?

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

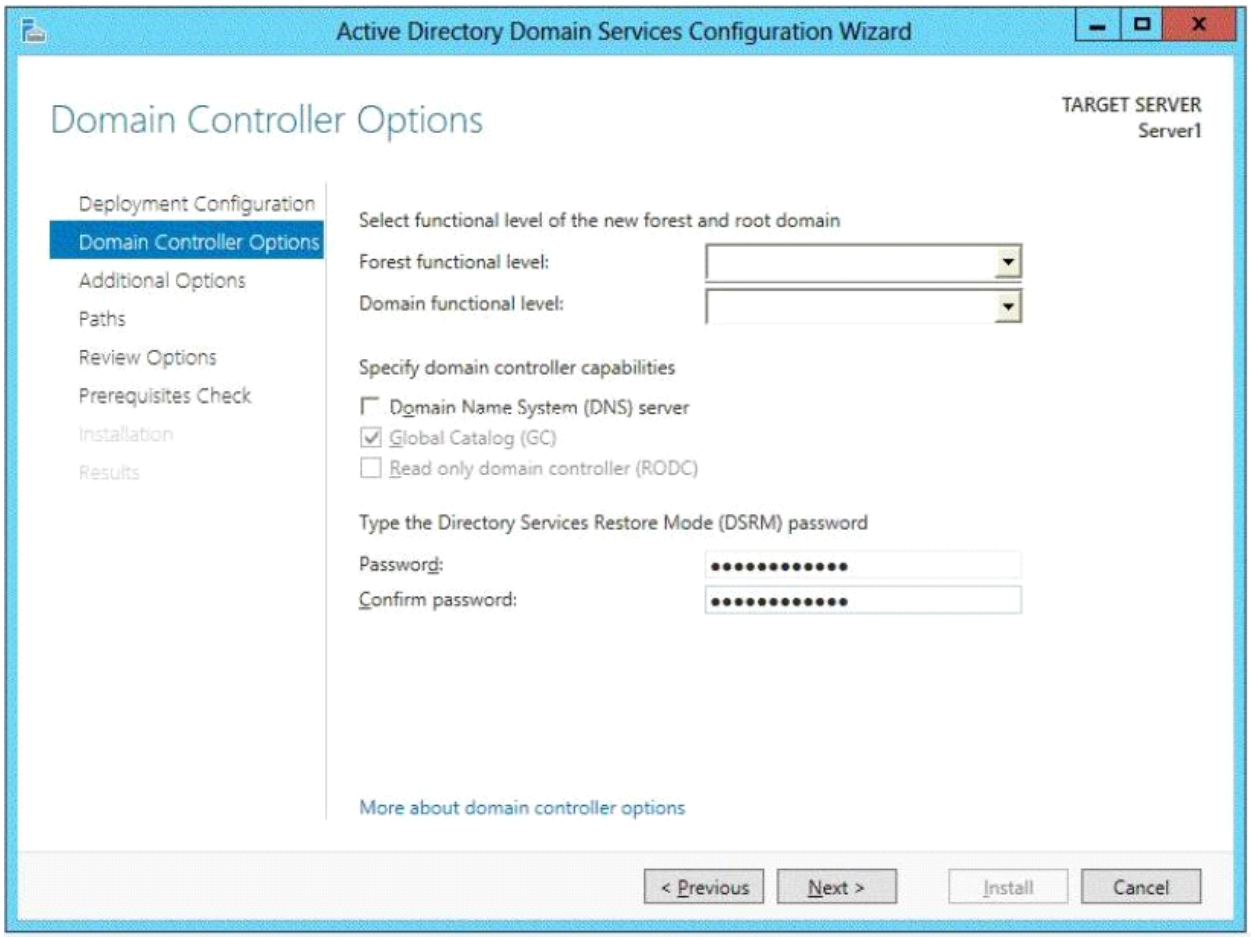
Answer: C

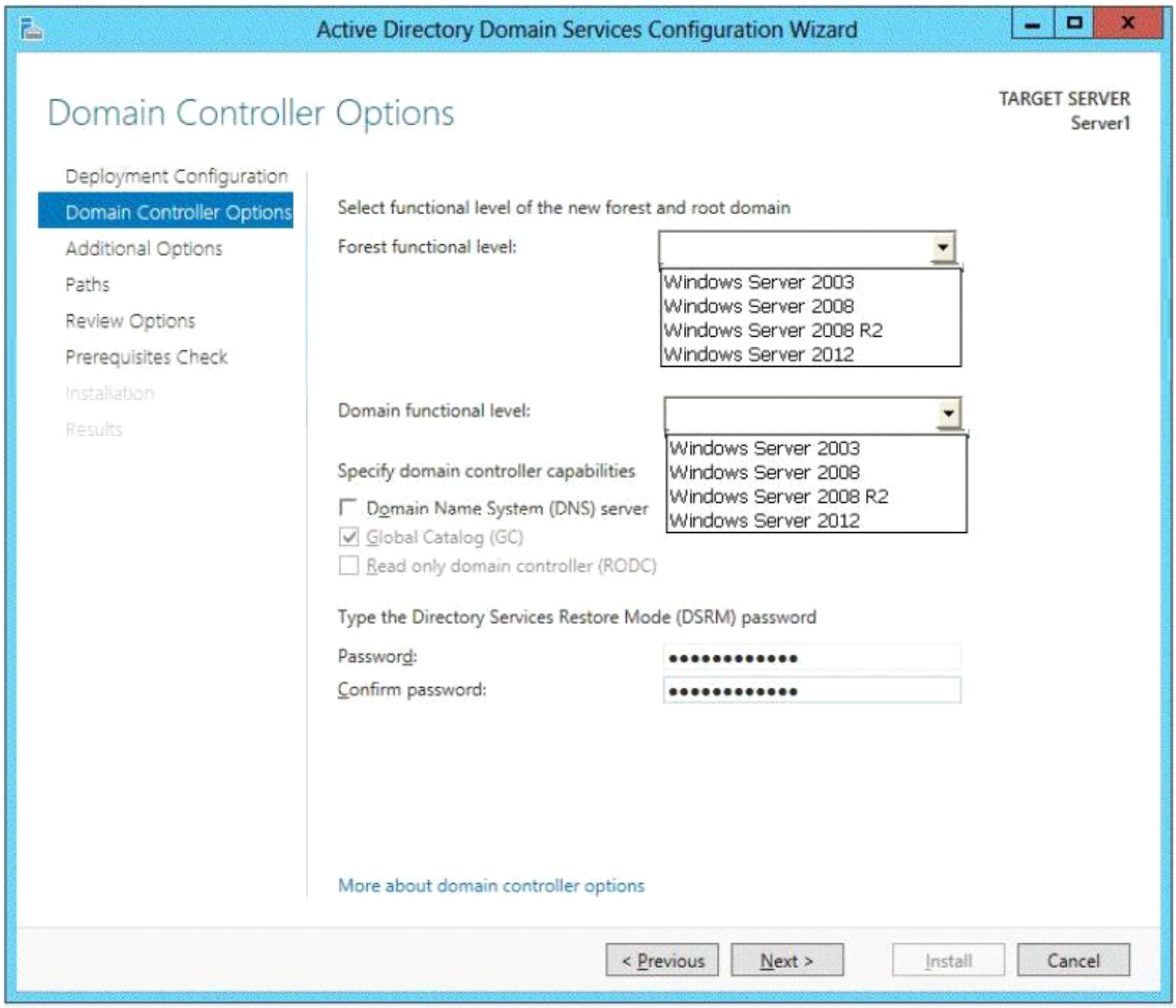
Explanation:
Security Considerations for Trusts
Need to gain access to the resources in contoso.com
Disabling SID Filter Quarantining on External Trusts
Although it reduces the security of your forest (and is therefore not recommended), you can disable SID filter quarantining for an external trust by using 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 them access to resources in the trusting domain based on the SID history attribute.
Etc.
Incorrect:
Not B. Enables administrators to manage Active Directory domains and trust relationships from the command prompt, /quarantine Sets or clears the domain quarantine.
Not D. Selective authentication over a forest trust restricts access to only those users in a trusted forest who have been explicitly given authentication permissions to computer objects (resource computers) that reside in the trusting forest.
Reference: Security Considerations for Trusts
http://technet.microsoft.com/en-us/library/cc755321(v=ws.10).aspx

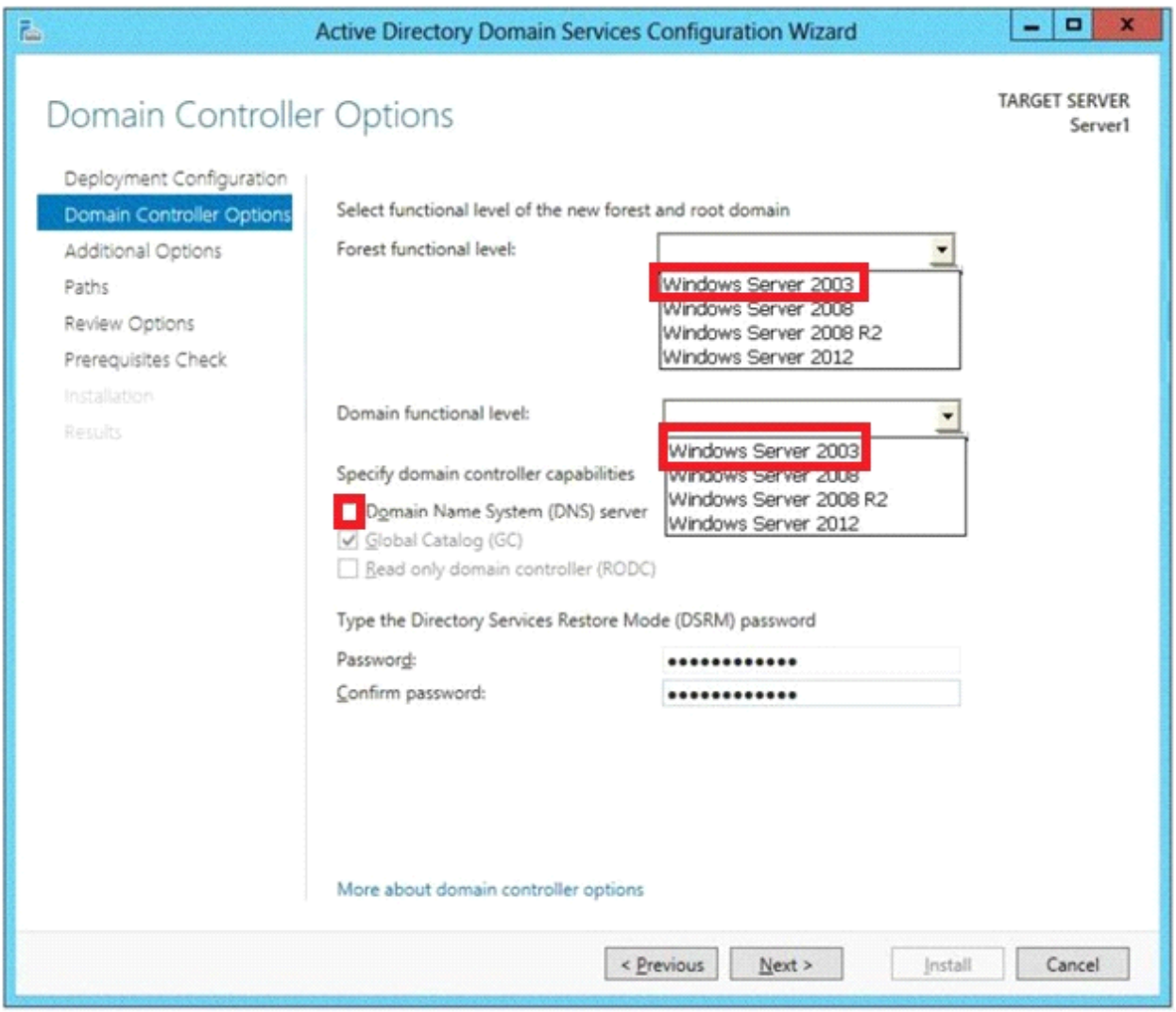
Question: 4

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
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
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
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
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

Answer:



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.
Reference: Understanding Active Directory Domain Services (AD DS) Functional Levels

Question: 5

Your network contains an Active Directory forest named adatum.com. The forest contains a single domain. The domain contains four servers. The servers are configured as shown in the following table.

Server name	Configuration	Operating system
DC1	• Global catalog server • Domain controller • Schema master • DNS server	Windows Server 2003 R2
DC2	• Domain controller • PDC emulator • DHCP server • DNS server	Windows Server 2003 R2
DC3	• Infrastructure master • Global catalog server • Domain controller • WINS server	Windows Server 2008 R2
Server1	• Member server • WINS server • DNS server	Windows Server 2003 R2

You need to update the schema to support a domain controller that will run Windows Server 2012 R2.
On which server should you run adprep.exe?

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

Answer: B

Explanation:
We must use the Windows Server 2008 R2 Server.
Upgrade Domain Controllers to Windows Server 2012 R2 and Windows Server 2012
You can use adprep.exe on domain controllers that run 64-bit versions of Windows Server 2008 or Windows Server 2008 R2 to upgrade to Windows Server 2012. You cannot upgrade domain controllers that run Windows Server 2003 or 32-bit versions of Windows Server 2008. To replace them, install domain controllers that run a later version of Windows Server in the domain, and then remove the domain controllers that Windows Server 2003.
Reference: Upgrade Domain Controllers to Windows Server 2012 R2 and Windows Server 2012, Supported in-place upgrade paths.
http://technet.microsoft.com/en-us/library/hh994618.aspx#BKMK_UpgradePaths

Question: 6

HOTSPOT
Your network contains three Active Directory forests. The forests are configured as shown in the following table.

Forest name	Forest functional level
Contoso.com	Windows Server 2012 R2
Division1.contoso.com	Windows Server 2012 R2
Dvision2.contoso.com	Windows Server 2012 R2

A two-way forest trust exists between contoso.com and divisionl.contoso.com. A two-way forest trust also exists between contoso.com and division2.contoso.com.
You plan to create a one-way forest trust from divisionl.contoso.com to division2.contoso.com.
You need to ensure that any cross-forest authentication requests are sent to the domain controllers in the appropriate forest after the trust is created.
How should you configure the existing forest trust settings?
In the table below, identify which configuration must be performed in each forest. Make only one selection in each column. Each correct selection is worth one point.

	Division1.contoso.com	Division2.contoso.com
Add division1.contoso.com as a name suffix routing entry.	○	○
Add division2.contoso.com as a name suffix routing entry.	○	○
Add division1.contoso.com as an exclusion to the name suffix routing entry of contoso.com.	○	○
Add division2.contoso.com as an exclusion to the name suffix routing entry of contoso.com.	○	○

Answer:

	Division1.contoso.com	Division2.contoso.com
Add division1.contoso.com as a name suffix routing entry.	○	●
Add division2.contoso.com as a name suffix routing entry.	○	○
Add division1.contoso.com as an exclusion to the name suffix routing entry of contoso.com.	○	○
Add division2.contoso.com as an exclusion to the name suffix routing entry of contoso.com.	●	○

Explanation:
There will be a one-way forest trust from division1.contoso.com to division2.contoso.com
Division1 trusts Division2. Division2 must be able to access resources in Division1.
Division1 should not be able to access resources in Division2.

Question: 7

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

Question: 8

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: A, D

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.

Question: 9

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains two domain controllers.
The domain controllers are configured as shown in the following table.

Domain controller name	Site name	Configuration
DC1	Main	Domain controller
DC10	Branch	Read-only domain controller (RODC)

You configure a user named User1 as a delegated administrator of DC10.
You need to ensure that User1 can log on to DC10 if the network link between the Main site and the Branch site fails.
What should you do?

A. Add User1 to the Domain Admins group.
B. On DC10, modify the User Rights Assignment in Local Policies.
C. Run repadmin and specify the /prp parameter.
D. On DC10, run ntdsutil and configure the settings in the Roles context.

Answer: C

Explanation:
repadmin /prp will allow the password caching of the local administrator to the RODC.
This command lists and modifies the Password Replication Policy (PRP) for read-only domain controllers (RODCs).
Reference: RODC Administration
https://technet.microsoft.com/en-us/library/cc755310%28v=ws.10%29.aspx

Question: 10

Your company has offices in Montreal, New York, and Amsterdam.
The network contains an Active Directory forest named contoso.com. An Active Directory site exists for each office. All of the sites connect to each other by using the DEFAULTIPSITELINK site link.
You need to ensure that only between 20:00 and 08:00, the domain controllers in the Montreal office replicate the Active Directory changes to the domain controllers in the Amsterdam office.
The solution must ensure that the domain controllers in the Montreal and the New York offices can replicate the Active Directory changes any time of day.
What should you do?

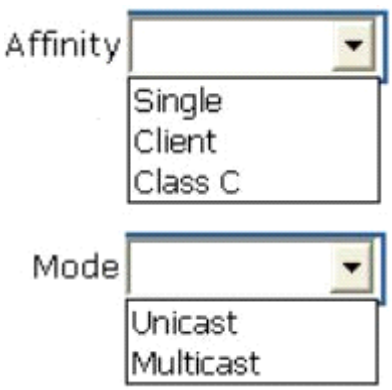
A. Create a new site link that contains Montreal and Amsterdam. Remove Amsterdam from DEFAULTIPSITE1INK. Modify the schedule of DEFAULTIPSITELINK.
B. Create a new site link that contains Montreal and Amsterdam. Create a new site link bridge. Modify the schedule of DEFAULTIPSITELINK.
C. Create a new site link that contains Montreal and Amsterdam. Remove Amsterdam from DEFAULTIPSITELINK. Modify the schedule of the new site link.
D. Create a new site link that contains Montreal and Amsterdam. Create a new site link bridge. Modify the schedule of the new site link.

Answer: C

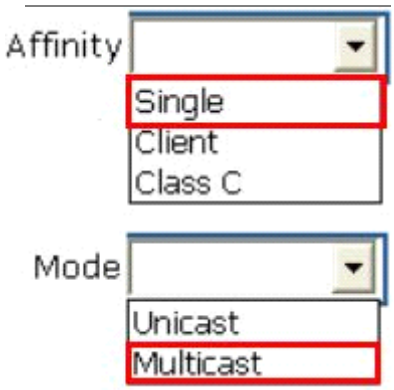
Explanation:
We create a new site link between Montreal and Amsterdam and schedule it only between 20:00 and 08:00. To ensure that traffic between Montreal and Amsterdam only occurs at this time we also remove Amsterdam from the DEFAULTIPSITELINK.
Reference: How Active Directory Replication Topology Works
http://technet.microsoft.com/en-us/library/cc755994(v=ws.10).aspx

Question: 11

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.



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.
Reference: Network Load Balancing Manager Properties
https://technet.microsoft.com/en-us/library/cc771709.aspx

Question: 12

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 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

Question: 13

Your network contains two servers named HV1 and HV2. Both servers run Windows Server 2012 R2 and have the Hyper-V server role installed.
HV1 hosts 25 virtual machines. The virtual machine configuration files and the virtual hard disks are stored in D:\VM.
You shut down all of the virtual machines on HV1.
You copy D:\VM to D:\VM on HV2.
You need to start all of the virtual machines on HV2. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Run the Import-VMInitialReplication cmdlet.
B. From HV1, export all virtual machines to D:\VM. Copy D:\VM to D:\VM on HV2 and overwrite the existing files. On HV2, run the Import Virtual Machine wizard.
C. From HV1, export all virtual machines to D:\VM. Copy D:\VM to D:\VM on HV2 and overwrite the existing files. On HV2, run the New Virtual Machine wizard.
D. Run the Import-VM cmdlet.

Answer: D

Explanation:
Import-VM
Imports a virtual machine from a file.
Example
Imports the virtual machine from its configuration file. The virtual machine is registered in-place, so its files are not copied.
Windows PowerShell
PS C:\> Import-VM –Path 'D:\Test\VirtualMachines\5AE40946-3A98-428E-8C83-081A3C6BD18C.XML'
Reference: Import-VM

Question: 14

HOTSPOT

Your network contains two Hyper-V hosts that are configured as shown in the following table.

Host name	Configuration
Server1	• 1 Intel i7 processor • 16 GB of memory • 1 TB of hard disk space • Two network adapters
Server2	• 4 Intel Xeon processors • 64 GB of memory • 4 TB of hard disk space • 4 network adapters

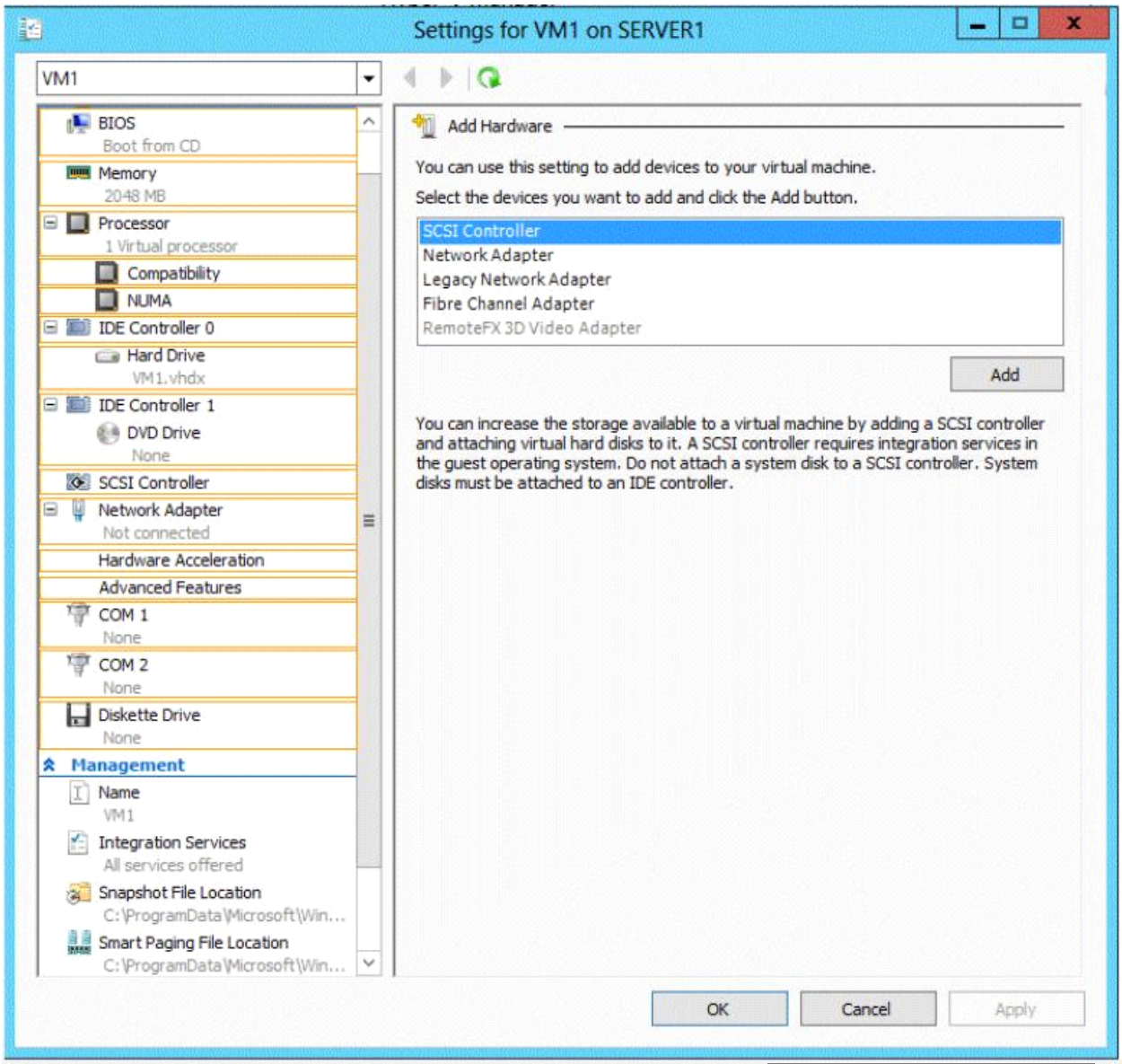
You create a virtual machine on Server1 named VM1.

You plan to export VM1 from Server1 and import VM1 to Server2.

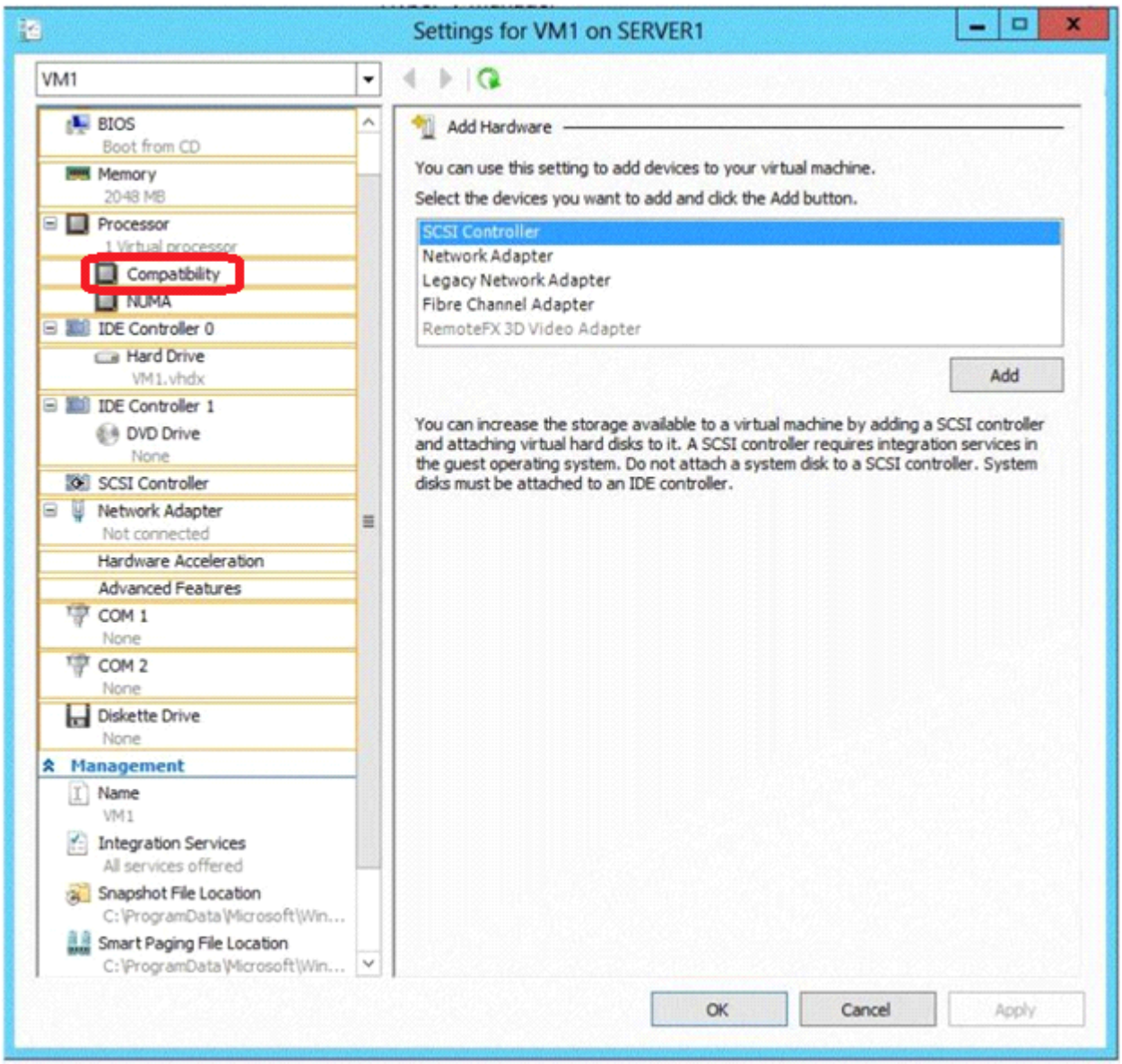
You need to ensure that you can start the imported copy of VM1 from snapshots.

What should you configure on VM1?

To answer, select the appropriate node in the answer area.


Settings for VM1 on SERVER1
VM1
BIOS
Boot from CD
Memory
2048 MB
Processor
1 Virtual processor
Compatibility
NUMA
IDE Controller 0
Hard Drive
VM1.vhdx
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
Not connected
Hardware Acceleration
Advanced Features
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
VM1
Integration Services
All services offered
Snapshot File Location
C:\ProgramData\Microsoft\Win...
Smart Paging File Location
C:\ProgramData\Microsoft\Win...
Add Hardware
You can use this setting to add devices to your virtual machine.
Select the devices you want to add and click the Add button.
SCSI Controller
Network Adapter
Legacy Network Adapter
Fibre Channel Adapter
RemoteFX 3D Video Adapter
Add
You can increase the storage available to a virtual machine by adding a SCSI controller and attaching virtual hard disks to it. A SCSI controller requires integration services in the guest operating system. Do not attach a system disk to a SCSI controller. System disks must be attached to an IDE controller.
OK
Cancel
Apply

Answer:



Note:

* If the CPUs are from the same manufacturer but not from the same type, you may need to use Processor Compatibility.

(Incorrect) The network adapter is already disconnected.

Question: 15

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.

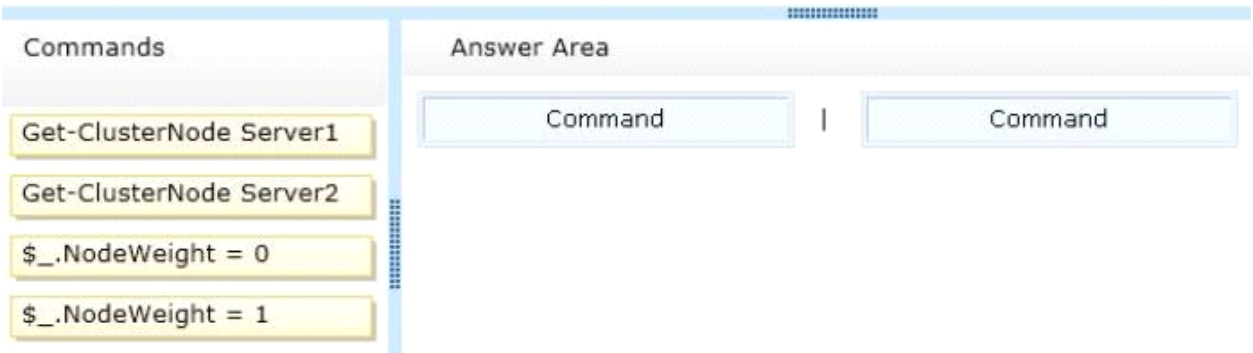
Server1 and Server2 are located in a site named Site1. Server3 and Server4 are located in a site named Site2. The servers are configured as nodes in a failover cluster named Cluster1.

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.



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
Reference: Configure Cluster Quorum NodeWeight Settings

Question: 16

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 cluster disk resource.
A developer creates an application named App1. App1 is NOT a cluster-aware application. App1 runs as a service. App1 stores date on the cluster disk resource.
You need to ensure that App1 runs in Cluster1. The solution must minimize development effort.
Which cmdlet should you run?

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

Answer: B

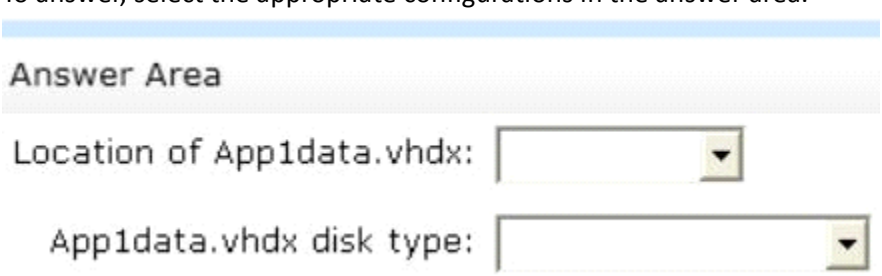
Explanation:
Add-ClusterGenericApplicationRole

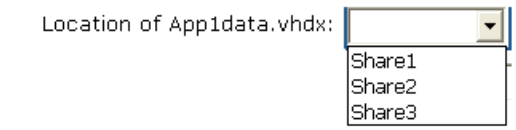
Configure high availability for an application that was not originally designed to run in a failover cluster.
If you run an application as a Generic Application, the cluster software will start the application, then periodically query the operating system to see whether the application appears to be 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

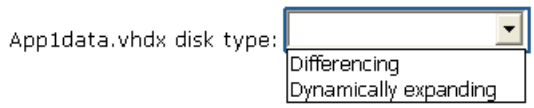
This command configures NewApplication.exe as a generic clustered application. A default name will be used for client access and this application requires no storage.
Reference: Add-ClusterGenericApplicationRole
http://technet.microsoft.com/en-us/library/ee460976.aspx

Question: 17

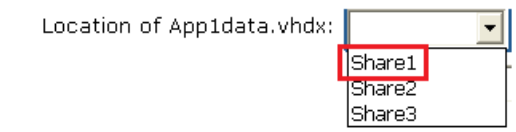
HOTSPOT
Your network contains an Active Directory domain named contoso.com.
You have a failover cluster named Cluster1 that contains two nodes named Server1 and Server2. Both servers run Windows Server 2012 R2 and have the Hyper-V server role installed.
You plan to create two virtual machines that will 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.

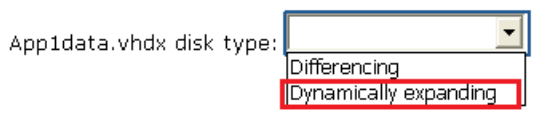






Answer:

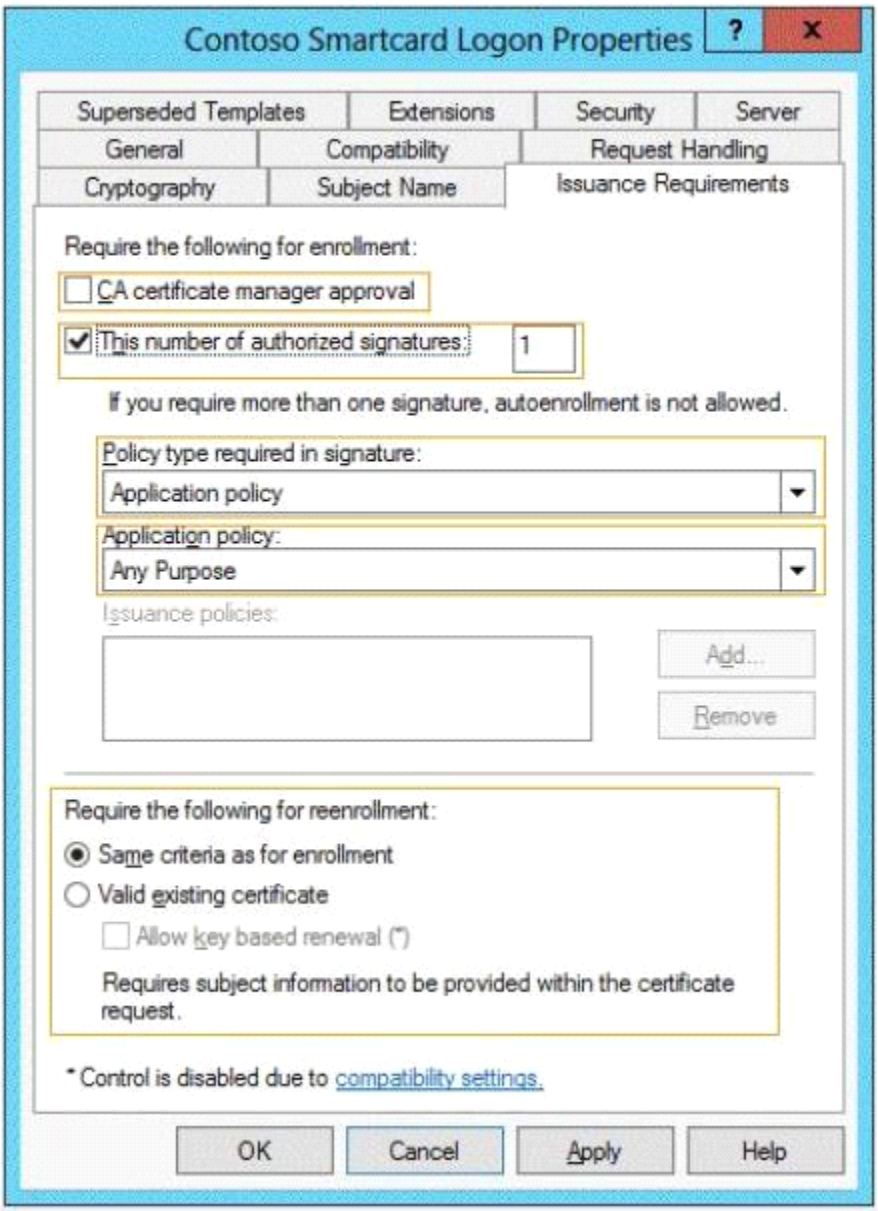




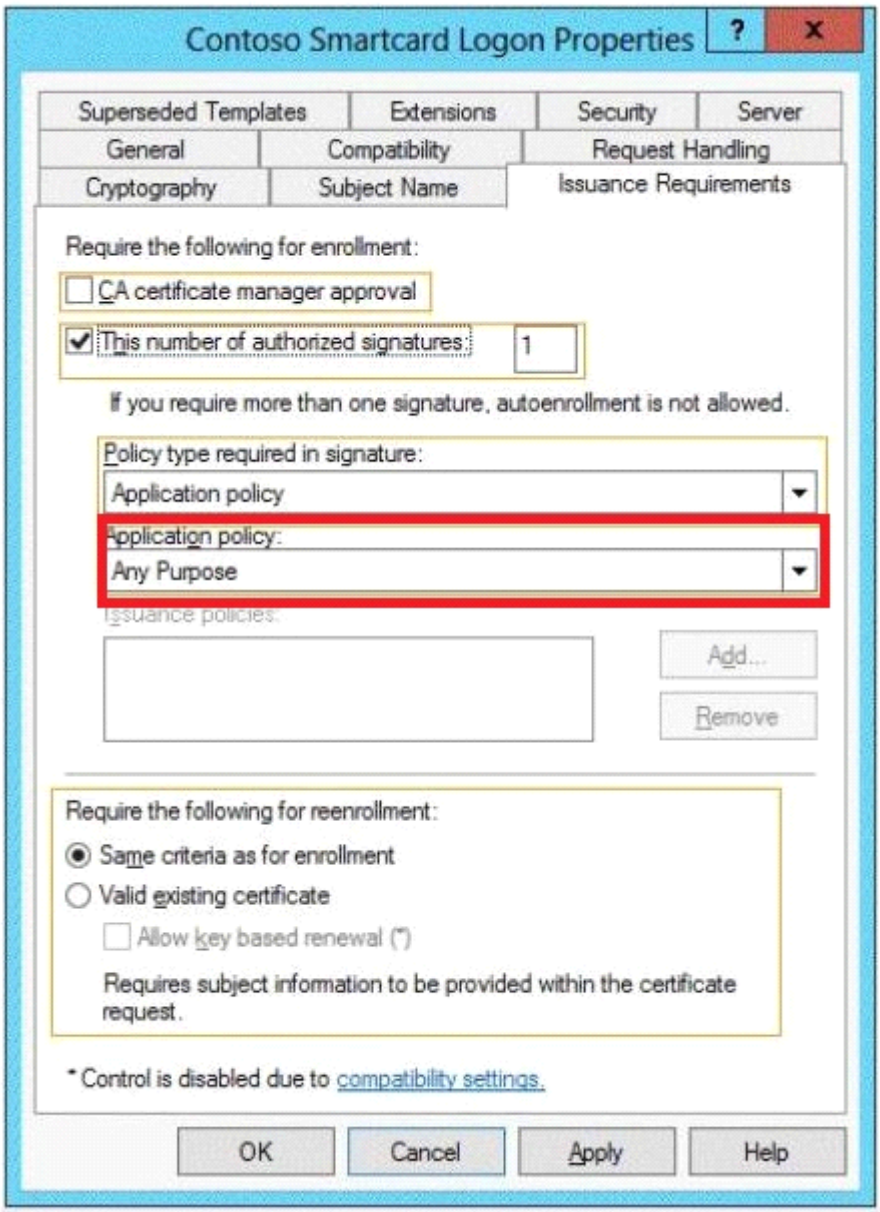
Explanation:
* Simultaneous access to vhd can only be done by scale-out file server
* Create your VHDX data files to be shared as fixed-size or dynamically expanding, on the disk where you manually attached the Shared VHDX filter. Old VHD files are not allowed. Differencing disks are not allowed.
Reference: Windows Server 2012 R2 Storage: Step-by-step with Storage Spaces, SMB Scale-Out and Shared VHDX (Virtual)

Question: 18

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.


Contoso Smartcard Logon Properties
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Subject Name
Issuance Requirements
Require the following for enrollment:
CA certificate manager approval
This number of authorized signatures:
1
If you require more than one signature, autoenrollment is not allowed.
Policy type required in signature:
Application policy
Application policy:
Any Purpose
Issuance policies:
Add...
Remove
Require the following for reenrollment:
Same criteria as for enrollment
Valid existing certificate
Allow key based renewal (*)
Requires subject information to be provided within the certificate request.
* Control is disabled due to compatibility settings.
OK
Cancel
Apply
Help

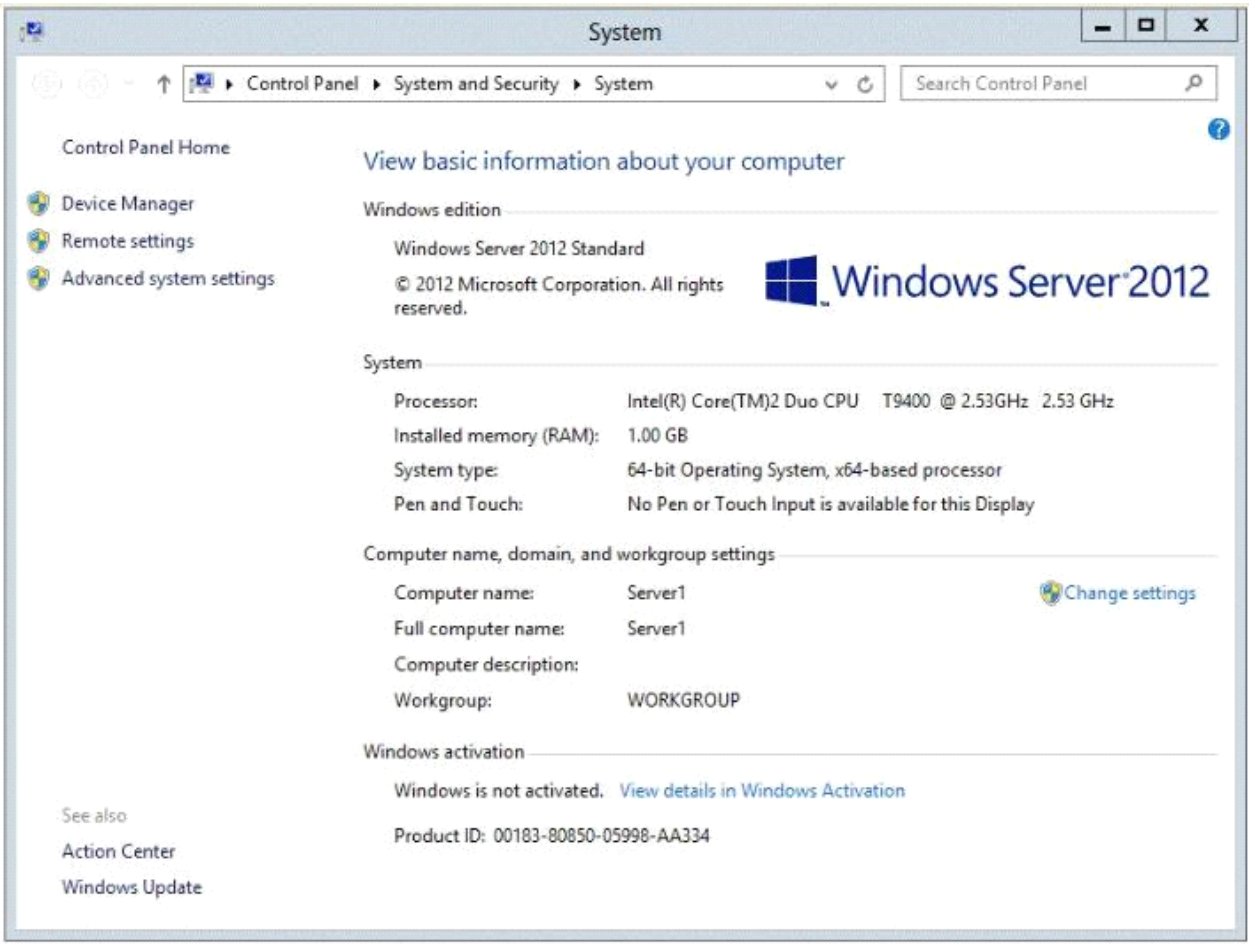
Answer:



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.
Reference: Administering Certificate Templates
http://technet.microsoft.com/en-us/library/cc725621(v=WS.10).aspx

Question: 19

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.)

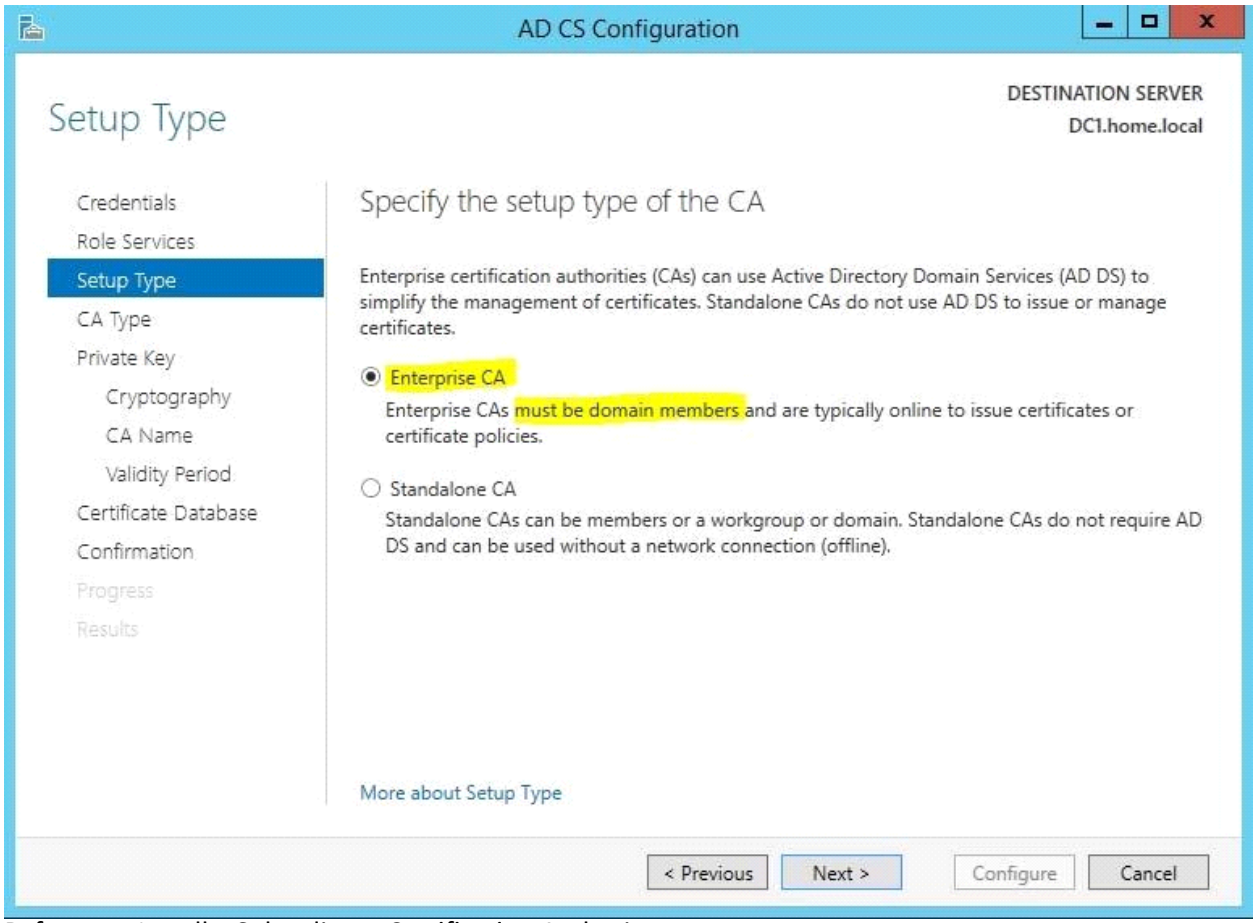


You need to configure Server1 as an enterprise subordinate certification authority (CA).
What should you do first?

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.



Reference: Install a Subordinate Certification Authority

Question: 20

Your network contains a perimeter network and an internal network. The internal network contains an Active Directory Federation Services (AD FS) 2.1 infrastructure. The infrastructure uses Active Directory as the attribute store.
You plan to deploy a federation server proxy to a server named Server2 in the perimeter network.
You need to identify which value must be included in the certificate that is deployed to Server2.
What should you identify?

A. The FQDN of the AD FS server
B. The name of the Federation Service
C. The name of the Active Directory domain
D. The public IP address of Server2

Answer: A

Explanation:
To add a host (A) record to corporate DNS for a federation server
On a DNS server for the corporate network, open the DNS snap-in.
1. In the console tree, right-click the applicable forward lookup zone, and then click New Host (A).

2. In Name, type only the computer name of the federation server or federation server cluster (for example, type fs for the fully qualified domain name (FQDN) fs.adatum.com).
3. In IP address, type the IP address for the federation server or federation server cluster (for example, 192.168.1.4).
4. Click Add Host.
Reference: Add a host (A) record to corporate DNS for a federation server
http://technet.microsoft.com/en-us/library/cc776786(v=ws.10).aspx

Question: 21

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?

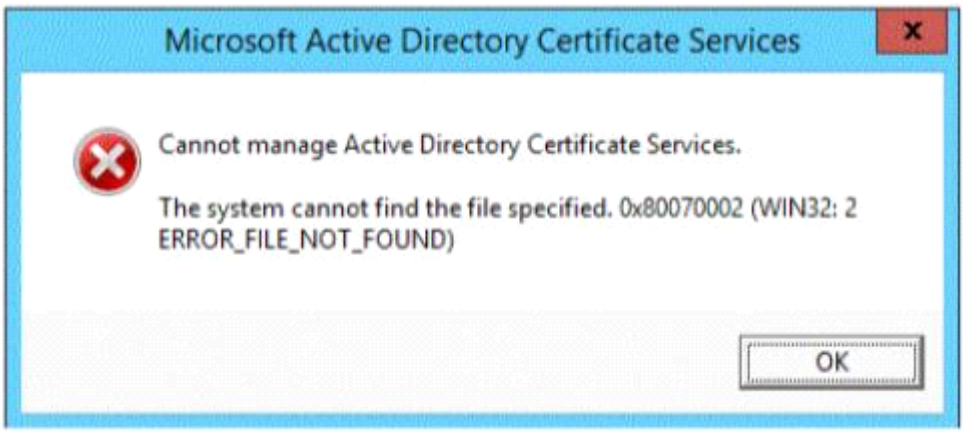
A. Modify the Service Connection Point (SCP).
B. Configure the Group Policy object (GPO) settings of the users in the west.contoso.com domain.
C. Configure the Group Policy object (GPO) settings of the users in the east.contoso.com domain.
D. Modify the properties of the AD RMS cluster in west.contoso.com.

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

Question: 22

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.

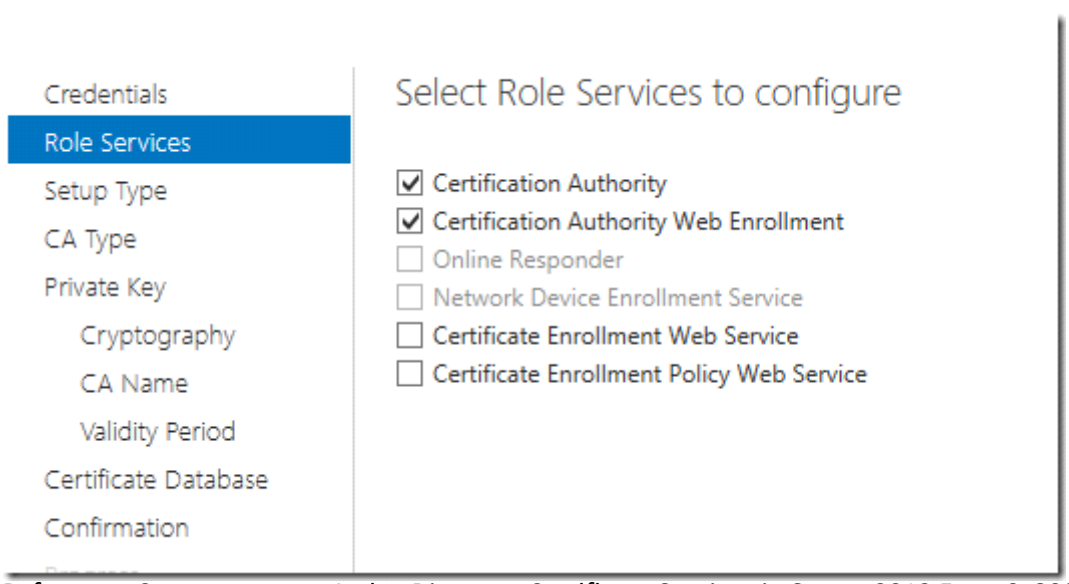


You need to ensure that when Admin1 opens the Certification Authority console on Server1, the error message does not appear.
What should you do?

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

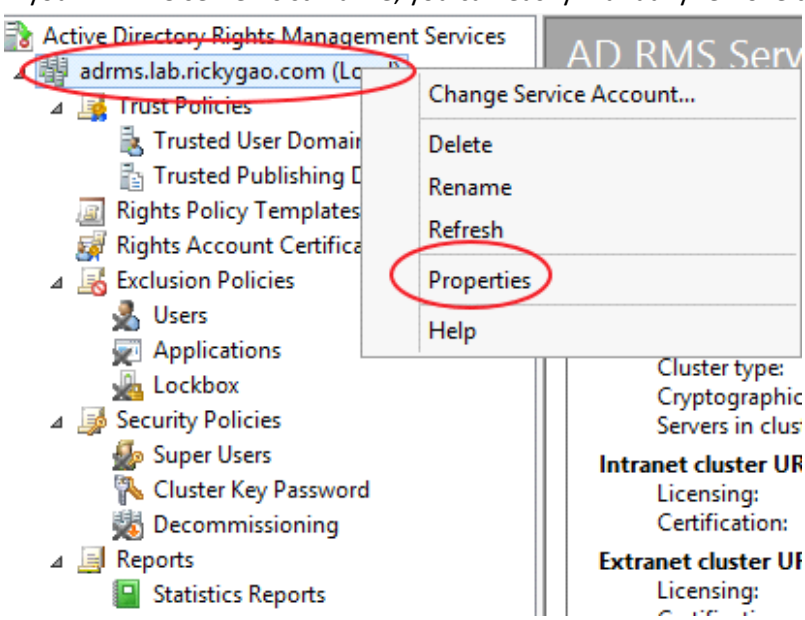
Question: 23

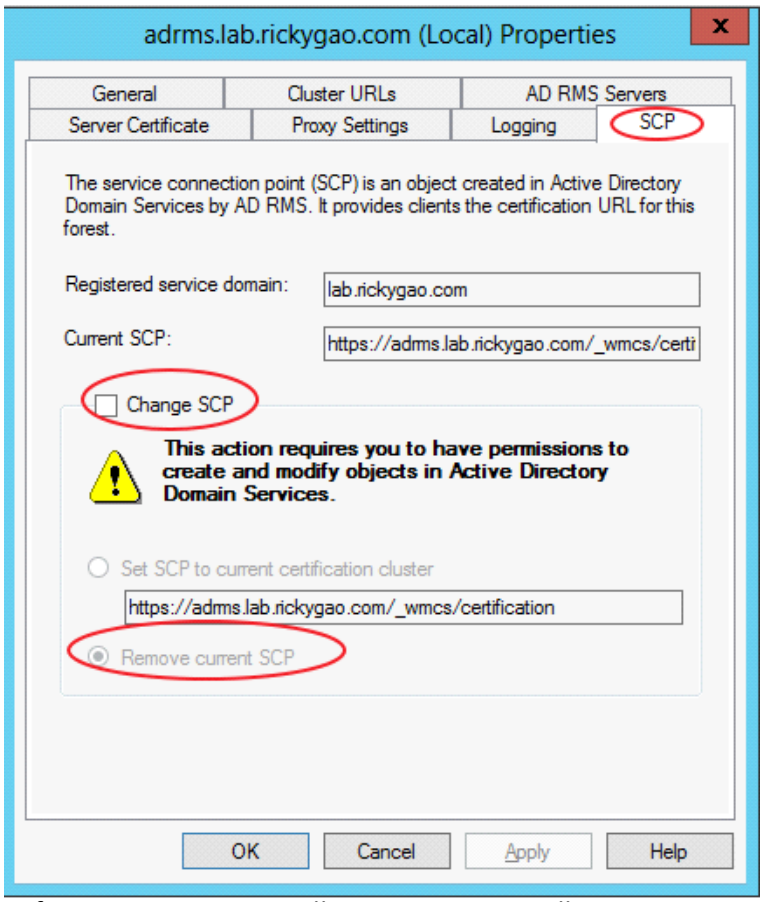
Your network contains an Active Directory domain named contoso.com.
A previous administrator implemented a Proof of Concept installation of Active Directory Rights Management Services (AD RMS).
After the proof of concept was complete, the Active Directory Rights Management Services server role was removed.
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:





Reference: How to manually remove or reinstall ADRMS

Question: 24

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.

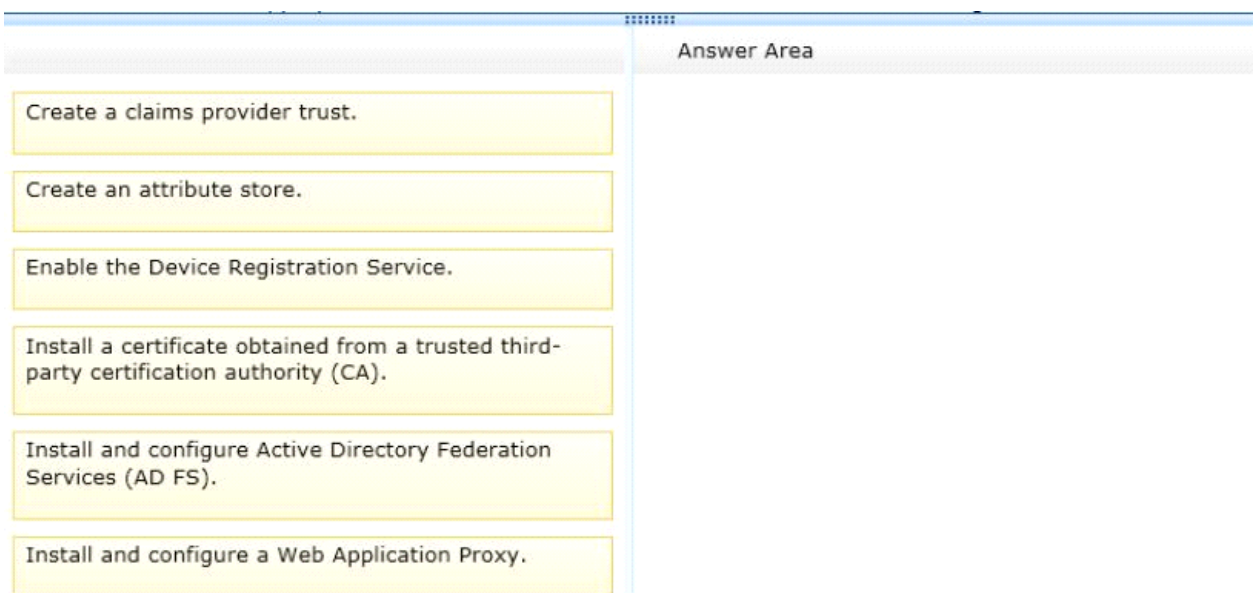
Answer: C, E

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.

Question: 25

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:

Box 1:
Install a certificate obtained from a trusted third-party certification authority (CA).
Box 2:
Install and configure Active Directory Federation Services (AD FS).
Box 3:

Enable the Device Registration Service.

Box 4:

Install and configure a Web Application Proxy.

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.

Reference: Deploying a Federation Server Farm.

Thank You For Trying 70-412 PDF Demo

To try our 70-412 Premium Files visit link below:

https://examsland.com/latest-exam-questions/70-412/

Start Your 70-412 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.