Microsoft

Exam Questions 70-411

Administering Windows Server 2012

NEW QUESTION 1
Your network contains a Hyper-V host named Hyperv1. Hyperv1 runs Windows Server 2012 R2.
Hyperv1 hosts four virtual machines named VM1, VM2, VM3, and VM4. AH of the virtual machines run Windows Server 2008 R2.
You need to view the amount of memory resources and processor resources that VM4 currently uses.
Which tool should you use on Hyperv1?

A. Windows System Resource Manager (WSRM)
B. Task Manager
C. Hyper-V Manager
D. Resource Monitor

Answer: C

**Explanation:** Hyper-V Performance Monitoring Tool
Know which resource is consuming more CPU. Find out if CPUs are running at full capacity or if they are being underutilized. Metrics tracked include Total CPU utilization, Guest CPU utilization, Hypervisor CPU utilization, idle CPU utilization, etc.
WSRM is deprecated starting with Windows Server 2012
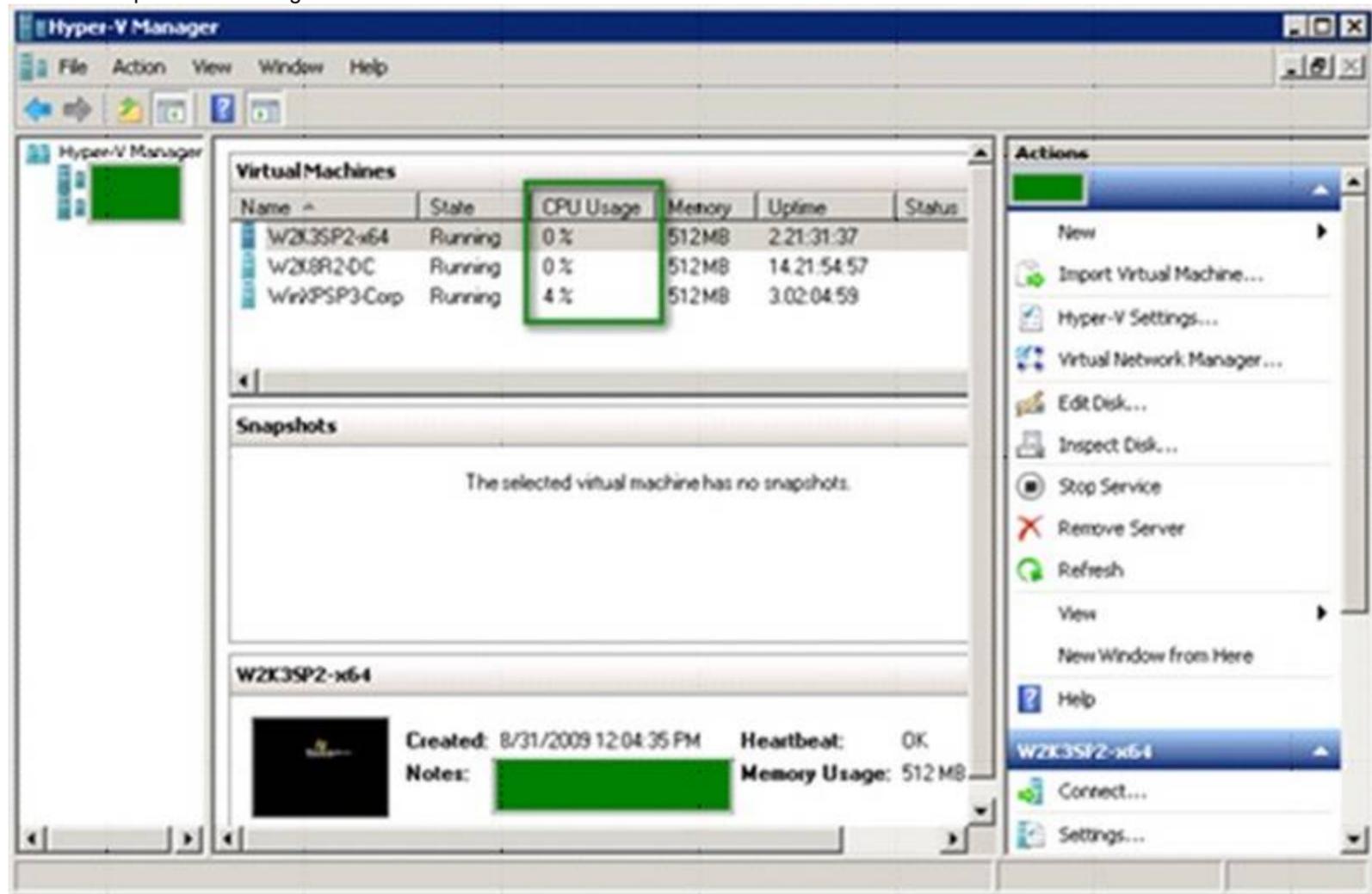
NEW QUESTION 2
HOTSPOT
Your network contains an Active Directory domain named contoso.com.
All DNS servers host a DNS zone named adatum.com. The adatum.com zone is not Active Directory-integrated.
An administrator modifies the start of authority (SOA) record for the adatum.com zone. After the modification, you discover that when you add or modify DNS records in the
adatum.com zone, the changes are not transferred to the DNS servers that host secondary
copies of the adatum.com zone.
You need to ensure that the records are transferred to all the copies of the adatum.com zone.
What should you modify in the SOA record for the adatum.com zone? To answer, select the appropriate setting in the answer area.
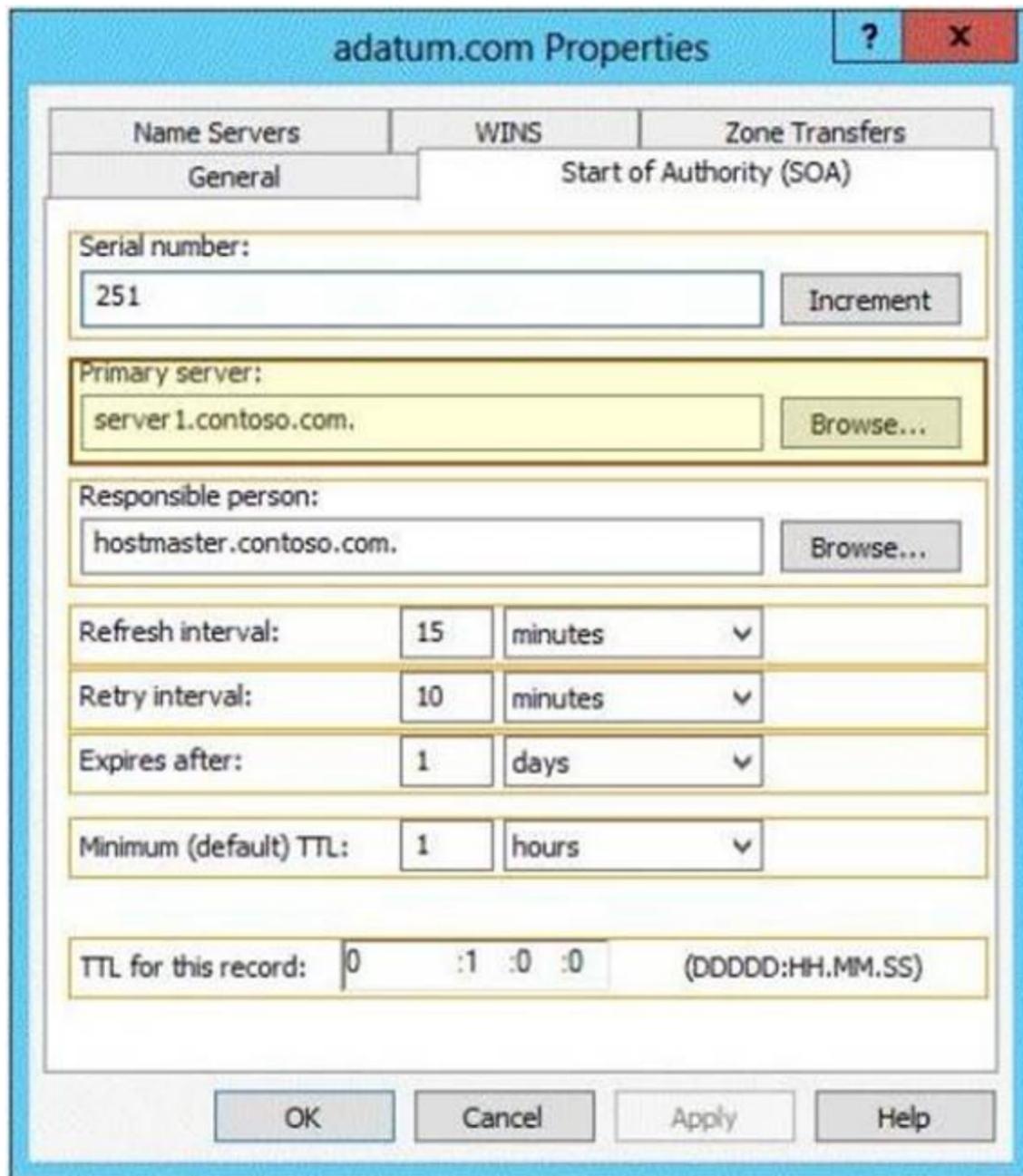
Answer:

Explanation: When a DNS server receives an update through Active Directory replication:
If the serial number of the replicated record is higher than the serial number in the SOA record of the local copy of the zone, the local zone serial number is set to the serial number in the replicated record.
Note Each DNS record in the zone has a copy of the zone serial number at the time when the record was last modified.
If the serial number of the replicated record is the same or lower than the local serial number, and if the local DNS server is configured not to allow zone transfer of the zone, the local zone serial number is not changed.
If the serial number of the replicated record is the same or lower than the local zone serial number, if the DNS server is configured to allow a zone transfer of the zone, and if the local
zone serial number has not been changed since the last zone transfer occurred to a remote DNS server, then the local zone serial number will be incremented.
Otherwise that is if a copy of the zone with the current local zone serial number has not been transferred to a remote DNS server, the local zone serial number is not changed.

NEW QUESTION 3
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2008 R2.
You plan to test Windows Server 2012 R2 by using native-boot virtual hard disks (VHDs). You attach a new VHD to Server1.
You need to install Windows Server 2012 R2 in the VHD. What should you do?

A. Run imagex.exe and specify the /append parameter.
B. Run dism.exe and specify the /apply-image parameter.
C. Run imagex.exe and specify the /export parameter.
D. Run dism.exe and specify the /append-image parameter.

Answer: B

Explanation: On the destination computer, you will create a structure for the partitions where you apply your images. The partition structure on the destination computer must match the partition structure of the reference computer. If you apply an image to a volume with an existing Windows installation, files from the previous installation may not be deleted. Format the volume by using a tool such as DiskPart before applying the new image.

NEW QUESTION 4
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs.
You have two GPOs linked to an organizational unit (OU) named OU1. You need to change the precedence order of the GPOs.
What should you use?

A. Dcgpofix
B. Get-GPOReport
C. Gpfixup
D. Gpresult
E. Gpedi
F. msc
G. Import-GPO
H. Restore-GPO
I. Set-GPInheritance
J. Set-GPLink
K. Set-GPPermission
L. Gpupdate
M. Add-ADGroupMember

Answer: I

Explanation: The Set-GPLinkcmdlet sets the properties of a GPO link. You can set the following properties:
? Enabled. If the GPO link is enabled, the settings of the GPO are applied when
Group Policy is processed for the site, domain or OU.
? Enforced. If the GPO link is enforced, it cannot be blocked at a lower-level (in the Group Policy processing hierarchy) container.
? Order. The order specifies the precedence that the settings of the GPO take over conflicting settings in other GPOs that are linked (and enabled) to the same site, domain, or OU.
Reference: http: //technet. microsoft. com/en-us/library/ee461022. aspx

NEW QUESTION 5
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains servers named Server1 and Server2. Both servers have the DFS Replication role service installed.
You need to configure the DFS Replication environment to meet the following requirements:
? Increase the quota limit of the staging folder.
? Configure the staging folder cleanup process to provide the highest amount of free space possible.
Which cmdlets should you use to meet each requirement? To answer, select the appropriate options in the answer area.

Answer Area

Increase the quota limit of the staging folder. [▼]

Configure the staging folder cleanup process to provide the highest amount of free space possible. [▼]

Answer Area

Increase the quota limit of the staging folder. [▼]
Set-DfsrGroupSchedule
Set-DfsrMembership
Set-DfsrReplicatedFolder
Set-DfsrServiceConfiguration

Configure the staging folder cleanup process to provide the highest amount of free space possible. [▼]
Set-DfsrGroupSchedule
Set-DfsrMembership
Set-DfsrReplicatedFolder
Set-DfsrServiceConfiguration

Answer:

Explanation:

Answer Area

Increase the quota limit of the staging folder.

▼

Set-DfsrGroupSchedule
Set-DfsrMembership
Set-DfsrReplicatedFolder
Set-DfsrServiceConfiguration

Configure the staging folder cleanup process to provide the highest amount of free space possible.

▼

Set-DfsrGroupSchedule
Set-DfsrMembership
Set-DfsrReplicatedFolder
Set-DfsrServiceConfiguration

NEW QUESTION 6
Your company has a main office and two branch offices. The main office is located in New York. The branch offices are located in Seattle and Chicago.
The network contains an Active Directory domain named contoso.com. An Active Directory site exists for each office. Active Directory site links exist between the main office and the branch offices. All servers run Windows Server 2012 R2.
The domain contains three file servers. The file servers are configured as shown in the following table.

Server name	Server location
NYC-SVR1	New York office
SEA-SVR1	Seattle office
CHI-SVR1	Chicago office

You implement a Distributed File System (DFS) replication group named ReplGroup. ReplGroup is used to replicate a folder on each file server. ReplGroup uses a hub and
spoke topology. NYC-SVR1 is configured as the hub server. You need to ensure that replication can occur if NYC-SVR1 fails.
What should you do?

A. Create an Active Directory site link bridge.
B. Create an Active Directory site link.
C. Modify the properties of Rep1Group.
D. Create a connection in Rep1Group.

Answer: D

Explanation: Unsure about this answer. D:
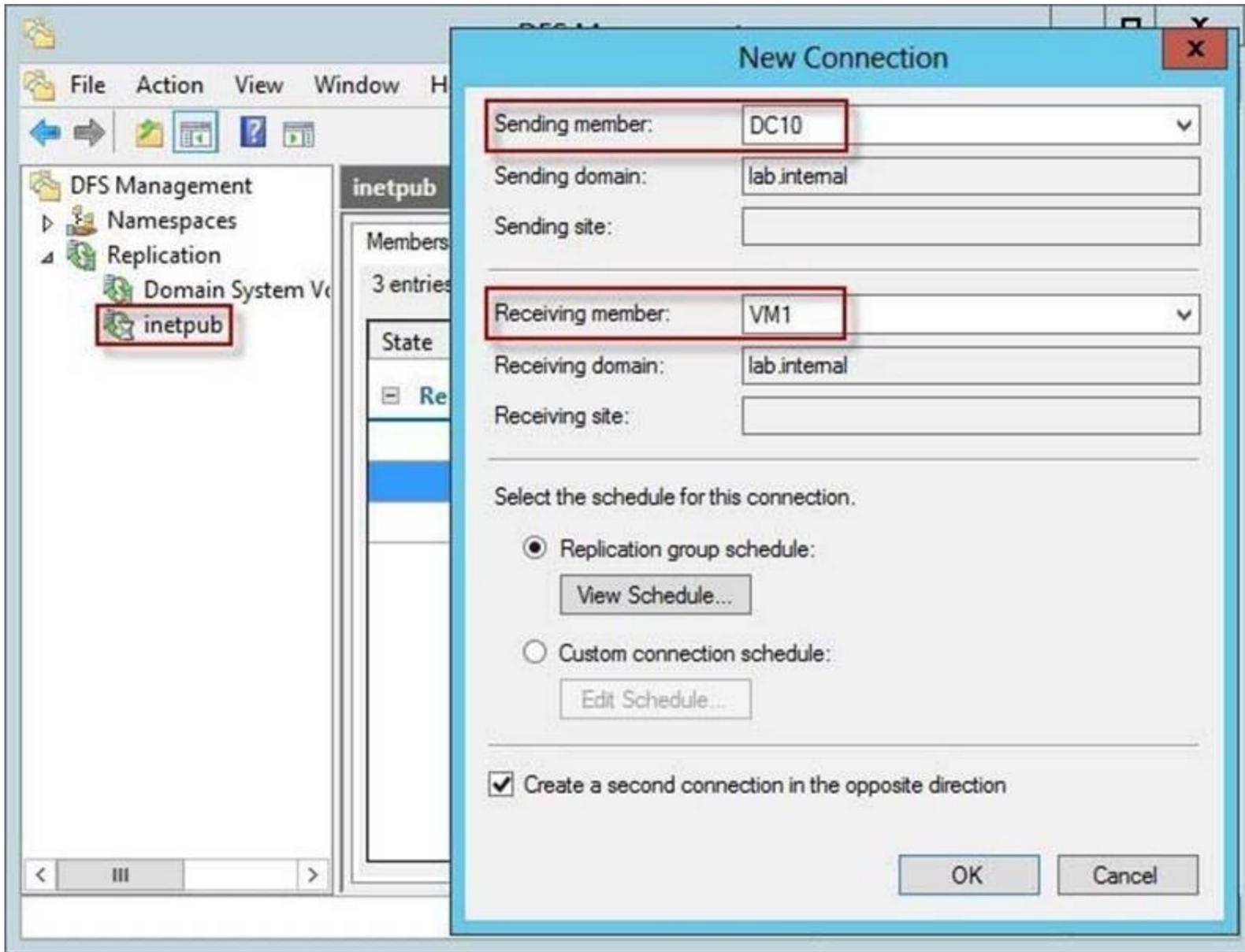
A:
The Bridge all site links option in Active Directory must be enabled. (This option is available in the Active Directory Sites and Services snap-in.) Turning off Bridge all site links can affect the ability of DFS to refer client computers to target computers that have the least expensive connection cost. An Intersite Topology Generator that is running Windows Server 2003 relies on the Bridge all site links option being enabled to generate the intersite cost matrix that DFS requires for its site-costing functionality. If you turn off this option, you must create site links between the Active Directory sites for which you want DFS to
calculate accurate site costs.
Any sites that are not connected by site links will have the maximum possible cost. For more information about site link bridging, see "Active Directory Replication Topology Technical Reference."

Reference:
http: //faultbucket. ca/2012/08/fixing-a-dfsr-connection-problem/
http: //faultbucket. ca/2012/08/fixing-a-dfsr-connection-problem/
http: //technet. microsoft. com/en-us/library/cc771941. aspx
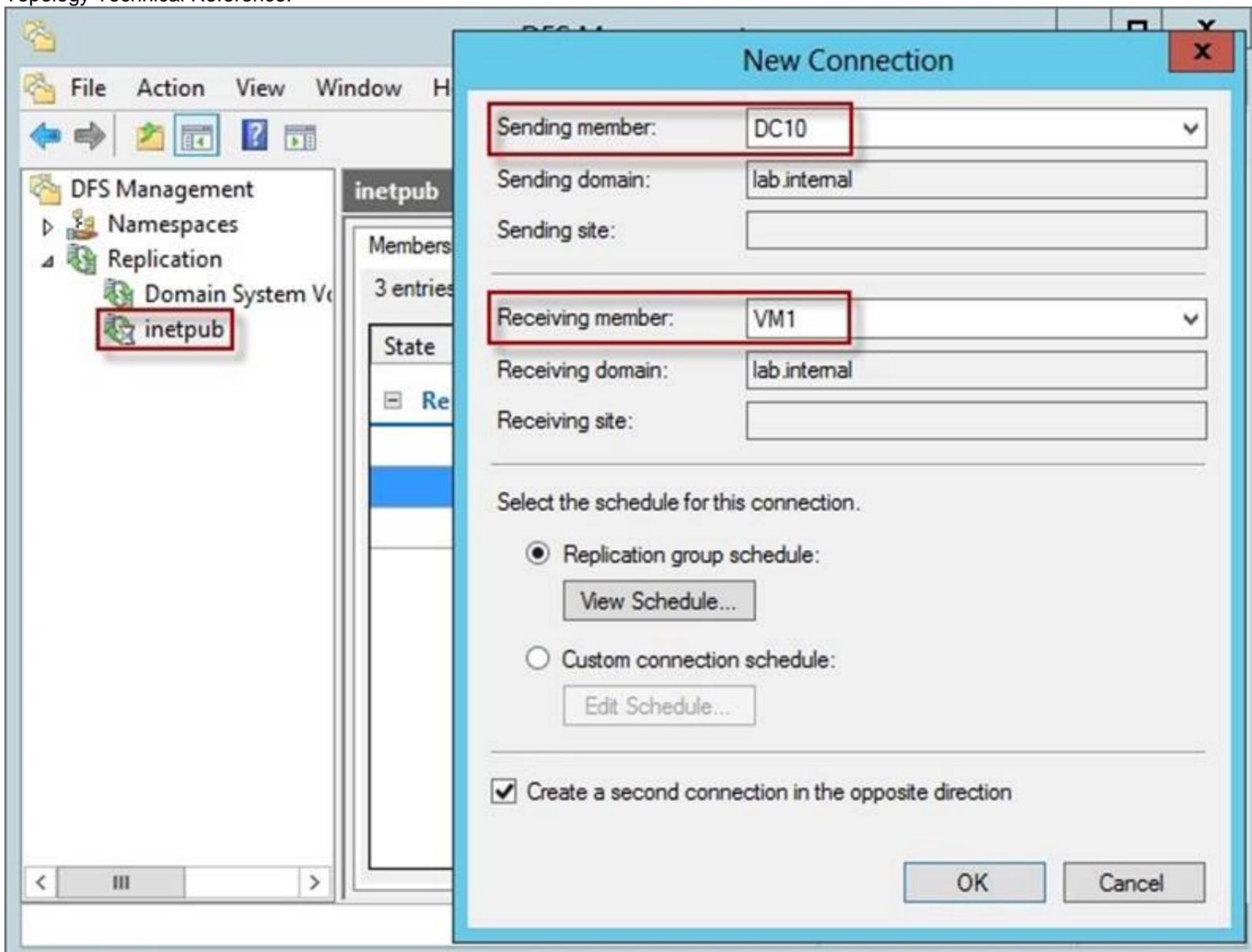
NEW QUESTION 7
Your network contains two DNS servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 hosts a primary zone for contoso.com. Server2 hosts a secondary zone for contoso.com.
You need to ensure that Server2 replicates changes to the contoso.com zone every five minutes.
Which setting should you modify in the start of authority (SOA) record?

A. Retry interval
B. Expires after
C. Minimum (default) TTL
D. Refresh interval

Answer: D

Explanation: By default, the refresh interval for each zone is set to 15 minutes. The refresh interval is used to determine how often other DNS servers that load and host the zone must attempt to renew the zone.
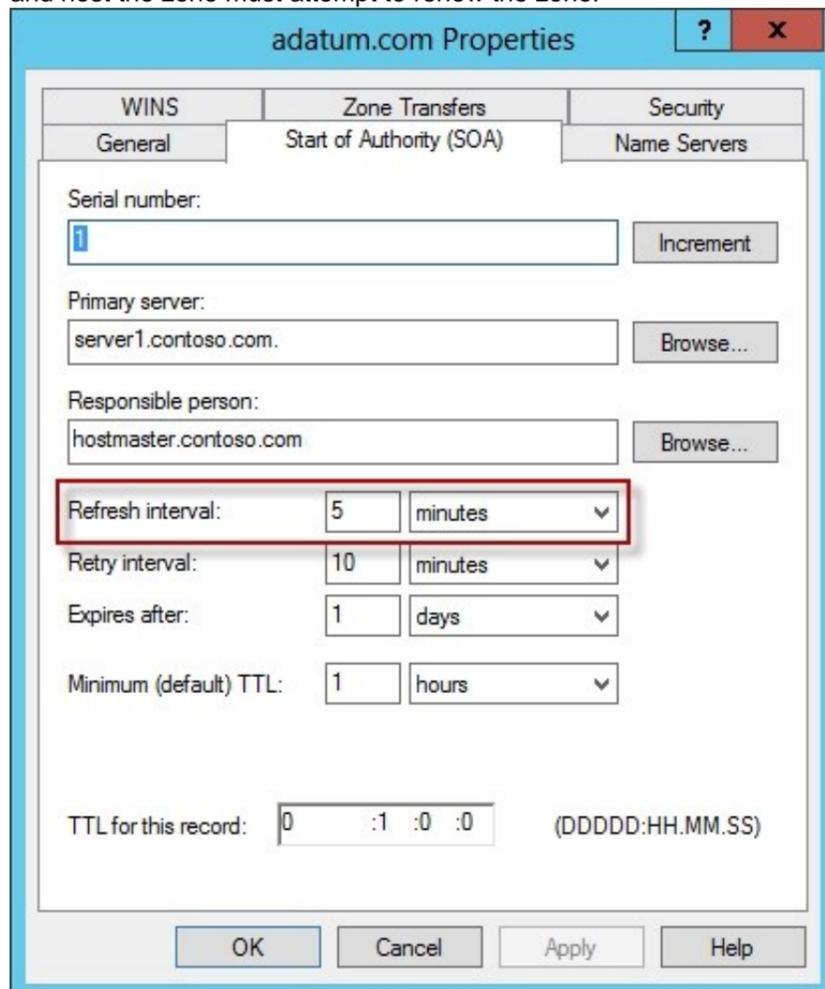
NEW QUESTION 8
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs.
The domain is renamed to adatum.com. Group Policies no longer function correctly.
You need to ensure that the existing GPOs are applied to users and computers. You want to achieve this goal by using the minimum amount of administrative effort.
What should you use?

A. Dcgpofix
B. Get-GPOReport
C. Gpfixup
D. Gpresult
E. Gpedi
F. msc
G. Import-GPO
H. Restore-GPO
I. Set-GPInheritance
J. Set-GPLink
K. Set-GPPermission
L. Gpupdate
M. Add-ADGroupMember

Answer: C

Explanation: You can use the gpfixup command-line tool to fix the dependencies that Group Policy objects (GPOs) and Group Policy links in Active Directory Domain Services (AD DS) have on Domain Name System (DNS) and NetBIOS names after a domain rename operation.
Reference: http: //technet. microsoft. com/en-us/library/hh852336(v=ws. 10). aspx

NEW QUESTION 9

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2. Server1 has a share named Share1.

When users without permission to Share1 attempt to access the share, they receive the Access Denied message as shown in the exhibit. (Click the Exhibit button.)
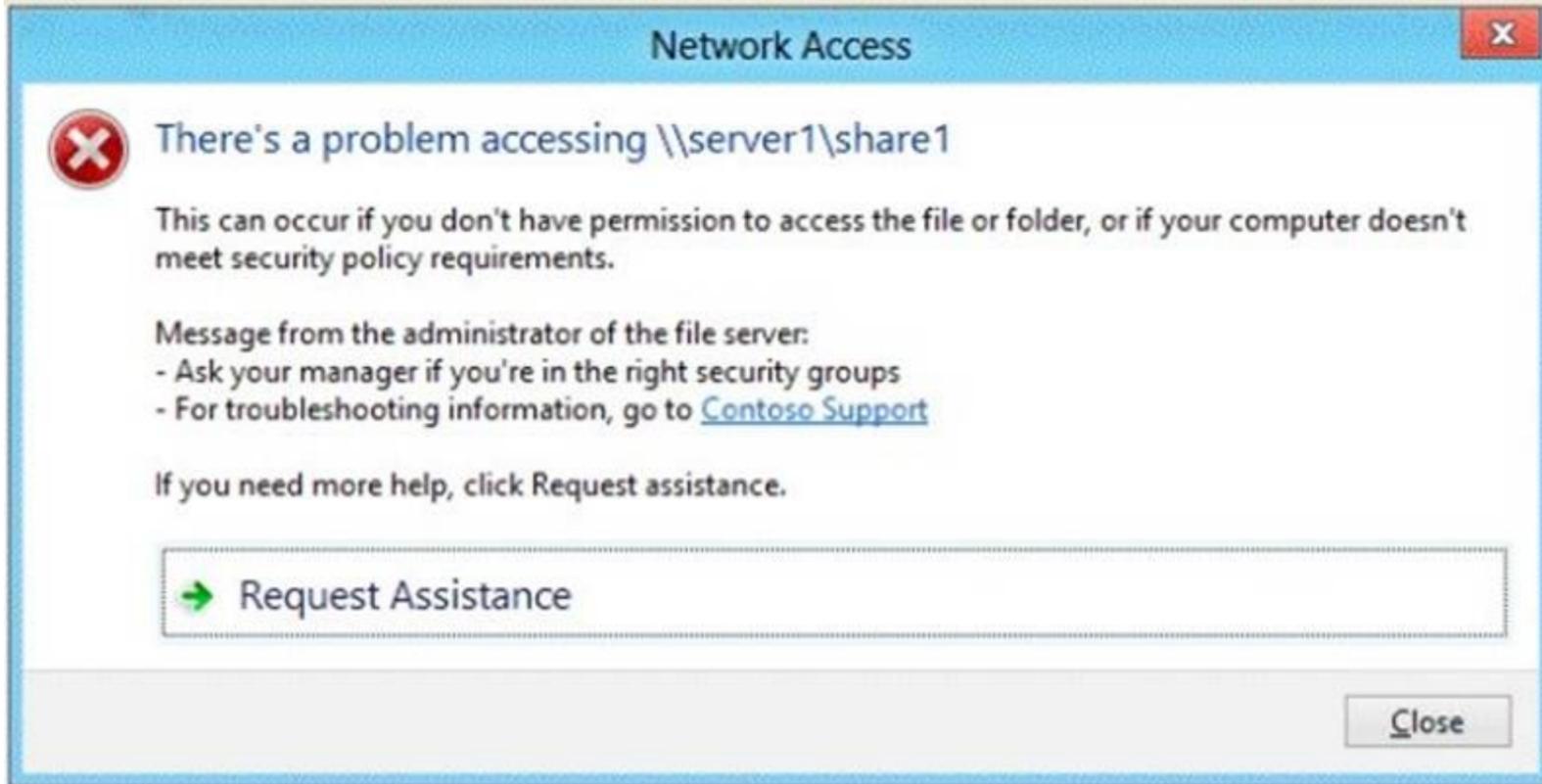

You deploy a new file server named Server2 that runs Windows Server 2012 R2.
You need to configure Server2 to display the same custom Access Denied message as Server1.
What should you install on Server2?

A. The Remote Assistance feature
B. The Storage Services server role
C. The File Server Resource Manager role service
D. The Enhanced Storage feature

Answer: C

Explanation: Access-Denied Assistance is a new role service of the File Server role in Windows Server 2012.
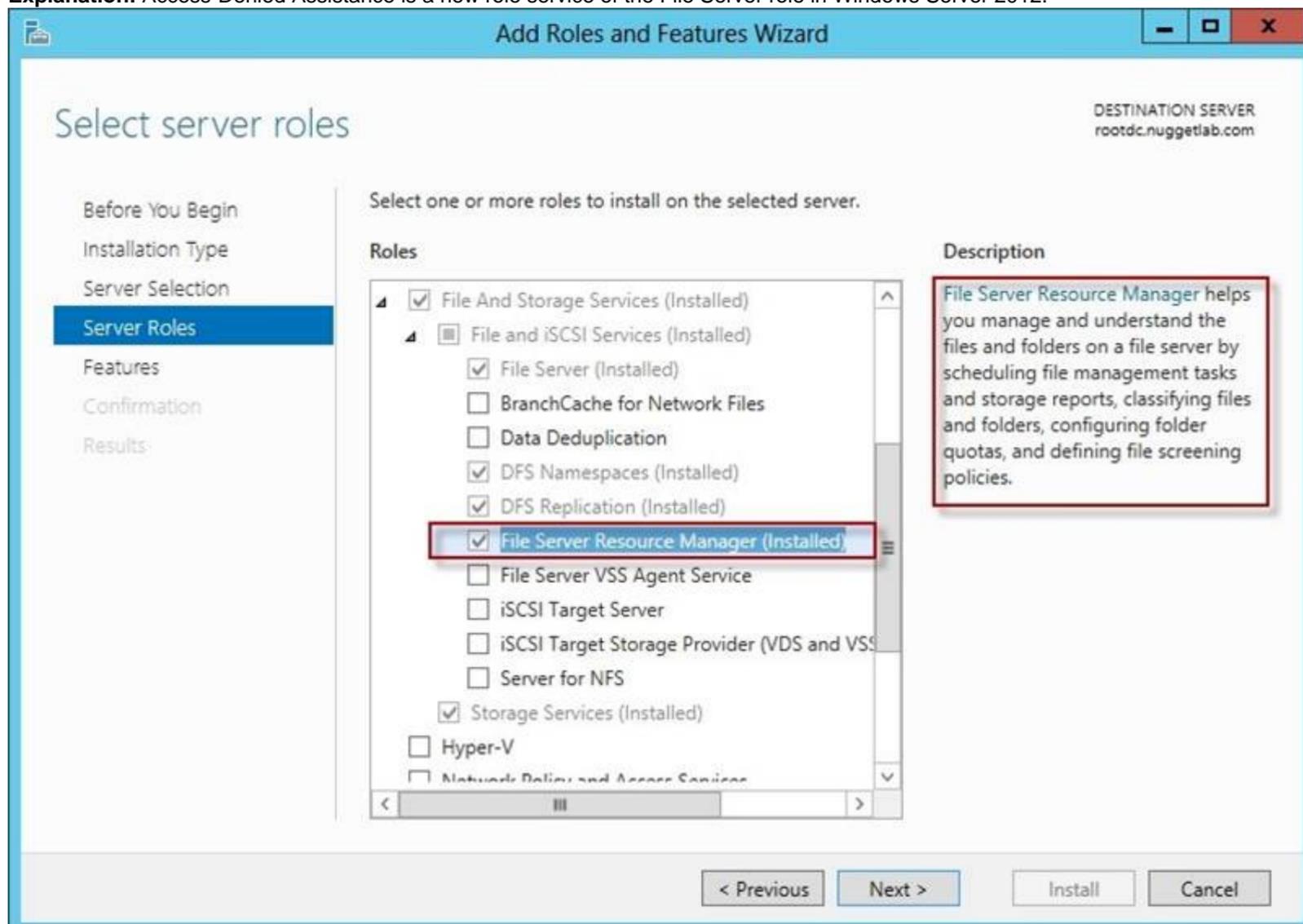

We need to install the prerequisites for Access-Denied Assistance.
Because Access-Denied Assistance relies up on e-mail notifications, we also need to configure each relevant file server with a Simple Mail Transfer Protocol (SMTP) server address. Let's do that quickly with Windows PowerShell:
Set-FSRMSetting -SMTPServer mailserver. nuggetlab.com -AdminEmailAddress admingroup@nuggetlab.com -FromEmailAddress admingroup@nuggetlab.com

You can enable Access-Denied Assistance either on a per-server basis or centrally via Group Policy. To my mind, the latter approach is infinitely preferable from an administration standpoint.

Create a new GPO and make sure to target the GPO at your file servers' Active Directory computer accounts as well as those of your AD client computers. In the Group Policy Object Editor, we are looking for the following path to configure Access-Denied Assistance:

\Computer Configuration\Policies\Administrative Templates\System\Access-Denied Assistance
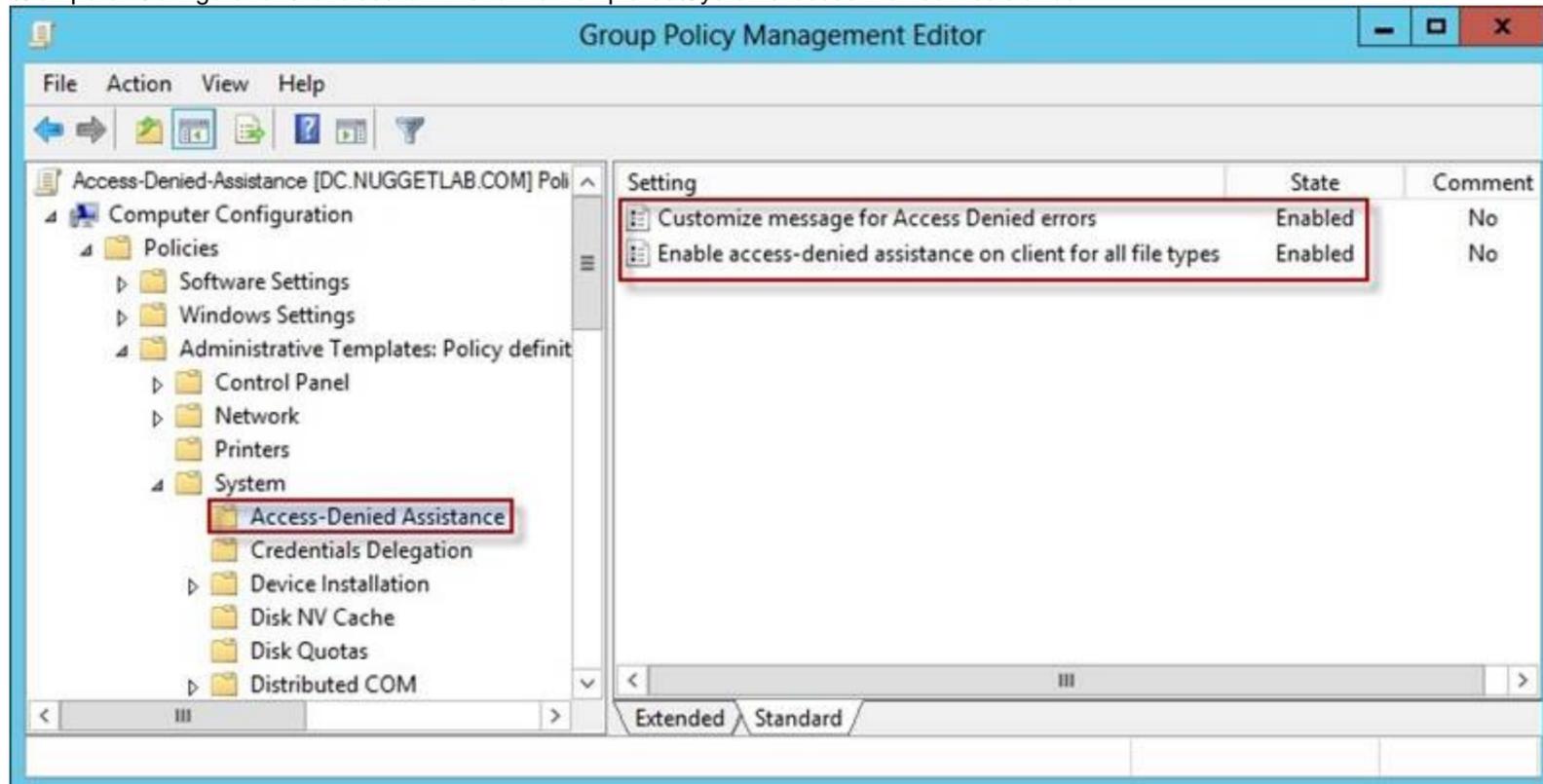
The Customize message for Access Denied errors policy, shown in the screenshot below, enables us to create the actual message box shown to users when they access a shared file to which their user account has no access.
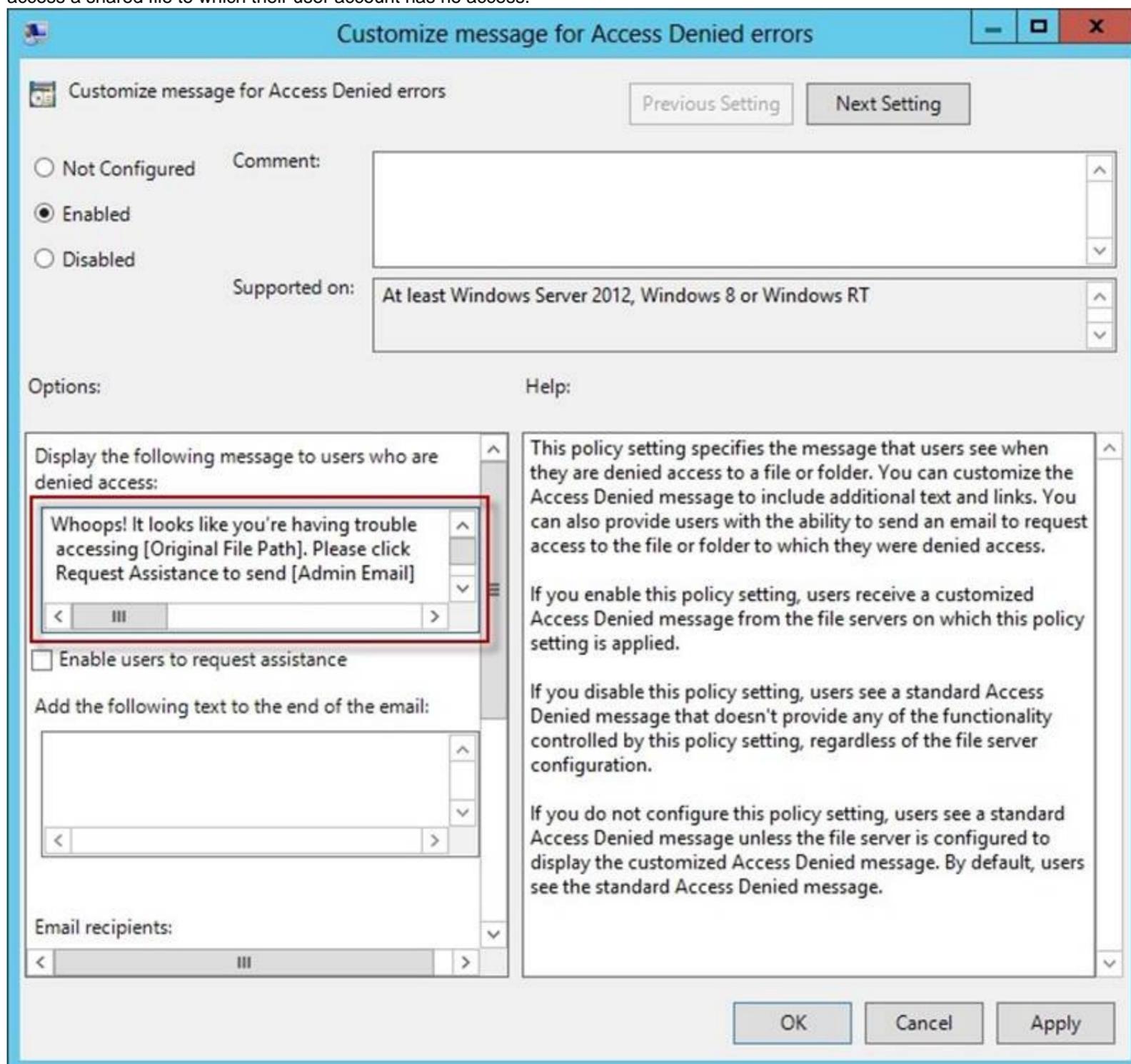
What's cool about this policy is that we can "personalize" the e-mail notifications to give us administrators (and, optionally, file owners) the details they need to resolve the permissions issue quickly and easily.

For instance, we can insert pre-defined macros to swap in the full path to the target file, the administrator e-mail address, and so forth. See this example:

Whoops! It looks like you're having trouble accessing [Original File Path]. Please click Request Assistance to send [Admin Email] a help request e-mail message. Thanks!

You should find that your users prefer these human-readable, informative error messages to the cryptic, non-descript error dialogs they are accustomed to dealing with.

The Enable access-denied assistance on client for all file types policy should be enabled to force client computers to participate in Access-Denied Assistance.

Again, you must make sure to target your GPO scope accordingly to "hit" your domain workstations as well as your Windows Server 2012 file servers.

Testing the configuration

This should come as no surprise to you, but Access-Denied Assistance works only with Windows Server 2012 and Windows 8 computers. More specifically, you must enable the Desktop Experience feature on your servers to see Access-Denied Assistance messages on server computers.

When a Windows 8 client computer attempts to open a file to which the user has no access, the custom Access-Denied Assistance message should appear:
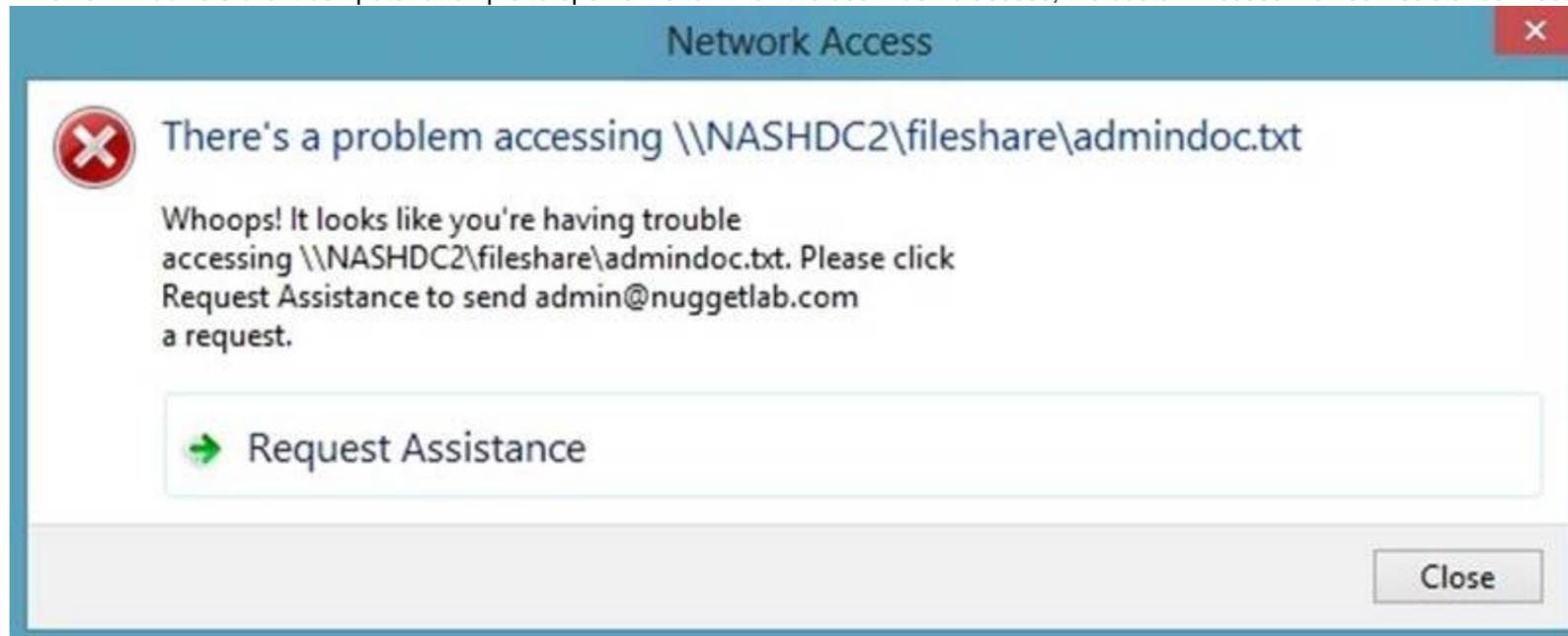
If the user clicks Request Assistance in the Network Access dialog box, they see a secondary message:
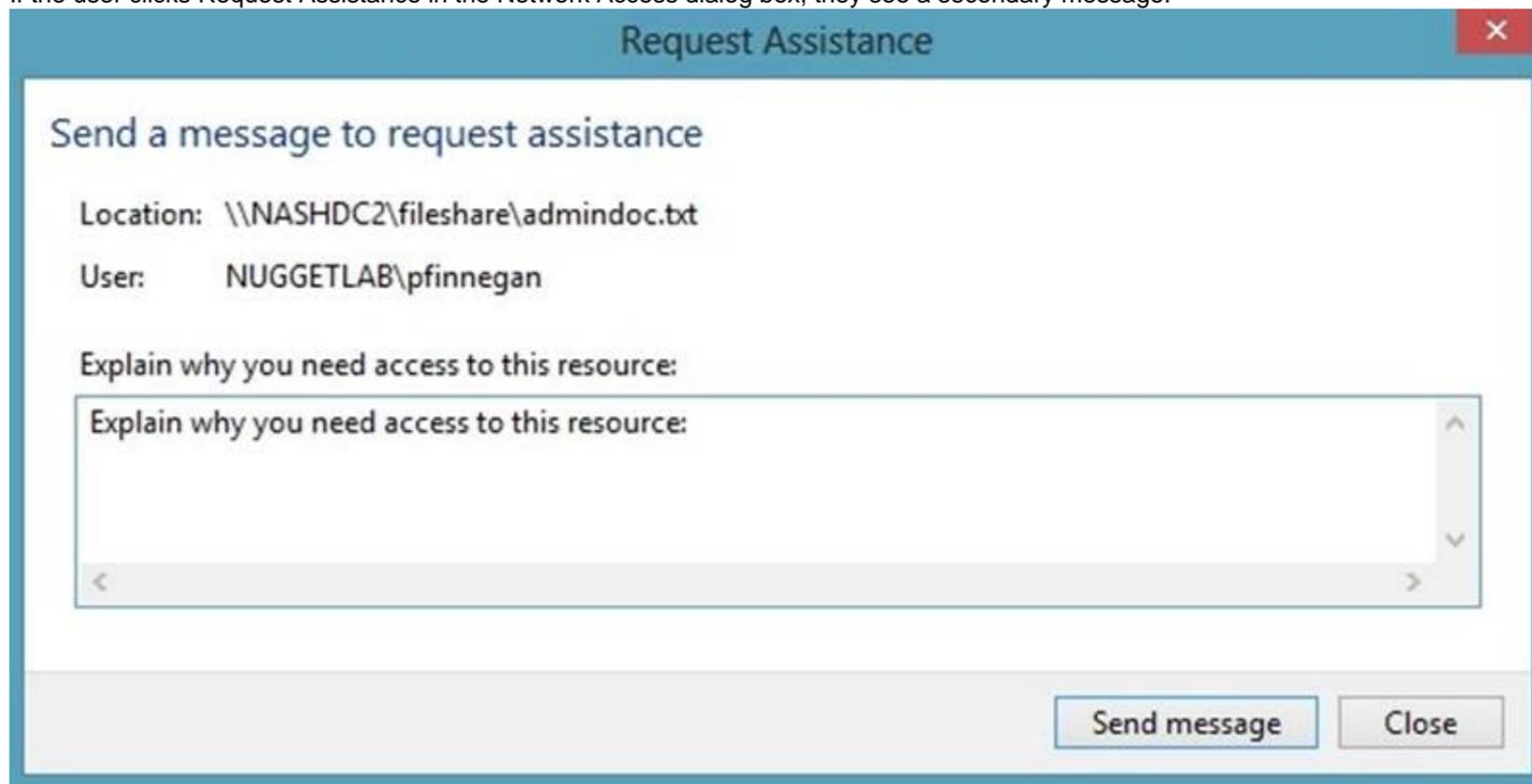
At the end of this process, the administrator(s) will receive an e-mail message that contains the key information they need in order to resolve the access problem:
The user's Active Directory identity The full path to the problematic file
A user-generated explanation of the problem

So that's it, friends! Access-Denied Assistance presents Windows systems administrators with an easy-to-manage method for more efficiently resolving user access problems on shared file system resources. Of course, the key caveat is that your file servers must run Windows Server 2012 and your client devices must run Windows 8, but other than that, this is a great technology that should save admins extra work and end-users extra headaches.

Reference: http: //4sysops. com/archives/access-denied-assistance-in-windows-server- 2012/

NEW QUESTION 10
Your network contains a server named Server1 that has the Network Policy and Access Services server role installed.
All of the network access servers forward connection requests to Server1.
You create a new network policy on Server1.
You need to ensure that the new policy applies only to connection requests from the 192.168.0.0/24 subnet.
What should you do?

A. Set the Client IP4 Address condition to 192.168.0.0/24.
B. Set the Client IP4 Address condition to 192.168.0.
C. Set the Called Station ID constraint to 192.168.0.0/24.
D. Set the Called Station ID constraint to 192.168.0.

Answer: B

Explanation: RADIUS client properties
Following are the RADIUS client conditions that you can configure in network policy.
? Calling Station ID: Specifies the network access server telephone number that was dialed by the dial-up access client.
? Client Friendly Name: Specifies the name of the RADIUS client that forwarded the connection request to the NPS server.
? Client IPv4 Address: Specifies the Internet Protocol (IP) version 4 address of the RADIUS client that forwarded the connection request to the NPS server.

? Client IPv6 Address: Specifies the Internet Protocol (IP) version 6 address of the RADIUS client that forwarded the connection request to the NPS server.
? Client Vendor: Specifies the name of the vendor or manufacturer of the RADIUS client that sends connection requests to the NPS server.
? MS RAS Vendor: Specifies the vendor identification number of the network access server that is requesting authentication.

NEW QUESTION 10
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 following role services installed:
? DirectAccess and VPN (RRAS)
? Network Policy Server
Remote users have client computers that run either Windows XP, Windows 7, or Windows 8.
You need to ensure that only the client computers that run Windows 7 or Windows 8 can establish VPN connections to Server1.
What should you configure on Server1?

A. A condition of a Network Policy Server (NPS) network policy
B. A constraint of a Network Policy Server (NPS) network policy
C. a condition of a Network Policy Server (NPS) connection request policy
D. A vendor-specific RADIUS attribute of a Network Policy Server (NPS) connection request policy

Answer: A

Explanation: If you want to configure the Operating System condition, click Operating System, and then click Add. In Operating System Properties, click Add, and then specify the operating system settings that are required to match the policy.
The Operating System condition specifies the operating system (operating system version or service pack number), role (client or server), and architecture (x86, x64, or ia64) required for the computer configuration to match the policy.

NEW QUESTION 14
Your network contains an Active Directory domain named contoso.com. The domain contains six domain controllers. The domain controllers are configured as shown in the following table.

Domain controller name	Operating system	FSMO role
DC1	Windows Server 2008 R2	PDC emulator
DC2	Windows Server 2012 R2	Schema master
DC3	Windows Server 2008 R2	Infrastructure master
DC4	Windows Server 2008 R2	Domain naming master
DC5	Windows Server 2008 R2	RID master
DC6	Windows Server 2012 R2	None

The network contains a server named Server1 that has the Hyper-v server role installed. DC6 is a virtual machine that is hosted on Server1.
You need to ensure that you can clone DC6. Which FSMO role should you transfer to DC2?

A. Rid master
B. Domain naming master
C. PDC emulator
D. Infrastructure master

Answer: C

Explanation: The clone domain controller uses the security context of the source domain controller (the domain controller whose copy it represents) to contact the Windows Server 2012 R2 Primary Domain Controller (PDC) emulator operations master role holder (also known as flexible single master operations, or FSMO).
The PDC emulator must be running Windows Server 2012 R2, but it does not have to be running on a hypervisor.
Reference:
http: //technet. microsoft. com/en-us/library/hh831734. aspx

NEW QUESTION 18
Your network contains an Active Directory domain named contoso.com. The domain contains three servers. The servers are configured as shown in the following table.

Server name	Role
Server1	Direct Access and VPN
Server2	File Server
Server3	Hyper-V

You need to ensure that end-to-end encryption is used between clients and Server2 when the clients connect to the network by using DirectAccess.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. From the Remote Access Management Console, reload the configuration.
B. Add Server2 to a security group in Active Directory.
C. Restart the IPSec Policy Agent service on Server2.
D. From the Remote Access Management Console, modify the Infrastructure Servers settings.
E. From the Remote Access Management Console, modify the Application Servers settings.

Answer: BE

Explanation: Unsure about these answers:
? A public key infrastructure must be deployed.
? Windows Firewall must be enabled on all profiles.
? ISATAP in the corporate network is not supported. If you are using ISATAP, you should remove it and use native IPv6.
? Computers that are running the following operating systems are supported as DirectAccess clients:
Windows Server® 2012 R2
Windows 8.1 Enterprise
Windows Server® 2012
Windows 8 Enterprise Windows Server® 2008 R2 Windows 7 Ultimate
Windows 7 Enterprise
? Force tunnel configuration is not supported with KerbProxy authentication.
? Changing policies by using a feature other than the DirectAccess management console or Windows PowerShell cmdlets is not supported.
? Separating NAT64/DNS64 and IPHTTPS server roles on another server is not supported.

NEW QUESTION 23
Your network contains two Active Directory forests named contoso.com and dev.contoso.com. The contoso.com forest contains a domain controller named DC1.
The dev.contoso.com forest contains a domain controller named DC2. Each domain contains an organizational unit (OU) named OU1.
Dev.contoso.com has a Group Policy object (GPO) named GPO1. GPO1 contains 200 settings, including several settings that have network paths. GPO1 is linked to OU1.
You need to copy GPO1 from dev.contoso.com to contoso.com. What should you do first on DC2?

A. From the Group Policy Management console, right-click GPO1 and select Copy.
B. Run the mtedit.exe command and specify the /Domaintcontoso.com /DC: DC 1 parameter.
C. Run the Save-NetGpocmdlet.
D. Run the Backup-Gpocmdlet.

Answer: A

Explanation: To copy a Group Policy object:
In the GPMC console tree, right-click the GPO that you want to copy, and then click Copy. To create a copy of the GPO in the same domain as the source GPO, right-click Group Policy objects, click Paste, specify permissions for the new GPO in the Copy GPO box, and then click OK.
For copy operations to another domain, you may need to specify a migration table.
The Migration Table Editor (MTE) is provided with Group Policy Management Console (GPMC) to facilitate the editing of migration tables. Migration tables are used for copying or importing Group Policy objects (GPOs) from one domain to another, in cases where the GPOs include domain-specific information that must be updated during copy or import. Source WS2008R2: Backup the existing GPOs from the GPMC, you need to ensure that the "Group Policy Objects" container is selected for the "Backup Up All" option to be available.
Copy a Group Policy Object with the Group Policy Management Console (GPMC)
You can copy a Group Policy object (GPO) either by using the drag-and-drop method or right-click method.
Applies To: Windows 8, Windows Server 2008 R2, Windows Server 2012
References:
http://technet.microsoft.com/en-us/library/cc785343(v=WS.10).aspx http://technet.microsoft.com/en-us/library/cc733107.aspx


NEW QUESTION 25
HOTSPOT
Your network contains a RADIUS server named Server1.
You install a new server named Server2 that runs Windows Server 2012 R2 and has Network Policy Server (NPS) installed.
You need to ensure that all accounting requests for Server2 are forwarded to Server1.
On Server2, you configure a Connection Request Policy.
What else should you configure on Server2? To answer, select the appropriate node in the answer area.

NPS (Local)
- RADIUS Clients and Servers
  - RADIUS Clients
  - Remote RADIUS Server Groups
- Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
  - System Health Validators
  - Remediation Server Groups
- Accounting
- Templates Management

Answer:

Explanation:

NPS (Local)
- RADIUS Clients and Servers
  - RADIUS Clients
  - Remote RADIUS Server Groups
- Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
  - System Health Validators
  - Remediation Server Groups
- Accounting
- Templates Management

NEW QUESTION 27
HOTSPOT
Your network contains an Active Directory named contoso.com. You have users named User1 and user2.
The Network Access Permission for User1 is set to Control access through NPS Network Policy. The Network Access Permission for User2 is set to Allow access.
A policy named Policy1 is shown in the Policy1 exhibit. (Click the Exhibit button.)
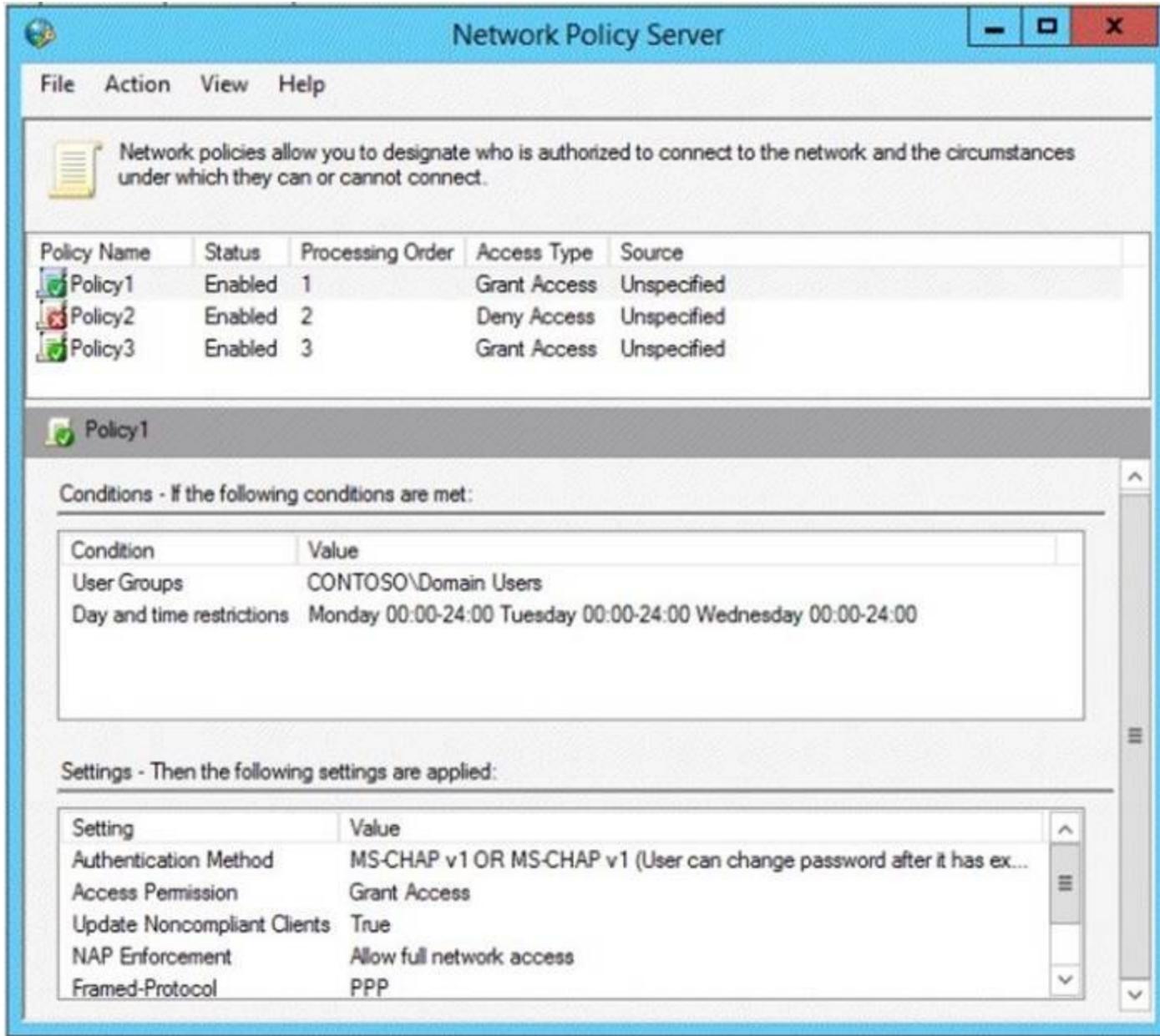
A policy named Policy2 is shown in the Policy2 exhibit. (Click the Exhibit button.)
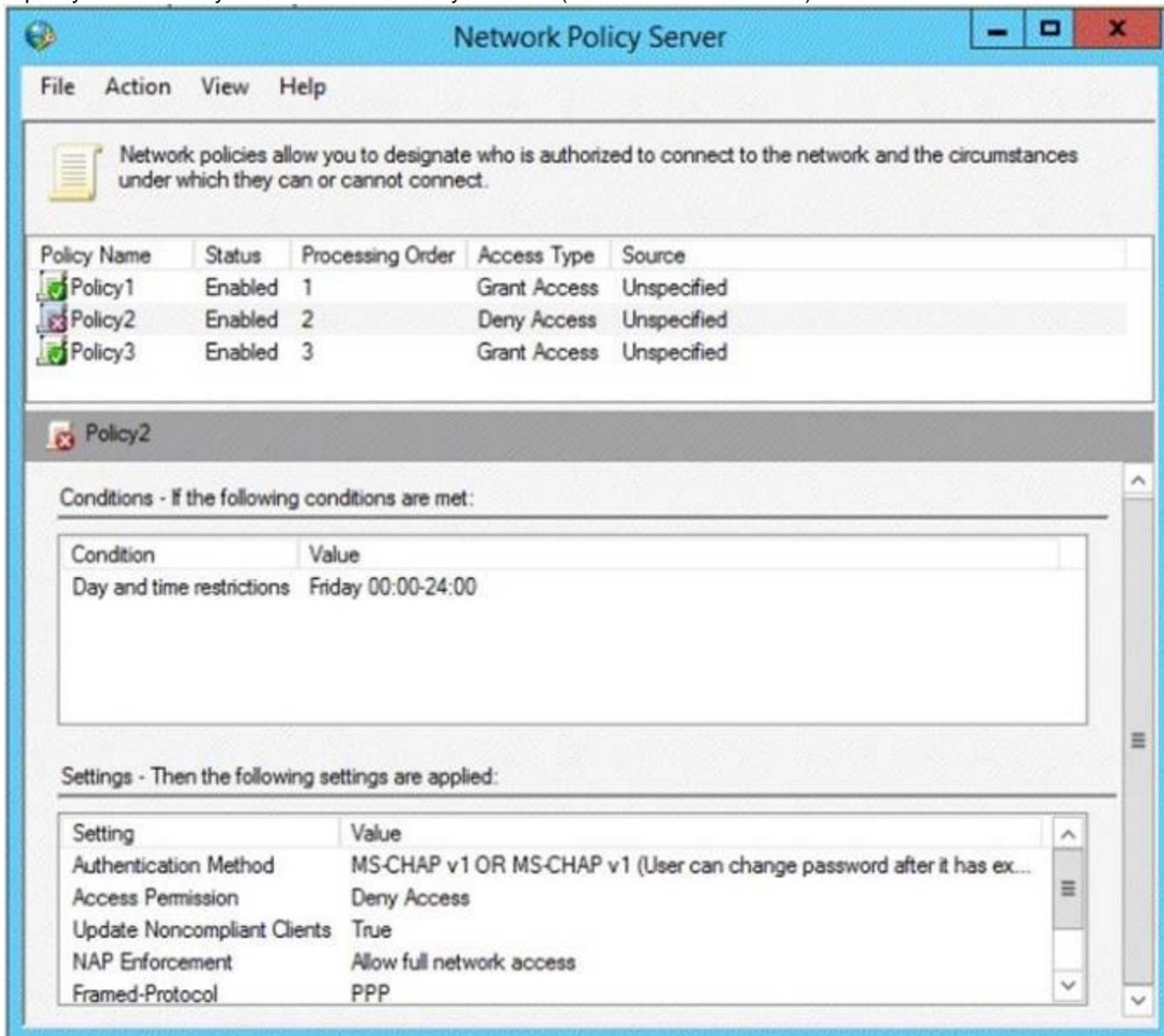
A policy named Policy3 is shown in the Policy3 exhibit. (Click the Exhibit button.)

Network Policy Server

File   Action   View   Help

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Policy1	Enabled	1	Grant Access	Unspecified
Policy2	Enabled	2	Deny Access	Unspecified
Policy3	Enabled	3	Grant Access	Unspecified

Policy3

Conditions - If the following conditions are met:

Condition	Value
User Groups	CONTOSO\Domain Users

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has e...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP

For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

	Yes	No
User1 will be able to establish a VPN connection on Thursday.	○	
User1 will be able to establish a VPN connection on Friday.	○	
User2 will be able to establish a VPN connection on Friday.	○	

Answer:

Explanation:

	Yes	No
User1 will be able to establish a VPN connection on Thursday.	○	
User1 will be able to establish a VPN connection on Friday.	○	○
User2 will be able to establish a VPN connection on Friday.	○	

NEW QUESTION 30
HOTSPOT

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Access server role installed.
You have a client named Client1 that is configured as an 802. IX supplicant.
You need to configure Server1 to handle authentication requests from Client1. The solution must minimize the number of authentication methods enabled on Server1.
Which authentication method should you enable? To answer, select the appropriate authentication method in the answer area.
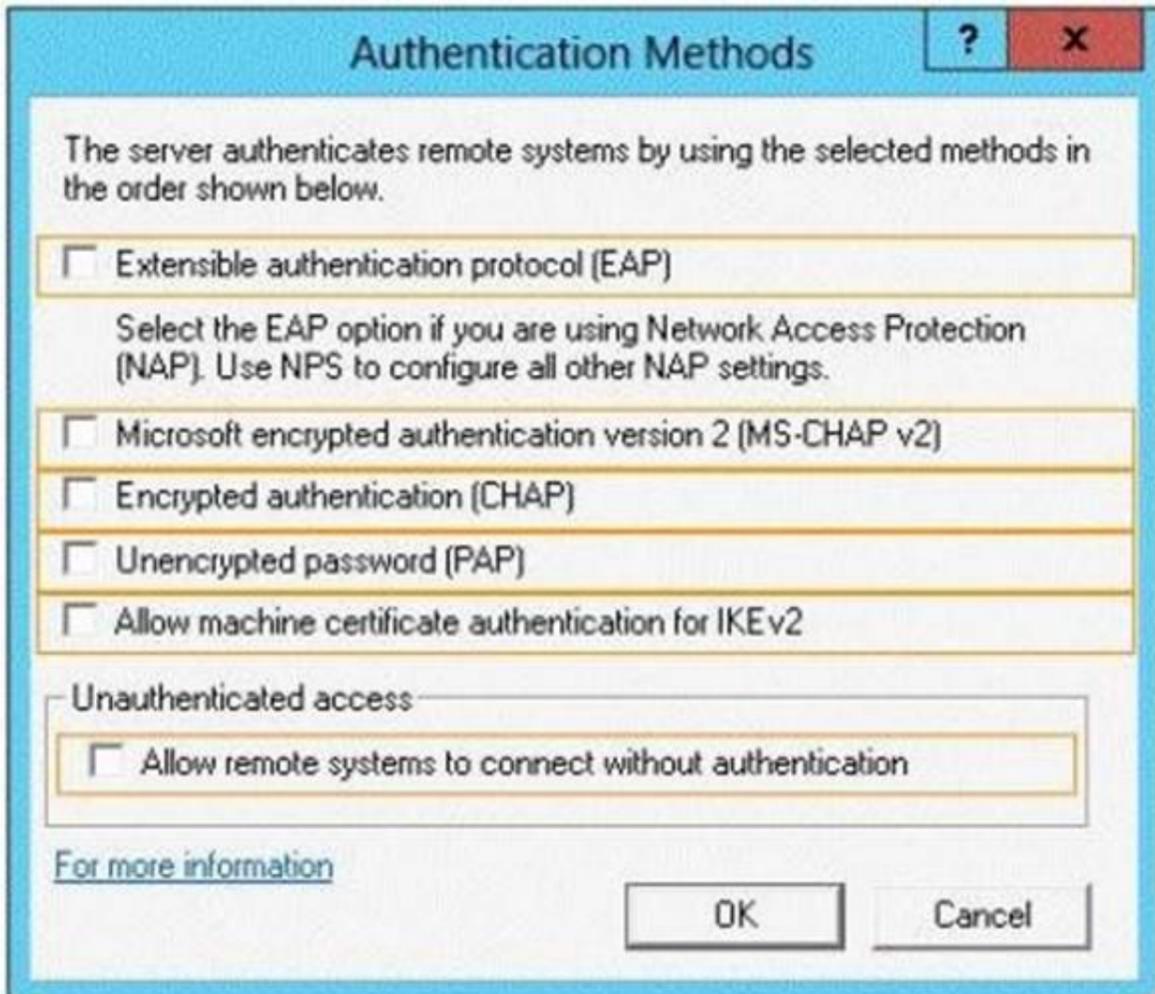
Answer:

Explanation: Microsoft® Windows® uses EAP to authenticate network access for Point-to-Point Protocol (PPP) connections (dial-up and virtual private network) and for IEEE 802.1X-based network access to authenticating Ethernet switches and wireless access points (APs).

NEW QUESTION 32
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains the users shown in the following table.

User name	Member of
User1	Group1
User2	Group2
User3	Group3

You have a Network Policy Server (NPS) server that has the network policies shown in the following table.

Policy name	Condition	Processing order
Policy1	Date and time restriction: Sunday 00:00 to Saturday 24:00	2
Policy2	CONTOSO\Group1	1
Policy3	CONTOSO\Group2 or CONTOSO\Group3	3

User1, User2, and User3 plan to connect to the network by using a VPN. You need to identify which network policy will apply to each user.
What should you identify?
To answer, select the appropriate policy for each user in the answer area.

Answer Area

User1: [▼]

User2: [▼]

User3: [▼]

Answer Area

User1: [dropdown]
Policy1
Policy2
Policy3

User2: [dropdown]
Policy1
Policy2
Policy3

User3: [dropdown]
Policy1
Policy2
Policy3

Answer:

Explanation: When you configure multiple network policies in NPS, the policies are an ordered list of rules. NPS evaluates the policies in listed order from first to last. If there is a network policy that matches the connection request, NPS uses the policy to determine whether to grant or deny access to the user or computer connection.
Network policies are evaulated according to the processing order. Once a match is found, no further network policy is processed.
Policies are processed in this order:
-Policy2 (applies only to members of Group1)
-Policy1 (applies to all users during specified time slot)
-Policy3 (applies only to members of Group2)
Since policy1 will always apply (sunday 0:00 to saturday 24:00 = always), policy3 will never be evaluated.
Correct answer is : User1: Policy2 User2: Policy1 User3: Policy1
https://technet.microsoft.com/en-us/library/cc732724(v=ws.10).aspx

NEW QUESTION 33
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 Access server role installed.
You log on to Server1 by using a user account named User2.
From the Remote Access Management Console, you run the Getting Started Wizard and you receive a warning message as shown in the exhibit. (Click the Exhibit button.)
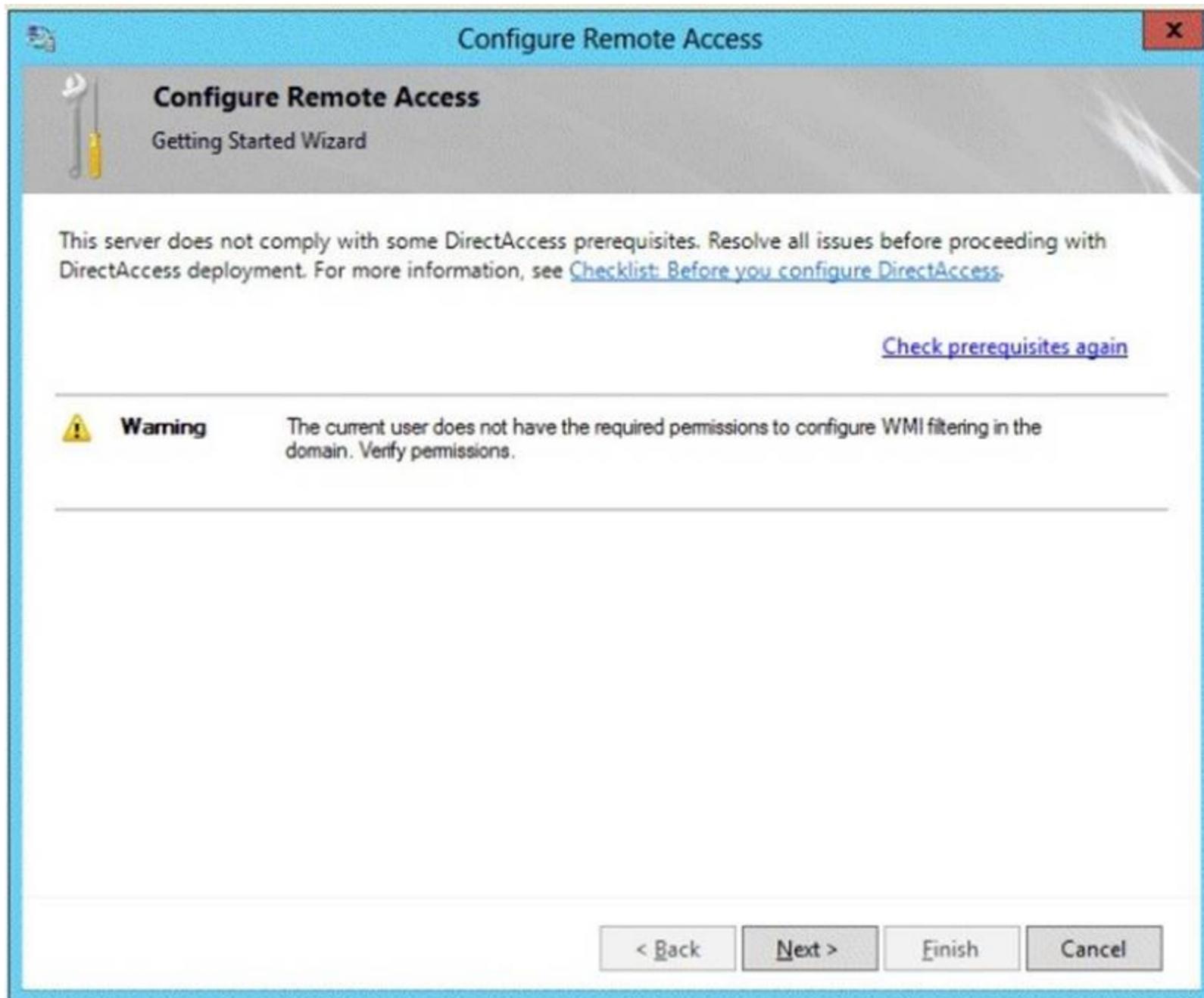
You need to ensure that you can configure DirectAccess successfully. The solution must minimize the number of permissions assigned to User2.
To which group should you add User2?

A. Enterprise Admins
B. Administrators
C. Account Operators
D. Server Operators

Answer: B

Explanation: You must have privileges to create WMI filters in the domain in which you want to create the filter. Permissions can be changed by adding a user to the Administrators group.
Administrators (A built-in group)
After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group. The Administrators
group has built-in capabilities that give its members full control over the system. The group is the default owner of any object that is created by a member of the group.
This example logs in as a test user who is not a domain user or an administrator on the server. This results in the error specifying that DA can only be configured by a user with local administrator permissions.
References:
http://technet.microsoft.com/en-us/library/cc780416(v=ws.10).aspx http://technet.microsoft.com/en-us/library/cc775497(v=ws.10).aspx

NEW QUESTION 34
You have a DNS server named Served that has a Server Core Installation on Windows Server 2012 R2.
You need to view the time-to-live (TTL) value of a name server (NS) record that is cached by the DNS Server service on Server1.
What should you run?

A. Show-DNSServerCache
B. nslookup.exe
C. ipconfig.exe /displaydns
D. dnscacheugc.exe

Answer: A

Explanation: The Show-DNSServerCache shows all cached Domain Name System (DNS) server resource records in the following format: Name, ResourceRecordData, Time-to-Live (TTL).

NEW QUESTION 35
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.
Each time a user receives an access-denied message after attempting to access a folder on Server1, an email notification is sent to a distribution list named DL1.
You create a folder named Folder1 on Server1, and then you configure custom NTFS permissions for Folder1.
You need to ensure that when a user receives an access-denied message while attempting to access Folder1, an email notification is sent to a distribution list named DL2. The solution must not prevent DL1 from receiving notifications about other access-denied messages.
What should you do?

A. From Server Manager, run the New Share Wizard to create a share for Folder1 by selecting the SMB Share - Advanced option.
B. From the File Server Resource Manager console, modify the Access-Denied Assistance settings.
C. From the File Server Resource Manager console, modify the Email Notifications settings.
D. From Server Manager, run the New Share Wizard to create a share for Folder1 by selecting the SMB Share -Applications option.

Answer: A

Explanation: When using the email model each of the file shares, you can determine whether access requests to each file share will be received by the administrator, a distribution list that represents the file share owners, or both.
The owner distribution list is configured by using the SMB Share – Advanced file share profile in the New Share Wizard in Server Manager.

NEW QUESTION 39
You have a server named Server1 that runs Windows Server 2012 R2.
On Server1, you configure a custom Data Collector Set (DCS) named DCS1. DCS1 is configured to store performance log data in C:\Logs.
You need to ensure that the contents of C:\Logs are deleted automatically when the folder reaches 100 MB in size.
What should you configure?

A. A File Server Resource Manager (FSRM) file screen on the C:\Logs folder
B. The Data Manager settings of DCS1
C. A schedule for DCS1
D. A File Server Resource Manager (FSRM) quota on the C:\Logs folder

Answer: B

Explanation: To configure data management for a Data Collector Set
1. In Windows Performance Monitor, expand Data Collector Sets and click User Defined.
2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click Data Manager.
3. On the Data Manager tab, you can accept the default values or make changes according to your data retention policy. See the table below for details on each option.
When Minimum free disk or Maximum folders is selected, previous data will be deleted according to the Resource policy you choose (Delete largest or Delete oldest) when the limit is reached. When Apply policy before the data collector set starts is selected, previous data will be deleted according to your selections before the data collector set creates its next log file.
When Maximum root path size is selected, previous data will be deleted according to your selections when the root log folder size limit is reached.
4. Click the Actions tab. You can accept the default values or make changes. See the table below for details on each option.
5. When you have finished making your changes, click OK.

NEW QUESTION 44
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains 500 client computers that run Windows 8 Enterprise.
You implement a Group Policy central store.
You have an application named App1. App1 requires that a custom registry setting be deployed to all of the computers.
You need to deploy the custom registry setting. The solution must minimize administrator effort.
What should you configure in a Group Policy object (GPO)?

A. The Software Installation settings
B. The Administrative Templates
C. An application control policy
D. The Group Policy preferences

Answer: D

Explanation: ? Open the Group Policy Management Console. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click Edit.
? In the console tree under Computer Configuration or User Configuration, expand
the Preferences folder, and then expand the Windows Settings folder.
? Right-click the Registry node, point to New, and select Registry Item.
Group Policy preferences provide the means to simplify deployment and standardize configurations. They add to Group Policy a centralized system for deploying preferences (that is, settings that users can change later).
You can also use Group Policy preferences to configure applications that are not Group Policy-aware. By using Group Policy preferences, you can change or delete almost any registry setting, file or folder, shortcut, and more. You are not limited by the contents of Administrative Template files. The Group Policy Management
Editor (GPME) includes Group Policy preferences. References:
http: //technet.microsoft.com/en-us/library/gg699429.aspx
http: //www. unidesk. com/blog/gpos-set-custom-registry-entries-virtual-desktops-disabling- machine-password
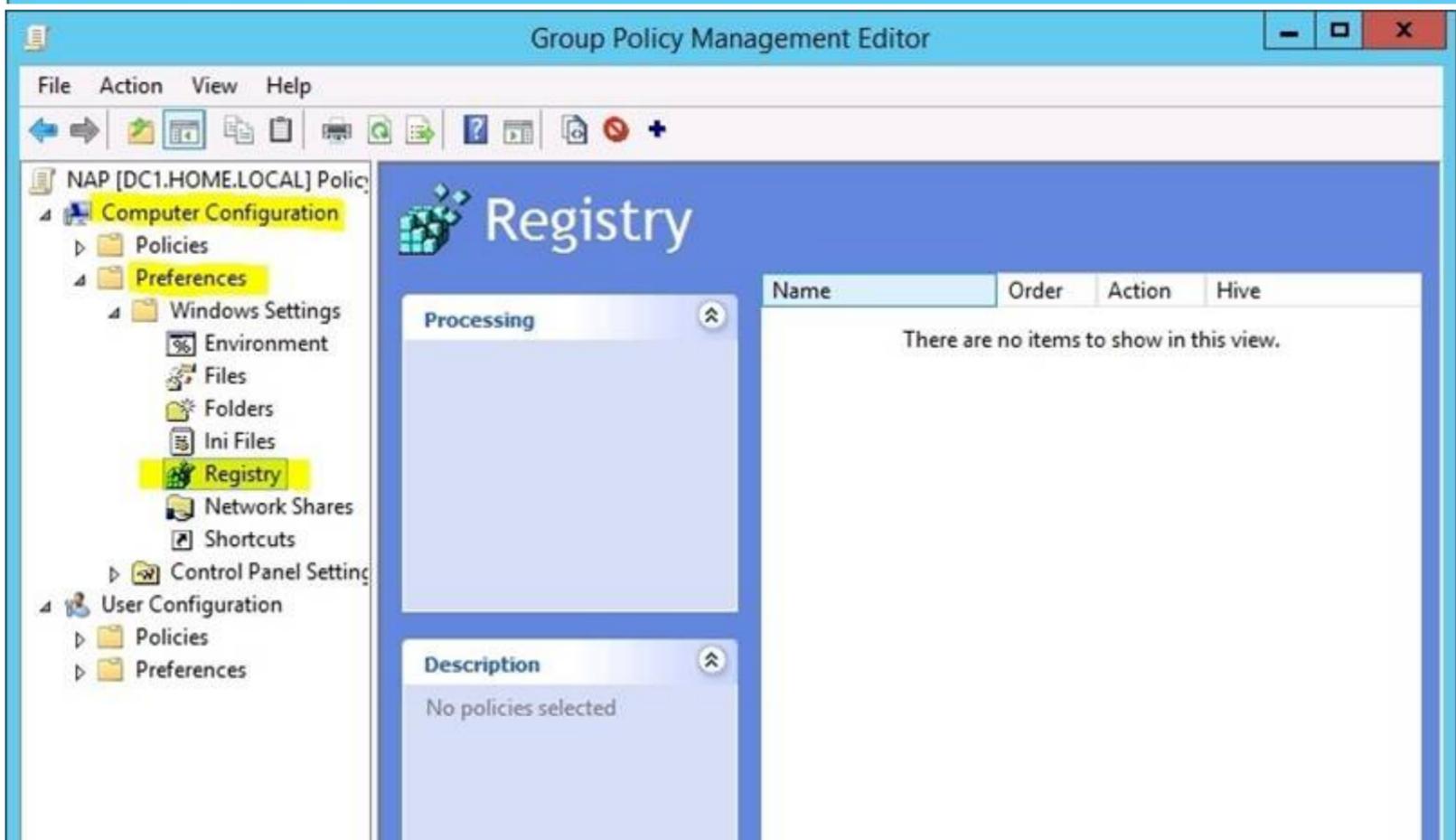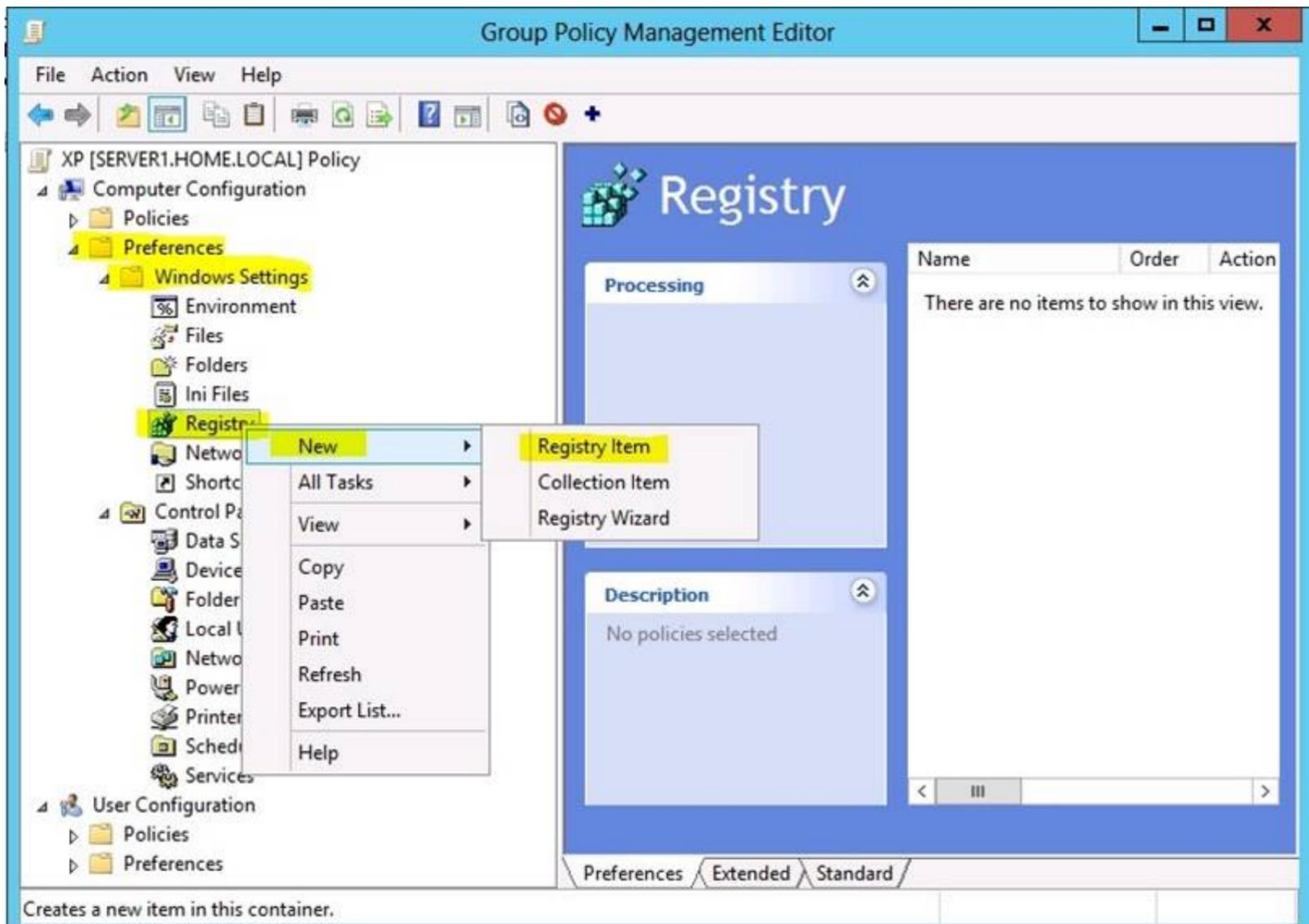
NEW QUESTION 48
Your network contains an Active Directory domain named contoso.com. All user accounts reside in an organizational unit (OU) named OU1.
You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preference of GPO1 to add a shortcut named Link1 to the desktop of each user.
You discover that when a user deletes Link1, the shortcut is removed permanently from the desktop.
You need to ensure that if a user deletes Link1, the shortcut is added to the desktop again. What should you do?

A. Enforce GPO1.
B. Modify the Link1 shortcut preference of GPO1.
C. Enable loopback processing in GPO1.
D. Modify the Security Filtering settings of GPO1.

Answer: B

Explanation: Replace Delete and recreate a shortcut for computers or users. The net result of the Replace action is to overwrite the existing shortcut. If the shortcut does not exist, then the Replace action creates a new shortcut.

This type of preference item provides a choice of four actions: Create, Replace, Update, and Delete. The behavior of the preference item varies with the action selected and whether the shortcut already exists.

Create	Create a new shortcut for computers or users.
Delete	Remove a shortcut for computers or users.
Replace	Delete and recreate a shortcut for computers or users. The net result of the **Replace** action is to overwrite the existing shortcut. If the shortcut does not exist, then the **Replace** action creates a new shortcut.
Update	Modify settings of an existing shortcut for computers or users. This action differs from **Replace** in that it only updates shortcut settings defined within the preference item. All other settings remain as configured in the shortcut. If the shortcut does not exist, then the **Update** action creates a new shortcut.

Refernces:
http: //technet.microsoft.com/en-us/library/cc753580.aspx http: //technet.microsoft.com/en-us/library/cc753580.aspx

NEW QUESTION 53
You have a server named Server 1.
You enable BitLocker Drive Encryption (BitLocker) on Server 1.
You need to change the password for the Trusted Platform Module (TPM) chip. What should you run on Server1?

A. Manage-bde.exe
B. Set-TpmOwnerAuth
C. bdehdcfg.exe
D. tpmvscmgr.exe

Answer: B

Explanation: The Set-TpmOwnerAuthcmdlet changes the current owner authorization value of the Trusted Platform Module (TPM) to a new value. You can specify the current owner authorization value or specify a file that contains the current owner authorization value. If you do not specify an owner authorization value, the cmdlet attempts to read the value from the registry.
Use the ConvertTo-TpmOwnerAuthcmdlet to create an owner authorization value. You can specify a new owner authorization value or specify a file that contains the new value.

NEW QUESTION 56
DRAG DROP
You have a WIM file that contains an image of Windows Server 2012 R2. applied a Microsoft Standalone Update Package (MSU) to the image. You need to remove the MSU package from the image.
Which three actions should you perform in sequence? To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.

	Answer Area
Run **dism.exe** and specify the /Capture-Image parameter.	
Run **dism.exe** and specify the /Apply-Image parameter.	
Run **wusa.exe** and specify the /uninstall parameter.	
Run **dism.exe** and specify the / RemovePackage parameter.	
Run **dism.exe** and specify the /Cleanup-Image parameter.	

Answer:

Explanation: Note:
* At a command prompt, specify the package identity to remove it from the image. You can remove multiple packages on one command line.
DISM /Image: C:\test\offline /Remove-Package /PackageName: Microsoft.Windows.Calc. Demo~6595b6144ccf1df~x86~en~1.0.0.0 /PackageName: Micro /Cleanup-Image
Performs cleanup or recovery operations on the image.

NEW QUESTION 60
You are a network administrator of an Active Directory domain named contoso.com.
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the DHCP Server server role and the Network Policy Server role service installed.
You enable Network Access Protection (NAP) on all of the DHCP scopes on Server1. You need to create a DHCP policy that will apply to all of the NAP non-

compliant DHCP
clients.
Which criteria should you specify when you create the DHCP policy?

A. The client identifier
B. The user class
C. The vendor class
D. The relay agent information

Answer: B

Explanation:
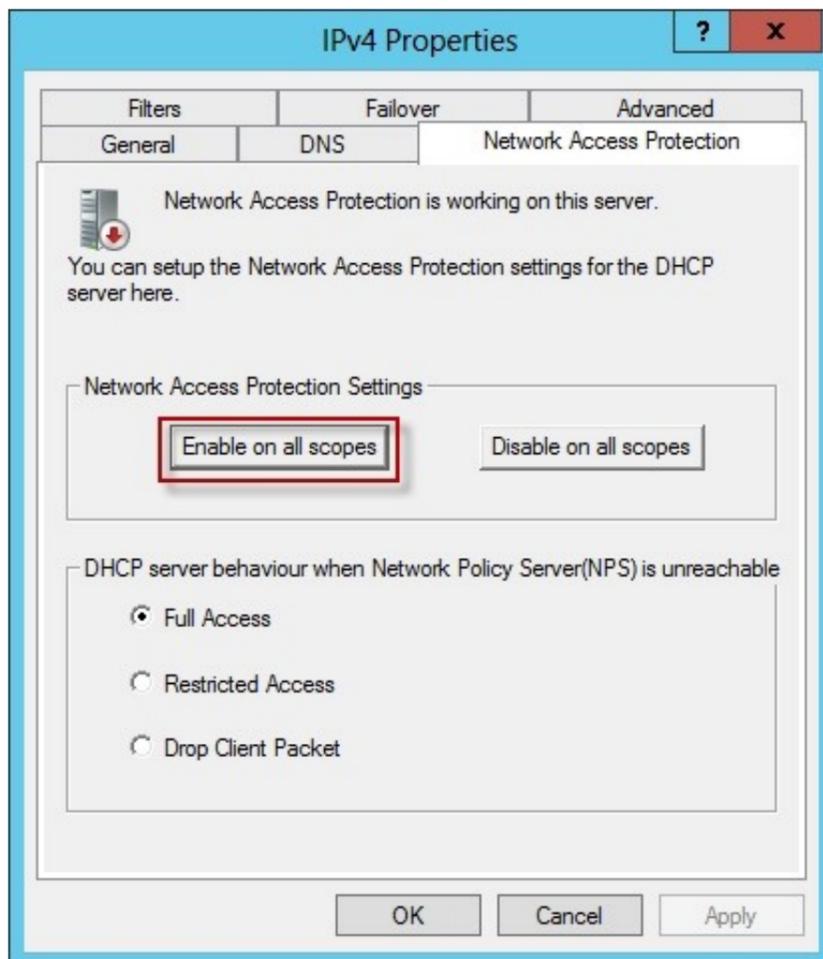
To configure a NAP-enabled DHCP server
? On the DHCP server, click Start, click Run, in Open, type dhcpmgmt. smc, and then press ENTER.
? In the DHCP console, open <servername>\IPv4.
? Right-click the name of the DHCP scope that you will use for NAP client computers, and then click Properties.
? On the Network Access Protection tab, under Network Access Protection Settings, choose Enable for this scope, verify that Use default Network Access Protection profile is selected, and then click OK.
? In the DHCP console tree, under the DHCP scope that you have selected, right- click Scope Options, and then click Configure Options.
? On the Advanced tab, verify that Default User Class is selected next to User class.
? Select the 003 Router check box, and in IP Address, under Data entry, type the IP
address for the default gateway used by compliant NAP client computers, and then click Add.
? Select the 006 DNS Servers check box, and in IP Address, under Data entry, type
the IP address for each router to be used by compliant NAP client computers, and then click Add.
? Select the 015 DNS Domain Name check box, and in String value, under Data
entry, type your organization's domain name (for example, woodgrovebank. local), and then click Apply. This domain is a full-access network assigned to compliant NAP clients.
? On the Advanced tab, next to User class, choose Default Network Access
Protection Class.
? Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by noncompliant NAP client computers, and then click Add. This can be the same default gateway that is used by compliant NAP clients.
? Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each DNS server to be used by noncompliant NAP client computers, and then click Add. These can be the same DNS servers used by compliant NAP clients.
? Select the 015 DNS Domain Name check box, and in String value, under Data entry, type a name to identify the restricted domain (for example, restricted.
Woodgrovebank. local), and then click OK. This domain is a restricted-access network assigned to noncompliant NAP clients.
? Click OK to close the Scope Options dialog box.
? Close the DHCP console.
Reference: http: //technet.microsoft.com/en-us/library/dd296905%28v=ws.10%29.aspx

NEW QUESTION 65
Your network contains two servers named Server1 and Server2 that run windows Server 2012 R2. Server1 and 5erver2 have the Windows Server Update Services server role installed.
Server1 synchronizes from Microsoft Update. Server2 is a Windows Server Update Services (WSUS) replica of Server1.
You need to configure replica downstream servers to send Server1 summary information about the computer update status.
What should you do?

A. From Server1, configure Reporting Rollup.
B. From Server2, configure Reporting Rollup.
C. From Server2, configure Email Notifications.
D. From Server1, configure Email Notifications.

Answer: A

Explanation: WSUS Reporting Rollup Sample Tool
This tool uses the WSUS application programming interface (API) to demonstrate centralized monitoring and reporting for WSUS. It creates a single report of update and computer status from the WSUS servers into your WSUS environment. The sample package also contains sample source files to customize or extend the tool functionality of the tool to meet specific needs. The WSUS Reporting Rollup Sample Tool and files are provided AS IS. No product support is available for this tool or sample files. For more information read the readme file.
Reference: http: //technet. microsoft. com/en-us/windowsserver/bb466192. aspx

NEW QUESTION 66
Your network contains an Active Directory domain named adatum.com. A network administrator creates a Group Policy central store.
After the central store is created, you discover that when you create new Group Policy objects (GPOs), the GPOs do not contain any Administrative Templates.
You need to ensure that the Administrative Templates appear in new GPOs.
What should you do?

A. Add your user account to the Group Policy Creator Owners group.
B. Configure all domain controllers as global catalog servers.
C. Copy files from %Windir%\Policydefinitions to the central store.
D. Modify the Delegation settings of the new GPOs.

Answer: C

Explanation: To take advantage of the benefits of .admx files, you must create a Central Store in the SYSVOL folder on a domain controller. The Central Store is a file location that is checked by the Group Policy tools. The Group Policy tools use any .admx files that are in the Central Store. The files that are in the Central Store are later replicated to all domain controllers in the domain.

NEW QUESTION 71
Your network contains a Hyper-V host named Server1 that hosts 20 virtual machines.
You need to view the amount of memory resources and processor resources each virtual machine uses currently.
Which tool should you use on Server1?

A. Hyper-V Manager
B. Task Manager
C. Windows System Resource Manager (WSRM)
D. Resource Monitor

Answer: A

NEW QUESTION 72
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
In a remote site, a support technician installs a server named DC10 that runs Windows Server 2012 R2. DC10 is currently a member of a workgroup.
You plan to promote DC10 to a read-only domain controller (RODC).
You need to ensure that a user named Contoso\User1 can promote DC10 to a RODC in the contoso.com domain. The solution must minimize the number of permissions assigned to User1.
What should you do?

A. From Active Directory Users and Computers, run the Delegation of Control Wizard on the contoso.com domain object.
B. From Active Directory Administrative Center, pre-create an RODC computer account.
C. From Ntdsutil, run the local roles command.
D. Join DC10 to the domai
E. Run dsmod and specify the /server switch.

Answer: B

Explanation: A staged read only domain controller (RODC) installation works in two discrete phases:
1. Staging an unoccupied computer account
2. Attaching an RODC to that account during promotion
Reference: Install a Windows Server 2012 R2 Active Directory Read-Only Domain Controller (RODC)

NEW QUESTION 73
You have a server named Server1 that runs Windows Server 2012 R2. You create a Data Collector Set (DCS) named DCS1.
You need to configure DCS1 to log data to D:\logs.
What should you do?

A. Right-click DCS1 and click Properties.
B. Right-click DCS1 and click Export list.
C. Right-click DCS1 and click Data Manager.
D. Right-click DCS1 and click Save template.

Answer: A

Explanation: The Root Directory will contain data collected by the Data Collector Set. Change this setting if you want to store your Data Collector Set data in a different location than the default. Browse to and select the directory, or type the directory name.
To view or modify the properties of a Data Collector Set after it has been created, you can:
* Select the Open properties for this data collector set check box at the end of the Data Collector Set Creation Wizard.
* Right-click the name of a Data Collector Set, either in the MMC scope tree or in the console window, and click Properties in the context menu.
Directory tab:
In addition to defining a root directory for storing Data Collector Set data, you can specify a single Subdirectory or create a Subdirectory name format by clicking

the arrow to the right of the text entry field.

NEW QUESTION 78
You manage a server that runs Windows Server 2012 R2. The server has the Windows Deployment Services server role installed.
You have a desktop computer that has the following configuration:
? Computer name: Computer1
? Operating system: Windows 8
? MAC address: 20-CF-30-65-D0-87
? GUID: 979708BF-C04B-4525-9FE0-C4150BB6C618
You need to configure a pre-staged device for Computer1 in the Windows Deployment Services console.
Which two values should you assign to the device ID? (Each correct answer presents a complete solution. Choose two.)

A. 20CF3065D08700000000000000000000
B. 979708BFC04B45259FE0C4150BB6C618
C. 979708BF-C04B-452S-9FE0-C4150BB6C618
D. 0000000000000000000020CF306SD087
E. 00000000-0000-0000-0000-C41S0BB6C618

Answer: CD

Explanation: In the text box, type the client computer's MAC address preceded with twenty zeros or the globally unique identifier (GUID) in the format: {XXXXXXXX-XXXX-XXXX-XXX- XXXXXXXXXXXX}.
* To add or remove pre-staged client to/from AD DS, specify the name of the computer or the device ID, which is a GUID, media access control (MAC) address, or Dynamic Host Configuration Protocol (DHCP) identifier associated with the computer.
* Example: Remove a device by using its ID from a specified domain
This command removes the pre-staged device that has the specified ID. The cmdlet searches the domain named TSQA.contoso.com for the device.
Windows PowerShell
PS C:\> Remove-WdsClient -DeviceID "5a7a1def-2e1f-4a7b-a792-ae5275b6ef92" -Domain
-DomainName "TSQA.contoso.com"

NEW QUESTION 79
DRAG DROP
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
The domain contains an organizational unit (OU) named OU1. OU1 contains an OU named OU2. OU2 contains a user named user1.
User1 is the member of a group named Group1. Group1 is in the Users container.
You create five Group Policy objects (GPO). The GPOs are configured as shown in the
following table.

GPO name	Linked to	Enforced setting	Additional permissions
GPO1	Contoso.com	Enabled	Group1 – Deny Apply Group Policy
GPO2	Contoso.com	Disabled	Not applicable
GPO3	OU1	Enabled	Group1 – Deny Read
GPO4	OU1	Disabled	Not applicable
GPO5	OU2	Enabled	Group1 – Full control

The Authenticated Users group is assigned the default permissions to all of the GPOs. There are no site-level GPOs.
You need to identify which three GPOs will be applied to User1 and in which order the GPOs will be applied to User1.
Which three GPOs should you identify in sequence? To answer, move the appropriate three GPOs from the list of GPOs to the answer area and arrange them in the correct order.

Actions	Answer Area
GPO5	
GPO3	
GPO2	
GPO1	
GPO4	

Answer:

Explanation: Box 1: GPO2
Box 2: GPO4
Box 3: GPO5
Note:
* First at the domain level (GPO2), then at the highest OU level GPO4, and finally at the OU level containing user1 GPO5.

Incorrect:
* Read and Apply group policy are both needed in order for the user or computer to receive and process the policy
Not GPO1: Group1 has Deny Apply Group Policy permissions on GPO1. Not GPO3: Group1 has Deny Read permissions on GPO3.
GPO2 and GPO4 are disabled.
* When a Group Policy Object (GPO) is enforced it means the settings in the Group Policy Object on an Organization Unit (which is shown as a folder within the Active Directory Users and Computers MMC) cannot be overruled by a Group Policy Object (GPO) which is link enabled on an Organizational Unit below the Organizational Unit with the enforced Group Policy Object (GPO).
* Group Policy settings are processed in the following order: 1 Local Group Policy object
2 Site.
3 Domain
4 Organizational units
GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

NEW QUESTION 83
HOTSPOT
Your network contains an Active Directory domain named contoso.com.
You create an organizational unit (OU) named OU1 and a Group Policy object (GPO) named GPO1. You link GPO1 to OU1.
You move several file servers that store sensitive company documents to OU1. Each file server contains more than 40 shared folders.
You need to audit all of the failed attempts to access the files on the file servers in OU1. The solution must minimize administrative effort.
Which two audit policies should you configure in GPO1? To answer, select the appropriate two objects in the answer area.

Answer:

Explanation:
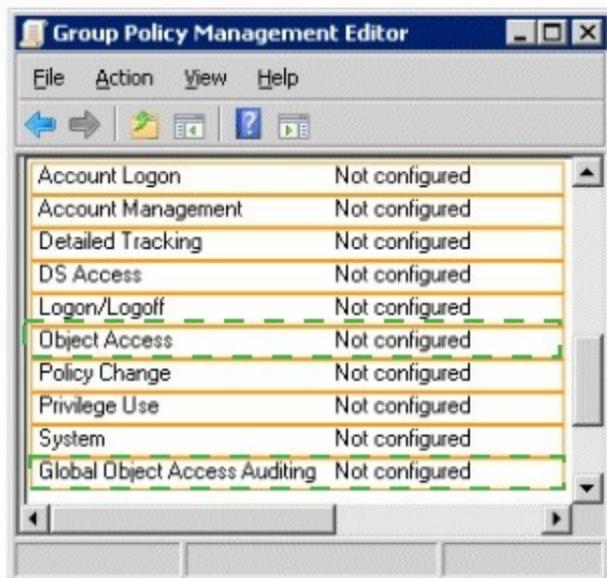
NEW QUESTION 85
Your network contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2 and have the DNS Server server role installed.
On Server1, you create a standard primary zone named contoso.com.
You need to ensure that Server2 can host a secondary zone for contoso.com. What should you do from Server1?

A. Add Server2 as a name server.
B. Create a trust anchor named Server2.
C. Convert contoso.com to an Active Directory-integrated zone.
D. Create a zone delegation that points to Server2.

Answer: A

Explanation: Typically, adding a secondary DNS server to a zone involves three steps:
1. On the primary DNS server, add the prospective secondary DNS server to the list of name servers that are authoritative for the zone.
2. On the primary DNS server, verify that the transfer settings for the zone permit the zone to be transferred to the prospective secondary DNS server.

3. On the prospective secondary DNS server, add the zone as a secondary zone.

You must add a new Name Server. To add a name server to the list of authoritative servers for the zone, you must specify both the server's IP address and its DNS name. When entering names, click Resolve to resolve the name to its IP address prior to adding it to the list.

Secondary zones cannot be AD-integrated under any circumstances.

You want to be sure Server2 can host, you do not want to delegate a zone.

Secondary Domain Name System (DNS) servers help provide load balancing and fault tolerance. Secondary DNS servers maintain a read-only copy of zone data that is transferred periodically from the primary DNS server for the zone. You can configure DNS clients to query secondary DNS servers instead of (or in addition to) the primary DNS server for a zone, reducing demand on the primary server and ensuring that DNS queries for the zone will be answered even if the primary server is not available.

How-To: Configure a secondary DNS Server in Windows Server 2012

We need to tell our primary DNS that it is ok for this secondary DNS to pull information from it. Otherwise replication will fail and you will get this big red X.
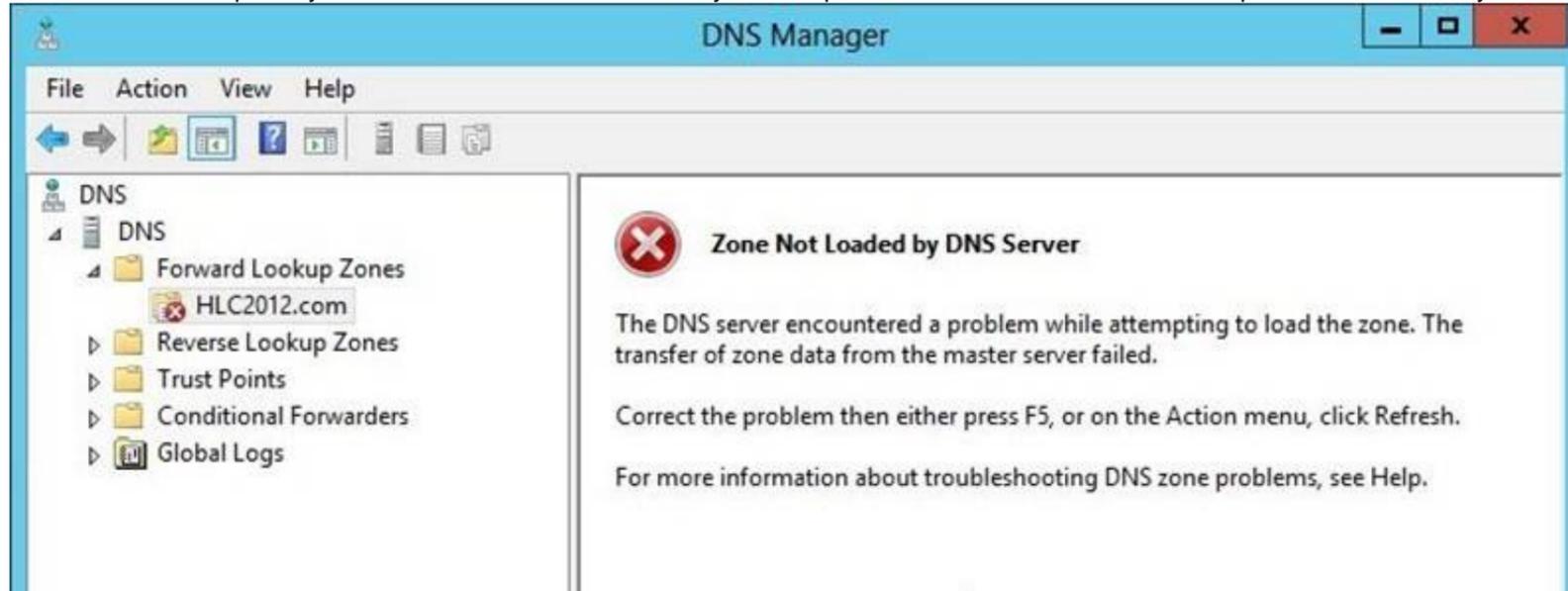
Head over to your primary DNS server, launch DNS manager, expand Forward Lookup Zones, navigate to your primary DNS zone, right-click on it and go to Properties.
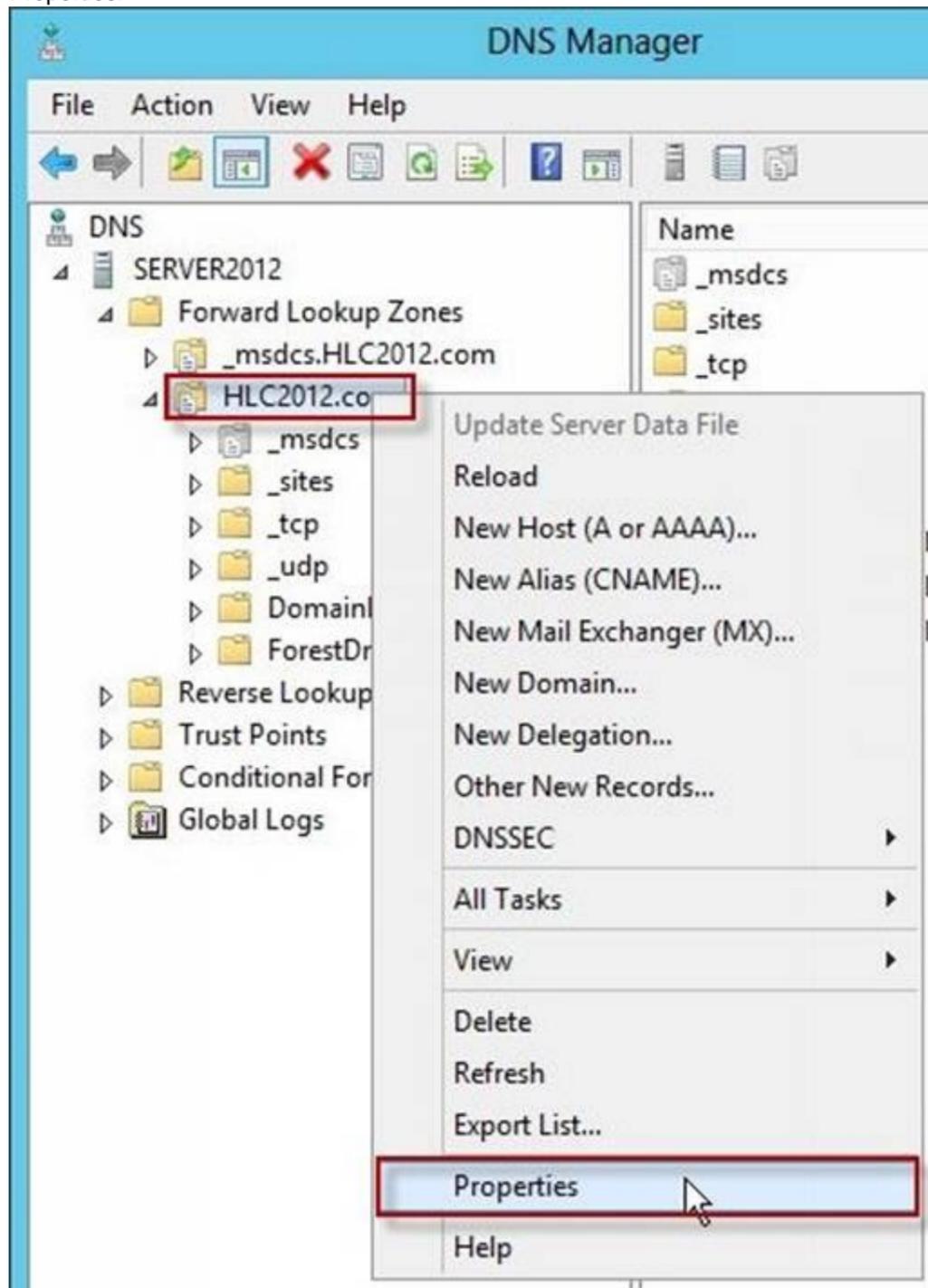
Go to "Zone Transfers" tab, by default, for security reasons, the "Allow zone transfers: " is un-checked to protect your DNS information. We need to allow zone transfers, if you value your DNS records, you do not want to select "To any server" but make sure you click on "Only to servers listed on the Name Servers tab".
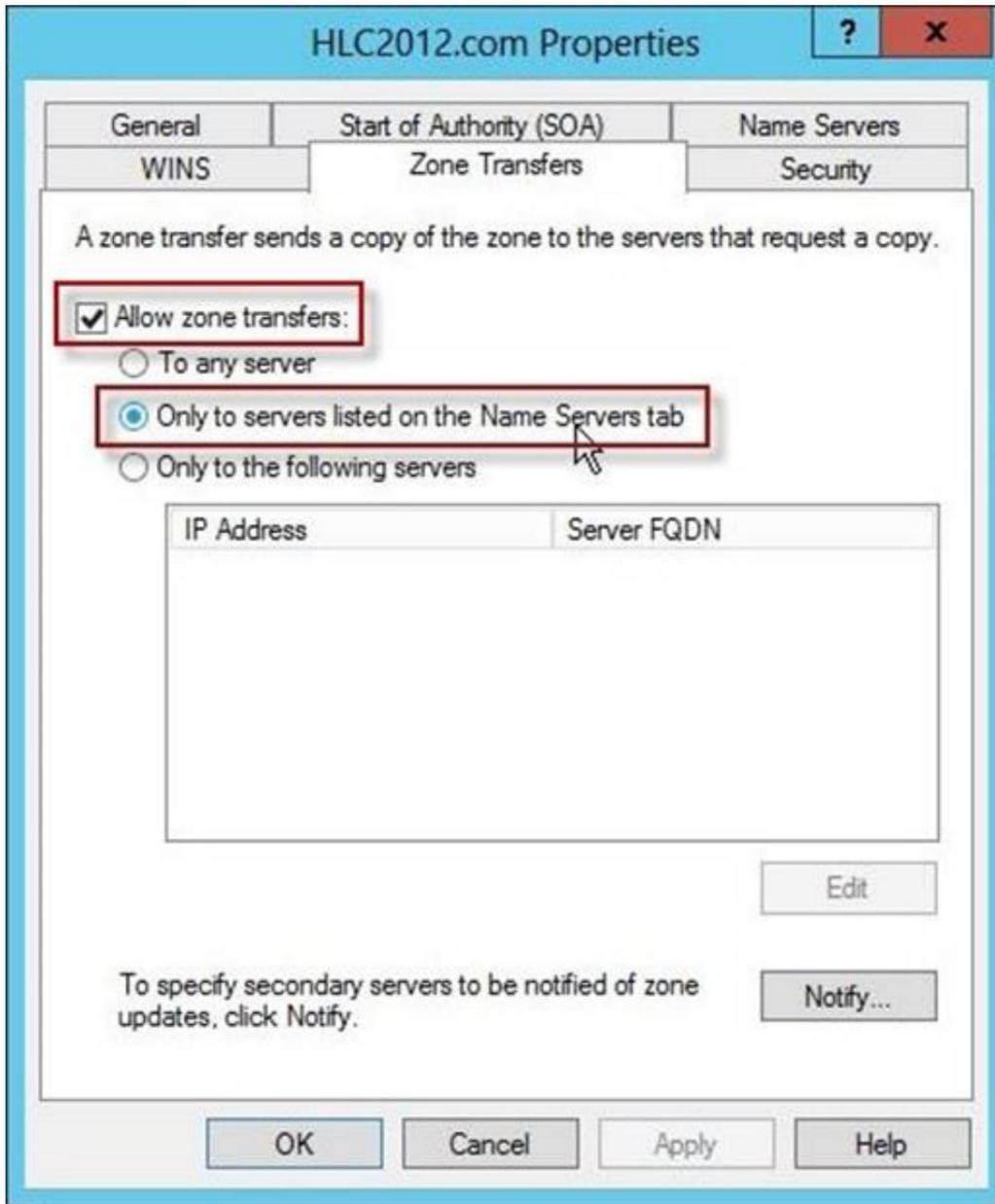
Head over to the "Name Servers" tab, click Add.
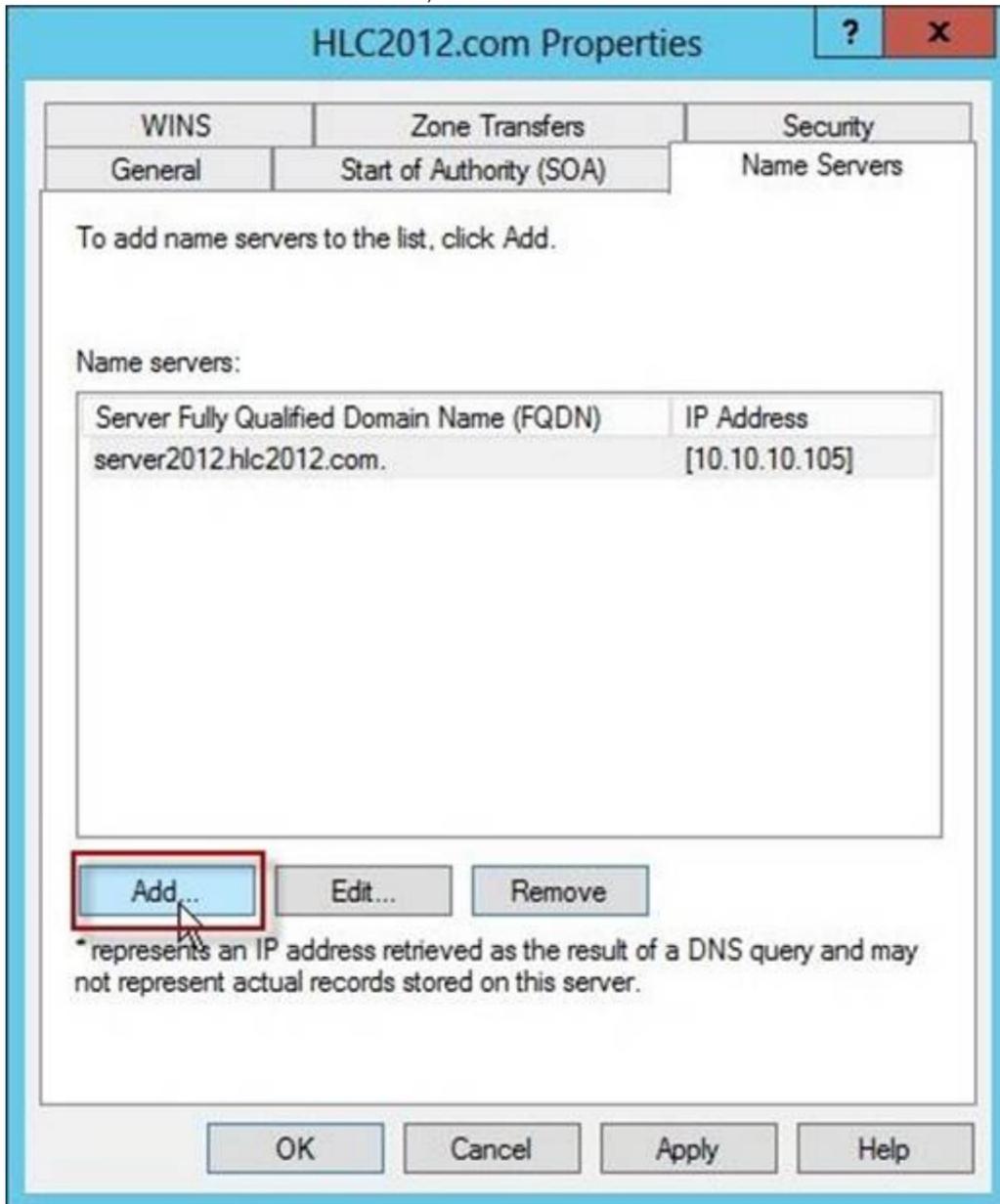
You will get "New Name Server Record" window, type in the name of your secondary DNS server. it is always better to validate by name not IP address to avoid future problems in case your IP addresses change. Once done, click OK.
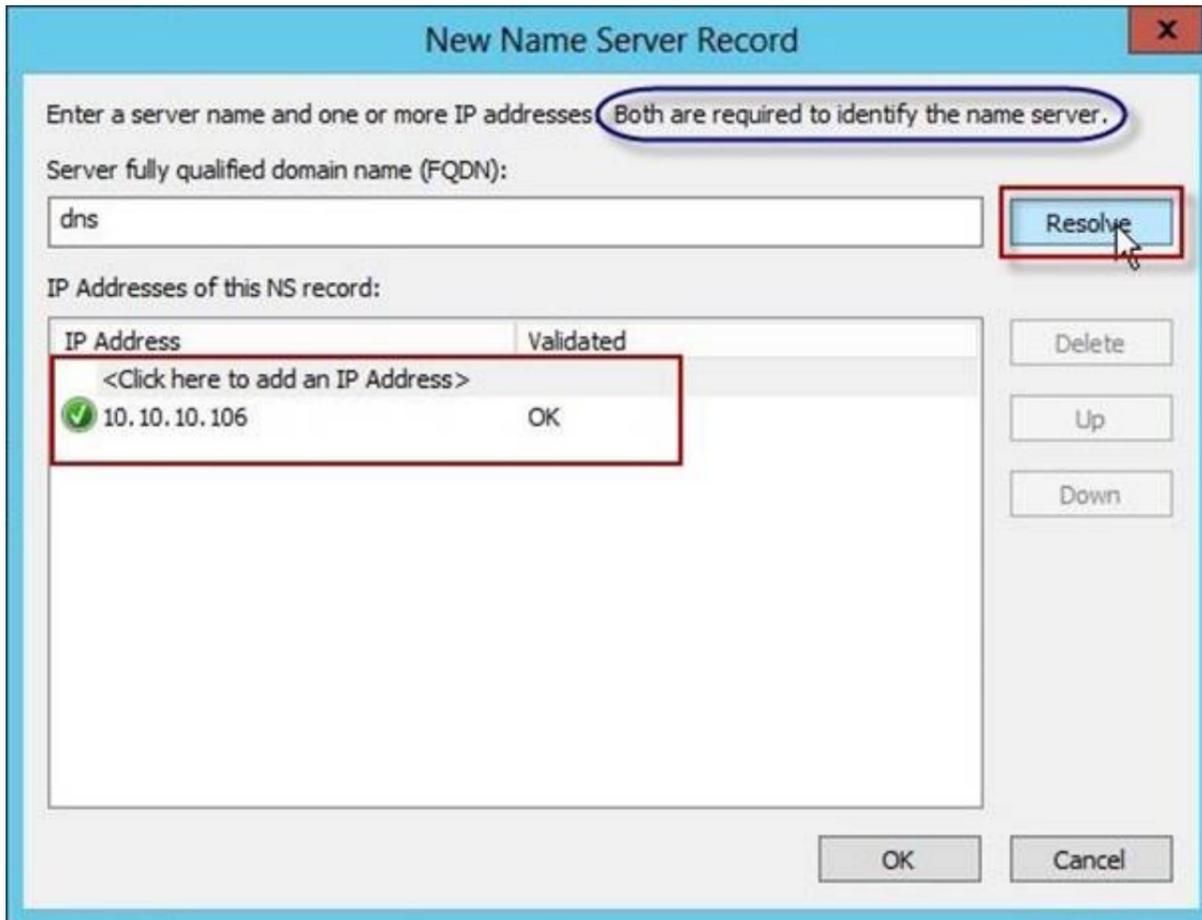
You will see your secondary DNS server is now added to your name servers selection, click OK.
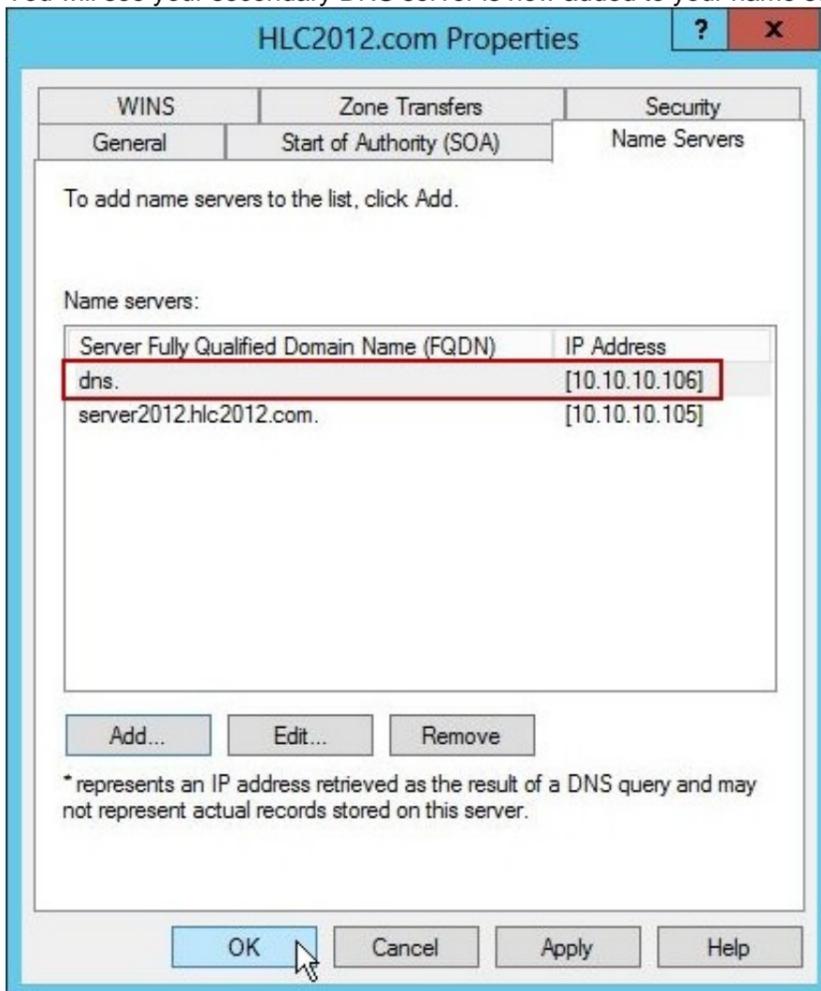
Now if you head back to your secondary DNS server and refresh, the big red X will go away and your primary zone data will populate.
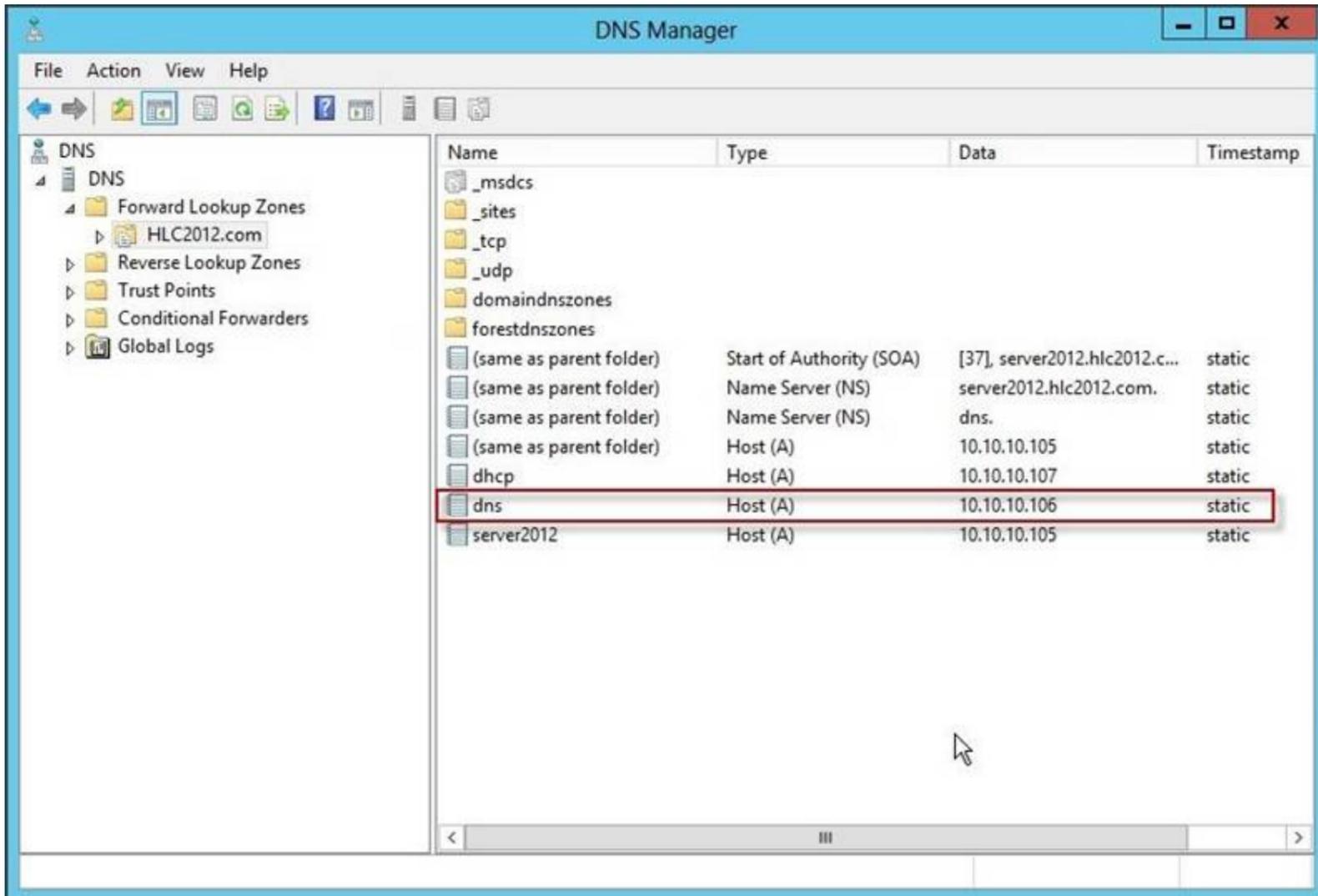
Your secondary DNS is fully setup now. You cannot make any DNS changes from your secondary DNS. Secondary DNS is a read-only DNS, Any DNS changes have to be done from the primary DNS.

References:

http: //technet. microsoft. com/en-us/library/cc816885%28v=ws. 10%29. aspx

http: //technet. microsoft. com/en-us/library/cc816814%28v=ws. 10%29. aspx

http: //blog. hyperexpert. com/how-to-configure-a-secondary-dns-server-in-windows-server- 2012/

http: //technet. microsoft. com/en-us/library/cc770984. aspx

http: //support. microsoft. com/kb/816101

http: //technet. microsoft. com/en-us/library/cc753500. aspx

http: //technet. microsoft. com/en-us/library/cc771640(v=ws. 10). aspx

http: //technet.microsoft.com/en-us/library/ee649280(v=ws. 10). aspx

NEW QUESTION 87

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains three member servers named Server1, Server2, and Server3. All servers run Windows Server 2012 R2 and have the Windows Server Update Services (WSUS) server role installed.

Server1 and Server2 are configured as replica servers that use Server3 as an upstream server.

You remove Servers from the network.

You need to ensure that WSUS on Server2 retrieves updates from Server1. The solution must ensure that Server1 and Server2 have the latest updates from Microsoft.

Which command should you run on each server? To answer, select the appropriate command to run on each server in the answer area.

Server1

| set-wsusserversynchronization –syncfrommu |
| set-wsusserversynchronization –useservername server1 |
| set-wsusserversynchronization –useservername server2 |
| wsusutil.exe movecontent \\server1\c$ |
| wsusutil.exe movecontent \\server2\c$ |

Server2

| set-wsusserversynchronization –syncfrommu |
| set-wsusserversynchronization –useservername server1 |
| set-wsusserversynchronization –useservername server2 |
| wsusutil.exe movecontent \\server1\c$ |
| wsusutil.exe movecontent \\server2\c$ |

Answer:

Explanation: Set-WsusServerSynchronization-SyncFromMU [-UpdateServer<IUpdateServer>] [- Confirm] [-WhatIf] [<CommonParameters>]
Set-WsusServerSynchronization-UssServerName<String> [-PortNumber<Int32>] [- Replica] [-UpdateServer<IUpdateServer>] [-UseSsl] [-Confirm] [-WhatIf] [<CommonParameters>]
The Set-WsusServerSynchronizationcmdlet sets whether the Windows Server Update Services (WSUS) server synchronizes from Microsoft Update or an upstream server. This cmdlet allows the user to specify settings such as the upstream server name, the port number, and whether or not to use Secure Sockets Layer (SSL).
References:
http: //technet. microsoft. com/en-us/library/hh826163. aspx
http: //technet. microsoft. com/en-us/library/cc708480%28v=ws. 10%29. aspx

NEW QUESTION 90
HOTSPOT
You have a server named Server1 that has the Web Server (IIS) server role installed. You obtain a Web Server certificate.
You need to configure a website on Server1 to use Secure Sockets Layer (SSL).
To which store should you import the certificate? To answer, select the appropriate store in the answer area.
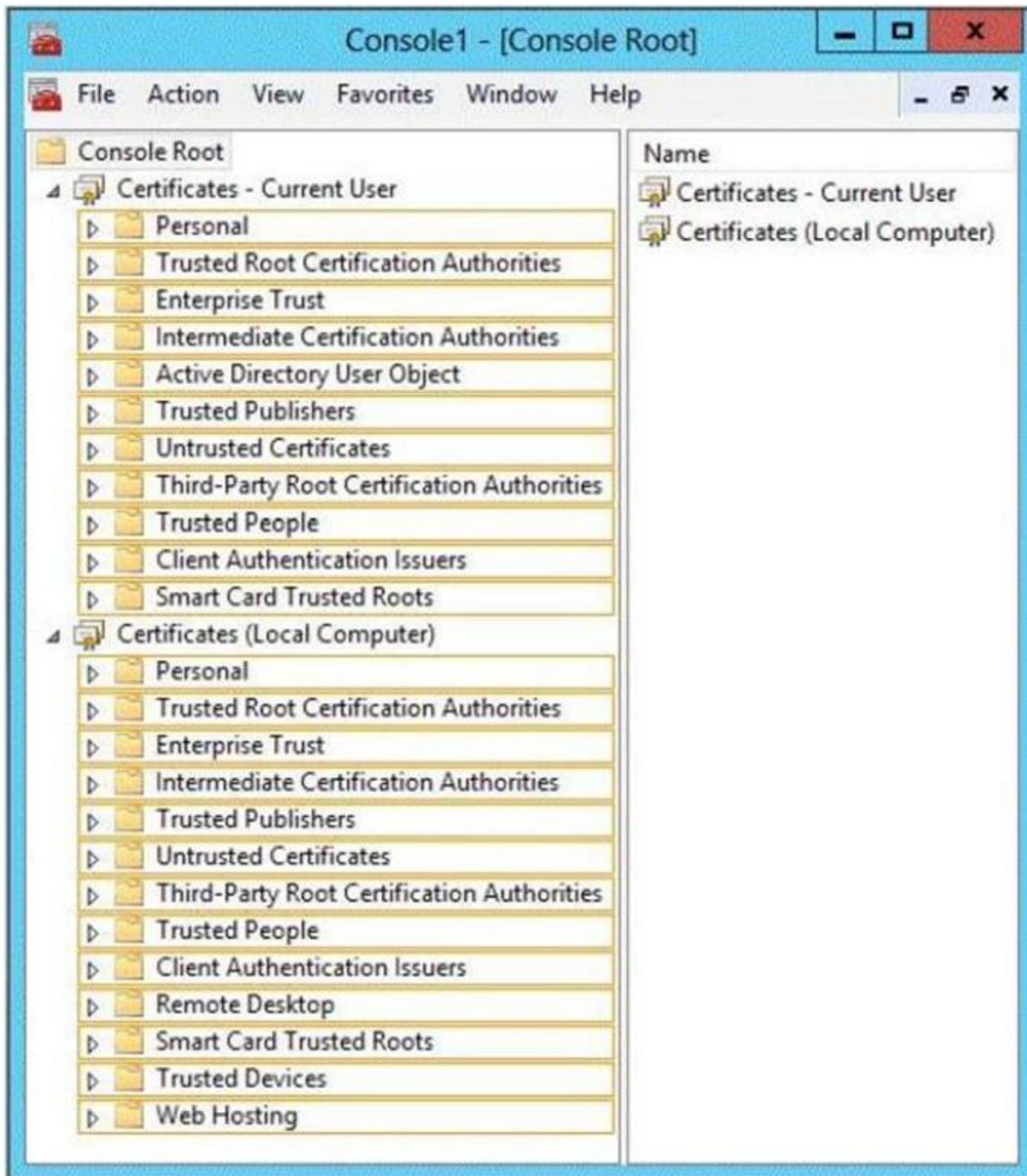
Answer:

Explanation: http: //technet.microsoft.com/en-us/library/cc740068(v=ws.10).aspx
When you enable secure communications (SSL and TLS) on an Internet Information Services (IIS) computer, you must first obtain a server certificate.
If it is a Self-Signed certificate, it only can be used on the local server machine.
If it is a public certificate, you'll need to download the CA root certificate of the certificate and install the CA root certificate into the Trusted Root Certificate Authorities store.
Root certificates provide a level of trust that certificates that are lower in the hierarchy can inherit. Each certificate is inspected for a parent certificate until the search reaches the root
certificate.
For more information about certificate, please refer to: References:
http: //technet.microsoft.com/en-us/library/cc700805.aspx http: //support.microsoft.com/kb/232137/en-us
http: //www.sqlservermart.com/HowTo/Windows_Import_Certificate.aspx
http: //msdn.microsoft.com/en-us/library/windows/hardware/ff553506%28v=vs.85%29.aspx
http: //www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis
http: //support.microsoft.com/kb/299875/en-us
http: //technet.microsoft.com/en-us/library/dd163531.aspx
http://blogs.msdn.com/b/mosharaf/archive/2006/10/30/using-test-certificate-with-reporting-services-2005-to-establish-ssl-connection.aspx

NEW QUESTION 91
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 is configured as a VPN server.
You need to configure Server1 to perform network address translation (NAT). What should you do?

A. From Network Connections, modify the Internet Protocol Version 4 (TCP/IPv4) setting of each network adapter.
B. From Network Connections, modify the Internet Protocol Version 6 (TCP/IPv6) setting of each network adapter.
C. From Routing and Remote Access, add an IPv6 routing protocol.
D. From Routing and Remote Access, add an IPv4 routing protocol.

Answer: D

Explanation: To configure an existing RRAS server to support both VPN remote access and NAT routing:
1. Open Server Manager.
2. Expand Roles, and then expand Network Policy and Access Services.
3. Right-click Routing and Remote Access, and then click Properties.
4. Select IPv4 Remote access Server or IPv6 Remote access server, or both.

NEW QUESTION 95
Your network contains an Active Directory domain named contoso.com. The domain contains five servers. The servers are configured as shown in the following table.

Server name	Configuration
Server1	Domain controller
Server2	DHCP server
Server3	DNS server
Server4	Network Policy Server (NPS)
Server5	Windows Deployment Services (WDS)

All desktop computers in contoso.com run Windows 8 and are configured to use BitLocker Drive Encryption (BitLocker) on all local disk drives.
You need to deploy the Network Unlock feature. The solution must minimize the number of features and server roles installed on the network.
To which server should you deploy the feature?

A. Server1
B. Server2
C. Server3
D. Server4
E. Server5

Answer: E

Explanation: The BitLocker Network Unlock feature will install the WDS role if it is not already installed. If you want to install it separately before you install BitLocker Network Unlock you can use Server Manager or Windows PowerShell. To install the role using Server Manager, select the Windows Deployment Services role in Server Manager.

NEW QUESTION 99
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. All of the DNS servers in both of the domains run Windows Server 2012 R2.
The network contains two servers named Server1 and Server2. Server1 hosts an Active Directory-integrated zone for contoso.com. Server2 hosts an Active Directory-integrated zone for fabrikam.com. Server1 and Server2 connect to each other by using a WAN link.
Client computers that connect to Server1 for name resolution cannot resolve names in fabnkam.com.
You need to configure Server1 to support the resolution of names in fabnkam.com. The solution must ensure that users in contoso.com can resolve names in fabrikam.com if the WAN link fails.
What should you do on Server1?

A. Create a stub zone.
B. Add a forwarder.
C. Create a secondary zone.
D. Create a conditional forwarder.

Answer: C

Explanation: http: //technet. microsoft. com/en-us/library/cc771898. aspx
When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone.
With secondary, you have ability to resolve records from the other domain even if its DNS servers are temporarily unavailable.
While secondary zones contain copies of all the resource records in the corresponding zone on the master name server, stub zones contain only three kinds of resource records: A copy of the SOA record for the zone.
Copies of NS records for all name servers authoritative for the zone. Copies of A records for all name servers authoritative for the zone.
References:
http: //www. windowsnetworking. com/articles-tutorials/windows-2003/DNS_Stub_Zones. html
http: //technet. microsoft. com/en-us/library/cc771898. aspx
http: //redmondmag. com/Articles/2004/01/01/The-Long-and-Short-of-Stub-Zones. aspx?Page=2

NEW QUESTION 101
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Server1 has the Network Policy Server server role installed. Server2 has the DHCP Server server role installed. Both servers run Windows Server 2012 R2.
You are configuring Network Access Protection (NAP) to use DHCP enforcement. You configure a DHCP scope as shown in the exhibit. (Click the Exhibit button.)

Scope [192.168.10.0] Scope1 Properties

General | DNS | Network Access Protection | Advanced

Network Access Protection

You can setup the Network Access Protection settings for this scope here.

Network Access Protection Settings

- ⦿ Enable for this scope

  - ○ Use default Network Access Protection profile
  - ⦿ Use custom profile

    Profile Name

    Profile1

- ○ Disable for this scope

[OK] [Cancel] [Apply]
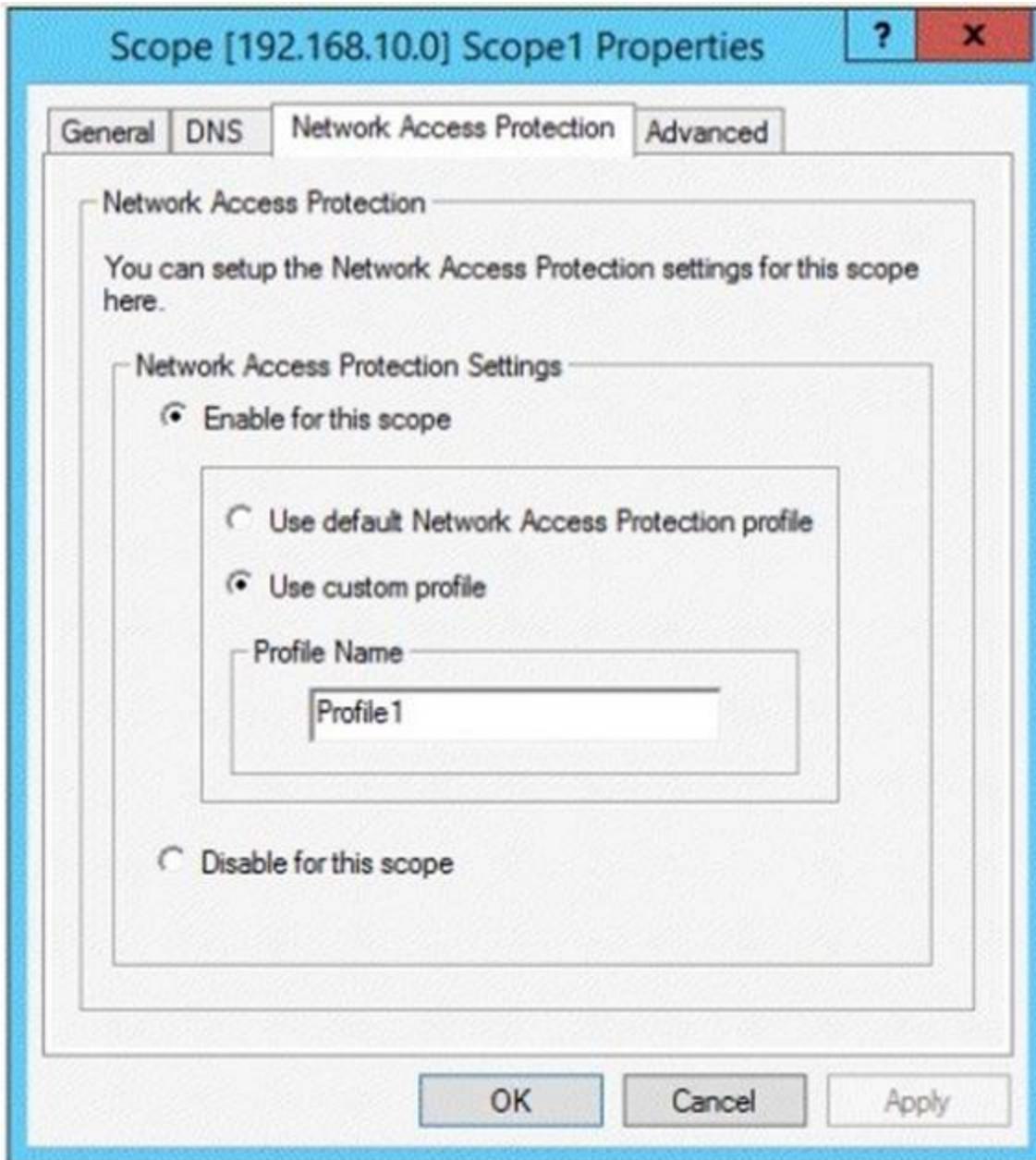
You need to ensure that non-compliant NAP clients receive different DHCP options than compliant NAP clients.
What should you configure on each server? To answer, select the appropriate options for each server in the answer area.

Answer Area

Server1: [▼]

Server2: [▼]

Answer Area

Server1: [▼]
Health Policies
Identity-Type
MS-Service Class
Service-Type

Server2: [▼]
filters
a policy
scope options
server options
a User class
a Vendor class

Answer:

Explanation: Health Policies Server Options
* Health policy on the NAP server.
* The DHCP server must be NAP enabled.
Note: With DHCP enforcement, a computer must be compliant to obtain an unlimited access IP address configuration from a DHCP server. For noncompliant computers, network access is limited by an IP address configuration that allows access only to the restricted network. DHCP enforcement enforces health policy requirements every time a DHCP client attempts to lease or renew an IP address configuration. DHCP enforcement also actively monitors the health status of the

NAP client and renews the IPv4 address configuration for access only to the restricted network if the client becomes noncompliant.

Topic 2, Exam Set B

NEW QUESTION 103
Your company deploys a new Active Directory forest named contoso.com. The first domain controller in the forest runs Windows Server 2012 R2. The forest contains a domain controller named DC10.
On DC10, the disk that contains the SYSVOL folder fails.
You replace the failed disk. You stop the Distributed File System (DFS) Replication service. You restore the SYSVOL folder.
You need to perform a non-authoritative synchronization of SYSVOL on DC10.
Which tool should you use before you start the DFS Replication service on DC10?

A. Dfsgui.msc
B. Dfsmgmt.msc
C. Adsiedit.msc
D. Ldp

Answer: C

Explanation: How to perform a non-authoritative synchronization of DFSR-replicated SYSVOL (like "D2" for FRS)
? In the ADSIEDIT. MSC tool modify the following distinguished name (DN) value and attribute on each of the domain controllers that you want to make non-authoritative:
CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR- LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain> msDFSR-Enabled=FALSE
? Force Active Directory replication throughout the domain.
? Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:
DFSRDIAG POLLAD
? You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated.
? On the same DN from Step 1, set: msDFSR-Enabled=TRUE
? Force Active Directory replication throughout the domain.
? Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:
DFSRDIAG POLLAD
? You will see Event ID 4614 and 4604 in the DFSR event log indicating SYSVOL has been initialized. That domain controller has now done a "D2" of SYSVOL.
Note: Active Directory Service Interfaces Editor (ADSI Edit) is a Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory. ADSI Edit (adsiedit. msc) provides a view of every object and attribute in an Active Directory forest. You can use ADSI Edit to query, view, and edit attributes that are not exposed through other Active Directory Microsoft Management Console (MMC) snap- ins: Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and Active Directory Schema.

NEW QUESTION 106
Your network contains an Active Directory domain named contoso.com.
You create a user account named User1. The properties of User1 are shown in the exhibit. (Click the Exhibit button.)
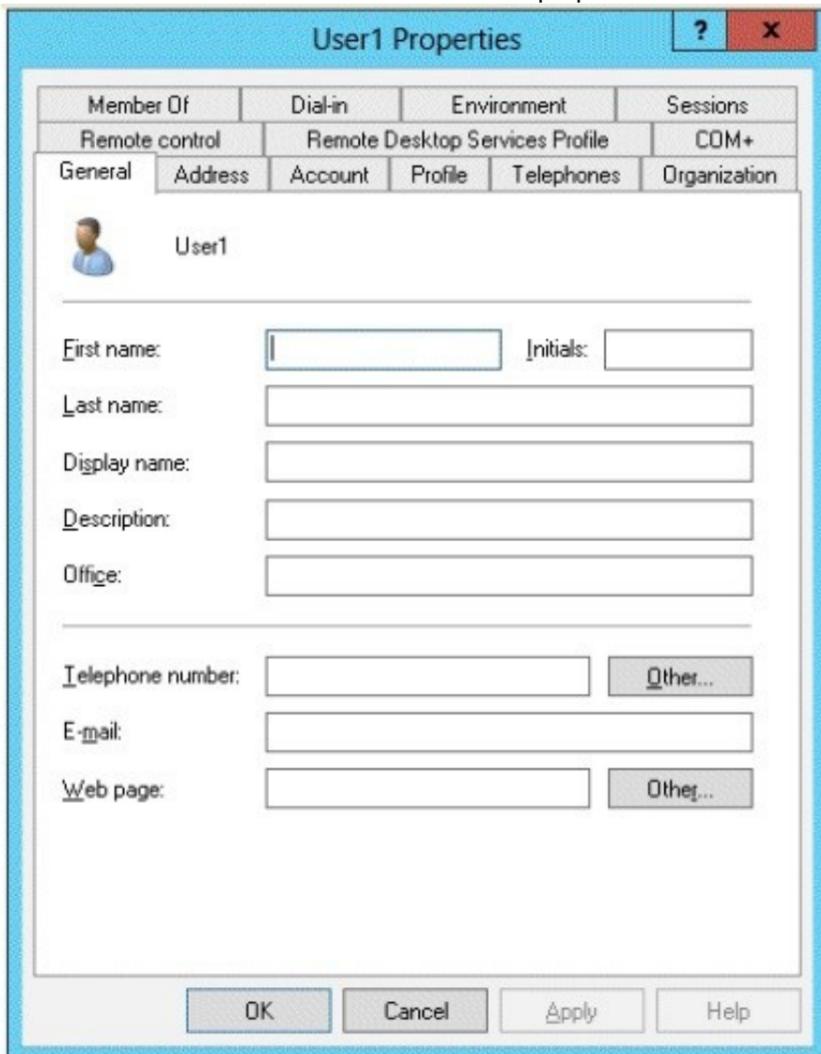
You plan to use the User1 account as a service account. The service will forward authentication requests to other servers.
You need to ensure that you can view the Delegation tab from the properties of the User1 account.
What should you do first?

A. Configure the Name Mappings of User1.
B. Modify the user principal name (UPN) of User1.

C. Configure a Service Principal Name (SPN) for User1.
D. Modify the Security settings of User1.

Answer: C

Explanation: If you cannot see the Delegation tab, do one or both of the following:
Register a Service Principal Name (SPN) for the user account with the Setspn utility in the support tools on your CD. Delegation is only intended to be used by service accounts, which should have registered SPNs, as opposed to a regular user account which typically does not have SPNs.
Raise the functional level of your domain to Windows Server 2003. For more information, see Related Topics.
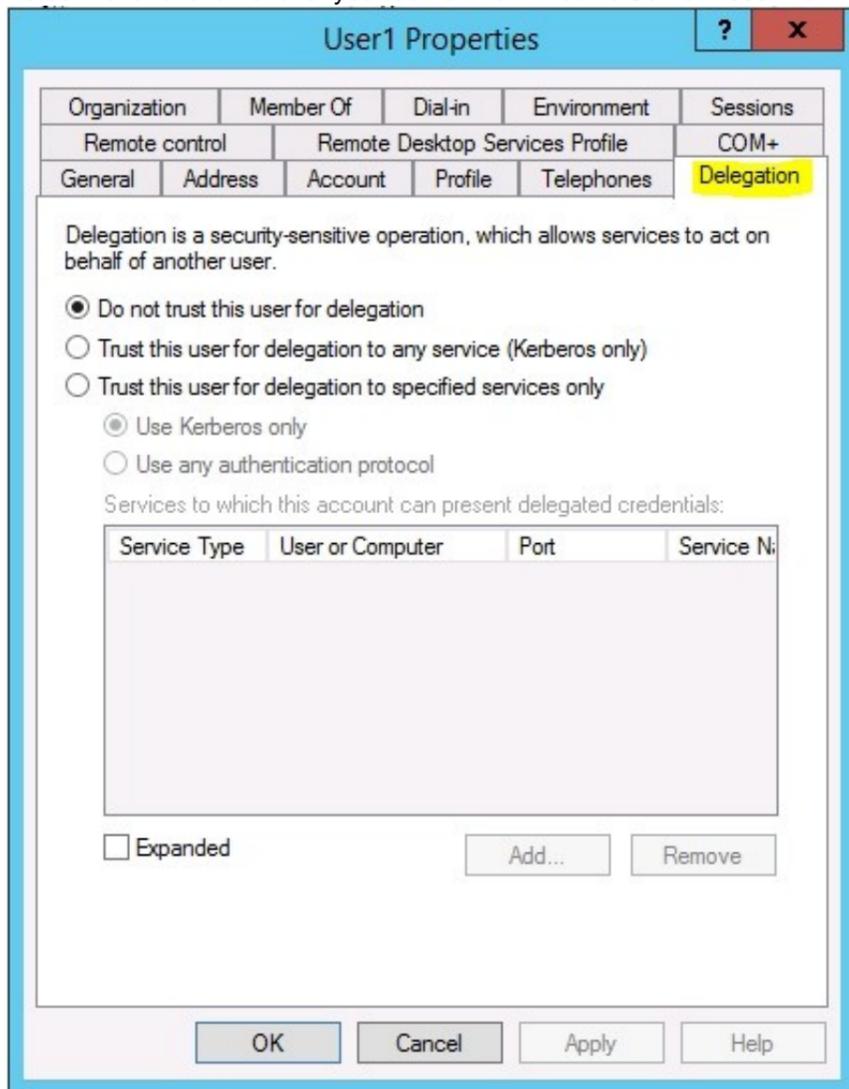
References:
http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set. aspx
http: //blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set. aspx
http: //technet. microsoft. com/en-us/library/cc739474(v=ws. 10). aspx
http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set. aspx

NEW QUESTION 110
HOTSPOT
Your network contains a RADIUS server named Admin1.
You install a new server named Server2 that runs Windows Server 2012 R2 and has Network Policy Server (NPS) installed.
You need to ensure that all accounting requests for Server2 are forwarded to Admin1. On Server2, you create a new remote RADIUS server group named Group1 that contains
Admin1.
What should you configure next on Server2?
To answer, select the appropriate node in the answer area.
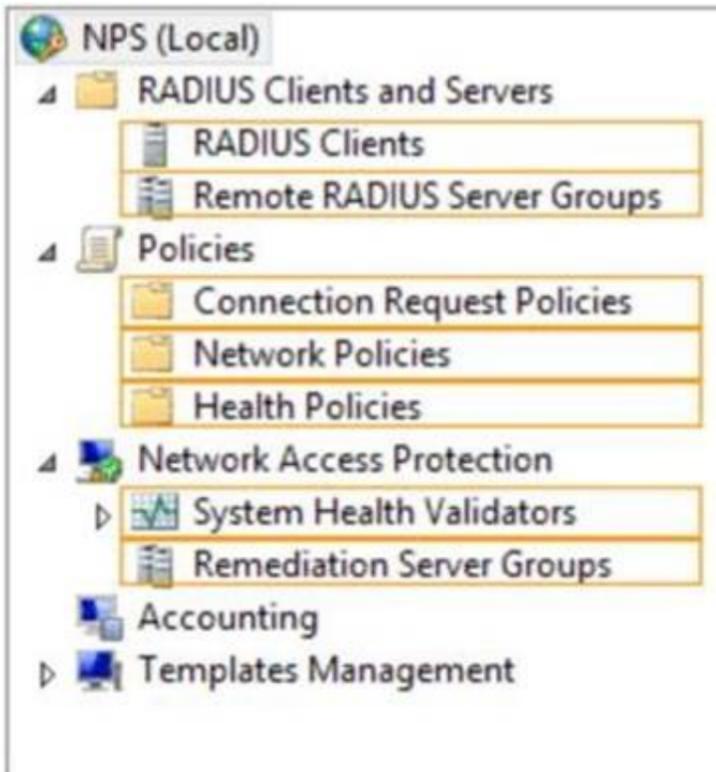
Answer:

Explanation: Connection request policies are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User Service (RADIUS) servers perform the authentication and authorization of connection requests that the server running Network Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS servers are used for RADIUS accounting.

NEW QUESTION 111
You have a DNS server named Server1.
Server1 has a primary zone named contoso.com.
Zone Aging/Scavenging is configured for the contoso.com zone.
One month ago, an administrator removed a server named Server2 from the network.
You discover that a static resource record for Server2 is present in contoso.com. Resource records for decommissioned client computers are removed automatically from contoso.com.
You need to ensure that the static resource records for all of the servers are removed automatically from contoso.com.
What should you modify?

A. The Expires after value of contoso.com
B. The Record time stamp value of the static resource records
C. The time-to-live (TTL) value of the static resource records
D. The Security settings of the static resource records

Answer: B

Explanation: Reset and permit them to use a current (non-zero) time stamp value. This enables these records to become aged and scavenged.
You can use this procedure to change how a specific resource record is scavenged.
A stale record is a record where both the No-Refresh Interval and Refresh Interval have passed without the time stamp updating.
DNS->View->Advanced
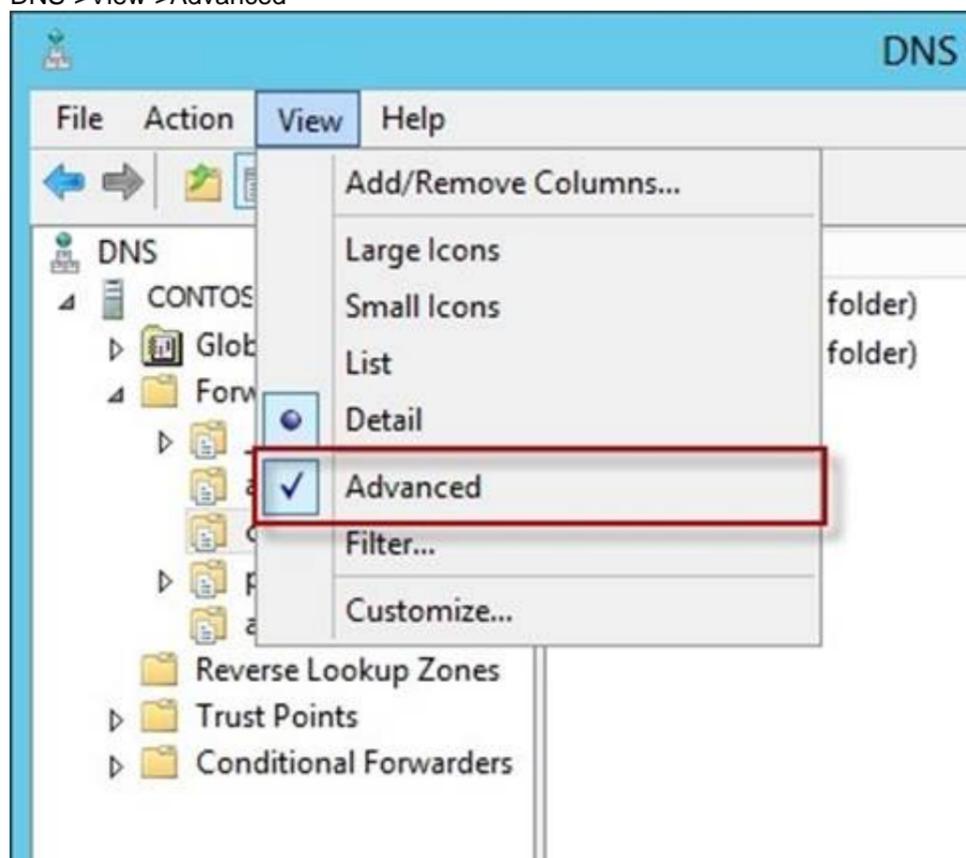
Depending on the how the resource record was originally added to the zone, do one of the following:

If the record was added dynamically using dynamic update, clear the Delete this record when it becomes stale check box to prevent its aging or potential removal during the scavenging process. If dynamic updates to this record continue to occur, the Domain Name System (DNS) server will always reset this check box so that the dynamically updated record can be deleted.

If you added the record statically, select the Delete this record when it becomes stale check box to permit its aging or potential removal during the scavenging process.

References:

http: //technet. microsoft. com/en-us/library/cc759204%28v=ws. 10%29. aspx http: //technet. microsoft. com/en-us/library/cc759204%28v=ws. 10%29. aspx

Typically, stale DNS records occur when a computer is permanently removed from the network. Mobile users who abnormally disconnect from the network can also cause stale DNS records. To help manage stale records, Windows adds a time stamp to dynamically added resource records in primary zones where aging and scavenging are enabled. Manually added records are time stamped with a value of 0, and they are automatically excluded from the aging and scavenging process.

To enable aging and scavenging, you must do the following:

Resource records must be either dynamically added to zones or manually modified to be used in aging and scavenging operations.

Scavenging and aging must be enabled both at the DNS server and on the zone. Scavenging is disabled by default.
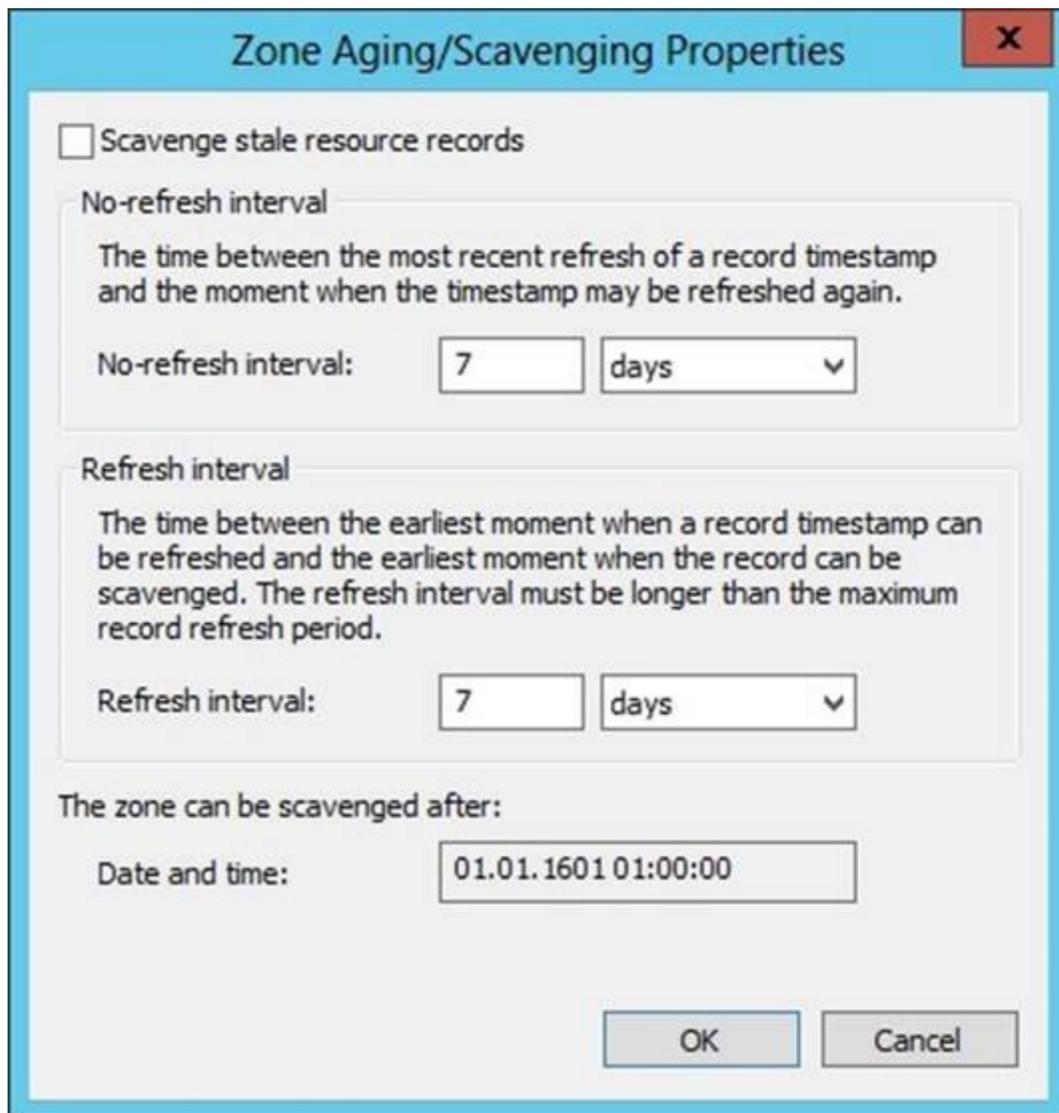
DNS scavenging depends on the following two settings:

No-refresh interval: The time between the most recent refresh of a record time stamp and the moment when the time stamp can be refreshed again. When scavenging is enabled, this is set to 7 days by default.

Refresh interval: The time between the earliest moment when a record time stamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period. When scavenging is enabled, this is set to 7 days by default.

A DNS record becomes eligible for scavenging after both the no-refresh and refresh intervals have elapsed. If the default values are used, this is a total of 14 days.

References:
http: //technet. microsoft. com/en-us/library/cc759204%28v=ws. 10%29. aspx
http: //technet. microsoft. com/en-us/library/cc759204%28v=ws. 10%29. aspx
http: //technet. microsoft. com/en-us/library/cc771570. aspx
http: //technet. microsoft. com/en-us/library/cc771677. aspx
http: //technet. microsoft. com/en-us/library/cc758321(v=ws. 10). aspx

NEW QUESTION 112
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
The domain contains an Edge Server named Server1. Server1 is configured as a DirectAccess server. Server1 has the following settings:

Internal DNS name: server1.contoso.com
External DNS name: da1.contoso.com
Internal IPv6 address: 2002:c1a8:6a:3333::1
External IPv4 address: 65.55.37.62

You run the Remote Access Setup wizard as shown in the following exhibit. (Click the Exhibit button.)
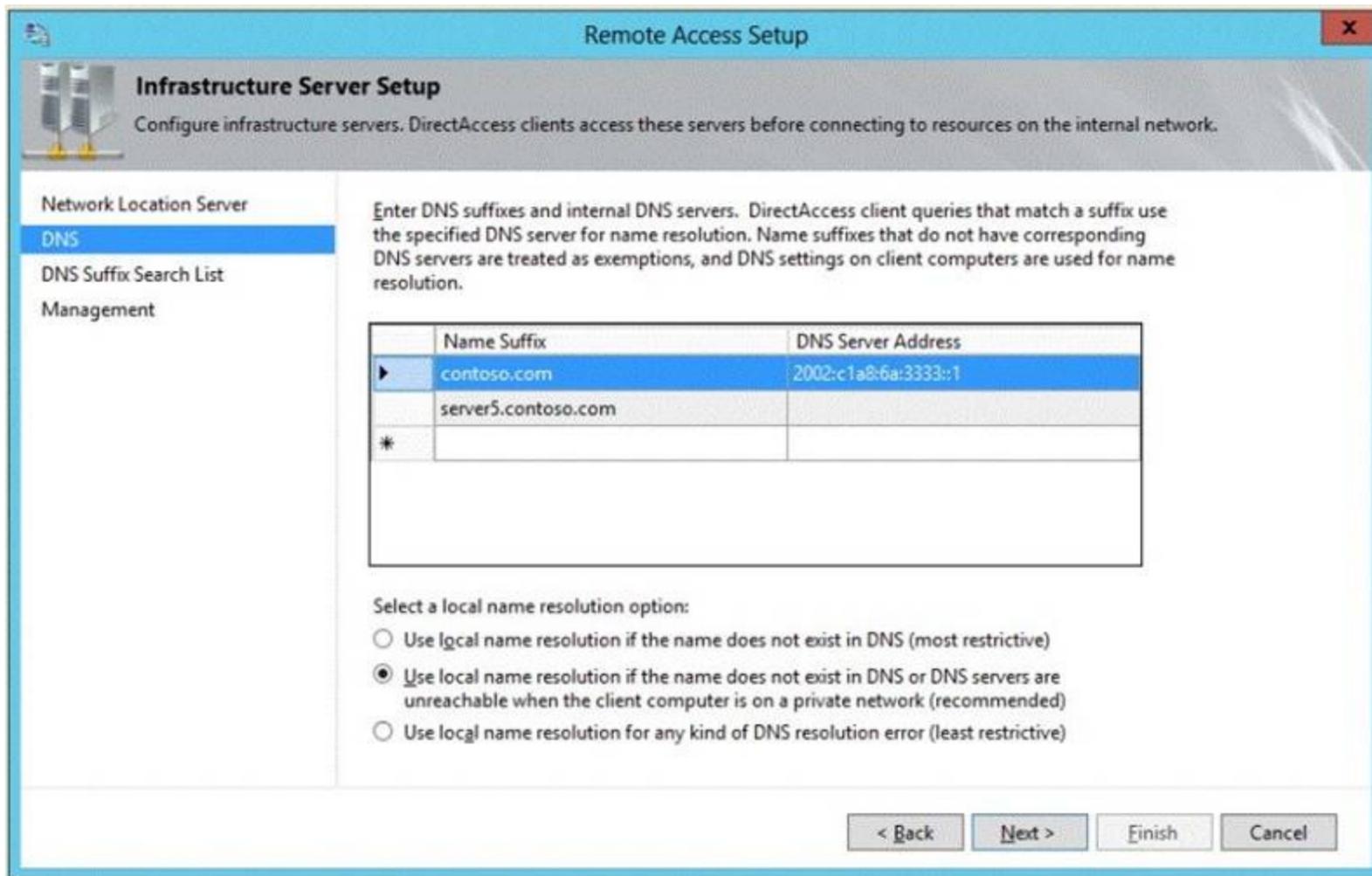
You need to ensure that client computers on the Internet can establish DirectAccess connections to Server1.
Which additional name suffix entry should you add from the Remote Access Setup wizard?

A. A Name Suffix value of dal.contoso.com and a blank DNS Server Address value
B. A Name Suffix value of Server1.contoso.com and a DNS Server Address value of 65.55.37.62
C. A Name Suffix value of dal.contoso.com and a DNS Server Address value of 65.55.37.62
D. A Name Suffix value of Server1.contoso.com and a blank DNS Server Address value

Answer: A

Explanation: Split-brain DNS is the use of the same DNS domain for both Internet and intranet resources. For example, the Contoso Corporation is using split brain DNS; contoso.com is the domain name for intranet resources and Internet resources. Internet users use http:
//www.contoso.com to access Contoso's public Web site and Contoso employees on the Contoso intranet use http: //www.contoso.com to access Contoso's intranet Web site. A Contoso employee with their laptop that is not a DirectAccess client on the intranet that accesses http: //www.contoso.com sees the intranet Contoso Web site. When they take their laptop to the local coffee shop and access that same URL, they will see the public Contoso Web site.
When a DirectAccess client is on the Internet, the Name Resolution Policy Table (NRPT) sends DNS name queries for intranet resources to intranet DNS servers. A typical NRPT for DirectAccess will have a rule for the namespace of the organization, such as contoso.com for the Contoso Corporation, with the Internet Protocol version 6 (IPv6) addresses of intranet DNS servers. With just this rule in the NRPT, when a user on a DirectAccess client on the Internet attempts to access the uniform resource locator (URL) for their Web site (such as http: //www.contoso.com), they will see the intranet version. Because of this rule, they will never see the public version of this URL when they are on the Internet.
For split-brain DNS deployments, you must list the FQDNs that are duplicated on the Internet and intranet and decide which resources the DirectAccess client should reach, the intranet version or the public (Internet) version. For each name that corresponds to a resource for which you want DirectAccess clients to reach the public version, you must add the corresponding FQDN as an exemption rule to the NRPT for your DirectAccess clients. Name suffixes that do not have corresponding DNS servers are treated as exemptions.
References:
http: //technet. microsoft. com/en-us/library/ee382323(v=ws. 10). aspx

NEW QUESTION 114
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
A domain controller named DO has the ADMX Migrator tool installed. You have a custom Administrative Template file on DC1 named Template1.adm.
You need to add a custom registry entry to Template1.adm by using the ADMX Migrator tool.
Which action should you run first?

A. Load Template
B. New Policy Setting
C. Generate ADMX from ADM
D. New Category

Answer: C

Explanation: The ADMX Migrator provides two conversion methods — through the editor or through a command-line program. From the ADMX Editor, choose the option to Generate ADMX from ADM. Browse to your ADM file, and the tool quickly and automatically converts it. You then can open the converted file in the editor to examine its values and properties and modify it
if you wish. The ADMX Migrator Command Window is a little more complicated; it requires you to type a lengthy command string at a prompt to perform the conversions. However, it includes some options and flexibility not available in the graphical editor.

References:
http: //technet. microsoft. com/pt-pt/magazine/2008. 02. utilityspotlight%28en-us%29. aspx http: //technet. microsoft. com/pt-pt/magazine/2008. 02. utilityspotlight%28en-us%29. aspx
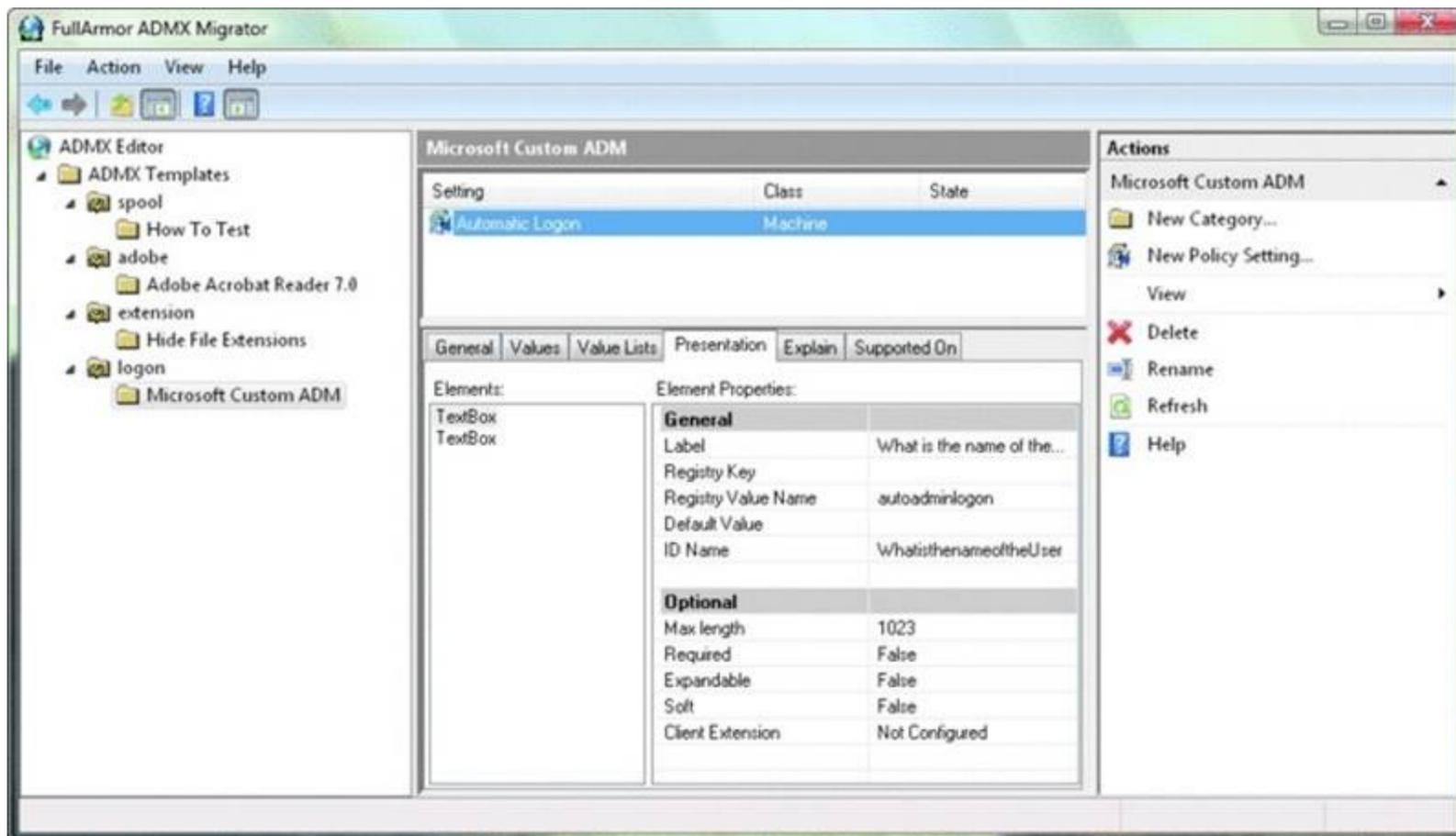
NEW QUESTION 116
Your network contains a single Active Directory domain named contoso.com. The domain contains a member server named Server1 that runs Windows Server 2012 R2.
Server1 has the Windows Server updates Services server role installed and is configured to download updates from the Microsoft Update servers.
You need to ensure that Server1 downloads express installation files from the Microsoft Update servers.
What should you do from the Update Services console?

A. From the Update Files and Languages options, configure the Update Files settings.
B. From the Automatic Approvals options, configure the Update Rules settings.
C. From the Products and Classifications options, configure the Products settings.
D. From the Products and Classifications options, configure the Classifications settings.

Answer: A

Explanation: To specify whether express installation files are downloaded during synchronization In the left pane of the WSUS Administration console, click Options.
In Update Files and Languages, click the Update Files tab.
If you want to download express installation files, select the Download express installation files check box. If you do not want to download express installation files, clear the check box.

Reference:
http: //technet. microsoft. com/en-us/library/cc708431. aspx
http: //technet. microsoft.com/en-us/library/cc708431. aspx
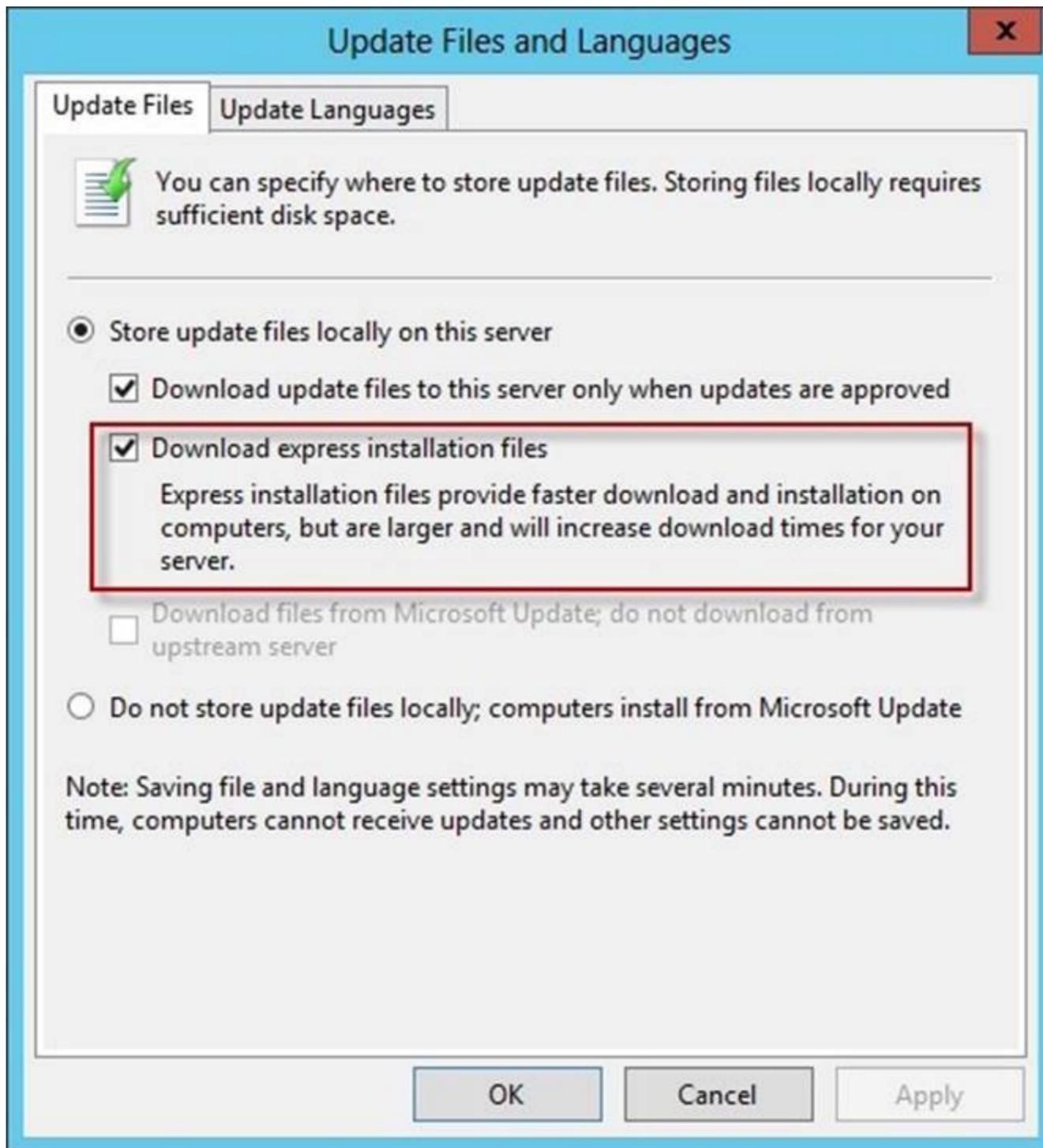
NEW QUESTION 120
Your network contains a single Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that hosts the primary DNS zone for contoso.com.
All servers dynamically register their host names.
You install three new Web servers that host identical copies of your company's intranet website. The servers are configured as shown in the following table.

Server name	IP address
WEB1.contoso.com	10.0.0.20
WEB2.contoso.com	10.0.0.21
WEB3.contoso.com	10.0.0.22

You need to use DNS records to load balance name resolution queries for intranet.contoso.com between the three Web servers.
What is the minimum number of DNS records that you should create manually?

A. 1
B. 3
C. 4
D. 6

Answer: B

Explanation: To create DNS Host (A) Records for all internal pool servers
1. Click Stabrt, click All Programs, click Administrative Tools, and then click DNS.
2. In DNS Manager, click the DNS Server that manages your records to expand it.
3. Click Forward Lookup Zones to expand it.
4. Right-click the DNS domain that you need to add records to, and then click New Host (A or AAAA).
5. In the Name box, type the name of the host record (the domain name will be automatically appended).
6. In the IP Address box, type the IP address of the individual Front End Server and then select Create associated pointer (PTR) record or Allow any authenticated user to update DNS records with the same owner name, if applicable.
7. Continue creating records for all member Front End Servers that will participate in DNS Load Balancing.
For example, if you had a pool named pool1.contoso.com and three Front End Servers, you would create the following DNS entries:

FQDN	Type	Data
Pool1.contoso.com	Host (A)	192.168.1.1
Pool1.contoso.com	Host (A)	192.168.1.2
Pool1.contoso.com	Host (A)	192.168.1.3

erence:
http: //technet. microsoft. com/en-us/library/cc772506. aspx
http: //technet. microsoft. com/en-us/library/gg398251. aspx

NEW QUESTION 123
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. All of the DNS servers in both of the domains run Windows Server 2012 R2.
The network contains two servers named Server1 and Server2. Server1 hosts an Active Directory-integrated zone for contoso.com. Server2 hosts an Active Directory-integrated zone for fabrikam.com. Server1 and Server2 connect to each other by using a WAN link.
Client computers that connect to Server1 for name resolution cannot resolve names in fabrikam.com.
You need to configure Server1 to resolve names in fabrikam.com. The solution must NOT require that changes be made to the fabrikam.com zone on Server2.
What should you create?

A. A trust anchor
B. A stub zone
C. A zone delegation
D. A secondary zone

Answer: B

Explanation: A stub zone is a copy of a zone that contains only those resource records necessary to identify the authoritative Domain Name System (DNS) servers for that zone. A stub zone is used to resolve names between separate DNS namespaces. This type of resolution may be necessary when a corporate merger requires that the DNS servers for two separate DNS namespaces resolve names for clients in both namespaces.

NEW QUESTION 124
HOTSPOT
Your network contains an Active Directory domain named contoso.com. All client computers are configured as DHCP clients.
You link a Group Policy object (GPO) named GPO1 to an organizational unit (OU) that contains all of the client computer accounts.
You need to ensure that Network Access Protection (NAP) compliance is evaluated on all of the client computers.
Which two settings should you configure in GPO1?
To answer, select the appropriate two settings in the answer area.

Answer:

Explanation:
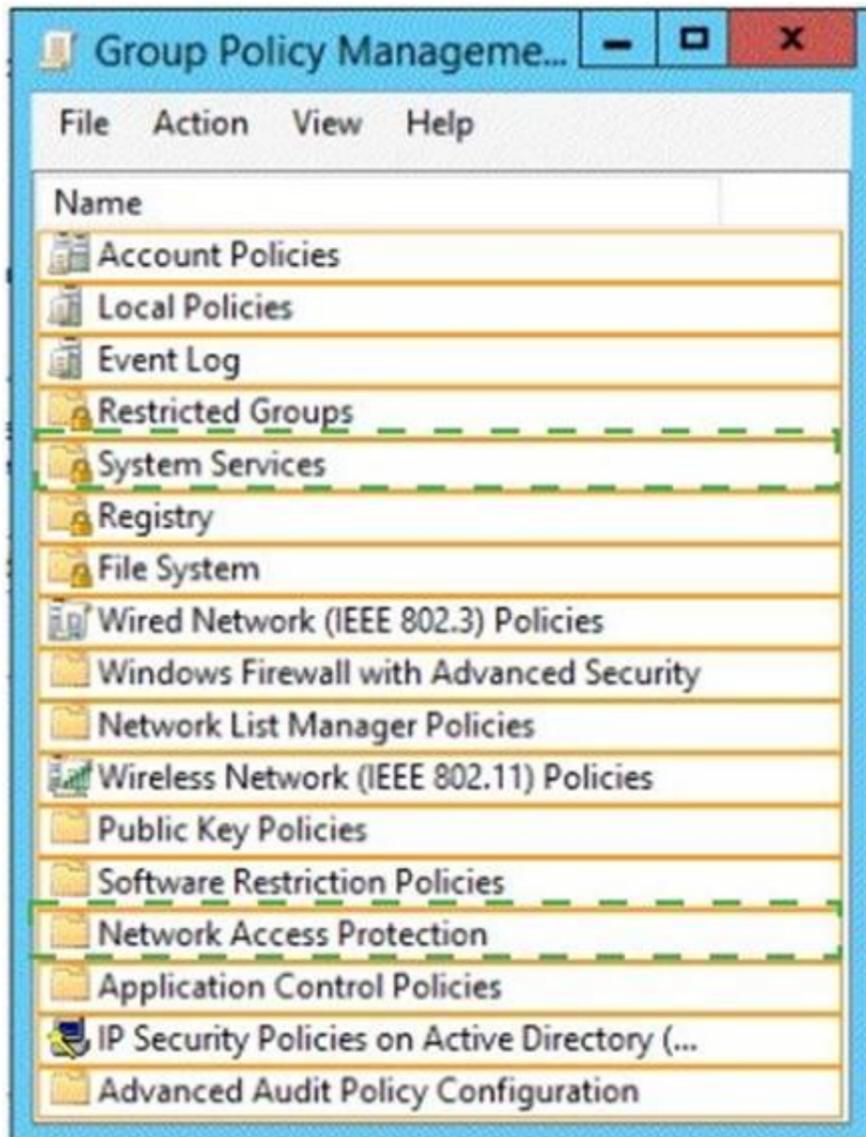
NEW QUESTION 129
You have a failover cluster that contains five nodes. All of the nodes run Windows Server 2012 R2. All of the nodes have BitLocker Drive Encryption (BitLocker) enabled.
You enable BitLocker on a Cluster Shared Volume (CSV).
You need to ensure that all of the cluster nodes can access the CSV. Which cmdlet should you run next?

A. Unblock-Tpm
B. Add-BitLockerKeyProtector
C. Remove-BitLockerKeyProtector
D. Enable BitLockerAutoUnlock

Answer: B

Explanation: 4. Add an Active Directory Security Identifier (SID) to the CSV disk using the Cluster Name Object (CNO) The Active Directory protector is a domain security identifier (SID) based protector for protecting clustered volumes held within the Active Directory infrastructure. It can be bound to a user account, machine account or group. When an unlock request is made for a protected volume, the BitLocker service interrupts the request and uses the BitLocker protect/unprotect APIs to unlock or deny the request. For the cluster service to selfmanage
BitLocker enabled disk volumes, an administrator must add the Cluster Name Object (CNO), which is the Active Directory identity associated with the Cluster Network name, as a BitLocker protector to the target disk volumes.
Add-BitLockerKeyProtector <drive letter or CSV mount point> - ADAccountOrGroupProtector – ADAccountOrGroup $cno

NEW QUESTION 131
HOTSPOT
Your network contains an Active Directory domain named contoso.com.
You need to create a certificate template for the BitLocker Drive Encryption (BitLocker) Network Unlock feature.
Which Cryptography setting of the certificate template should you modify? To answer, select the appropriate setting in the answer area.
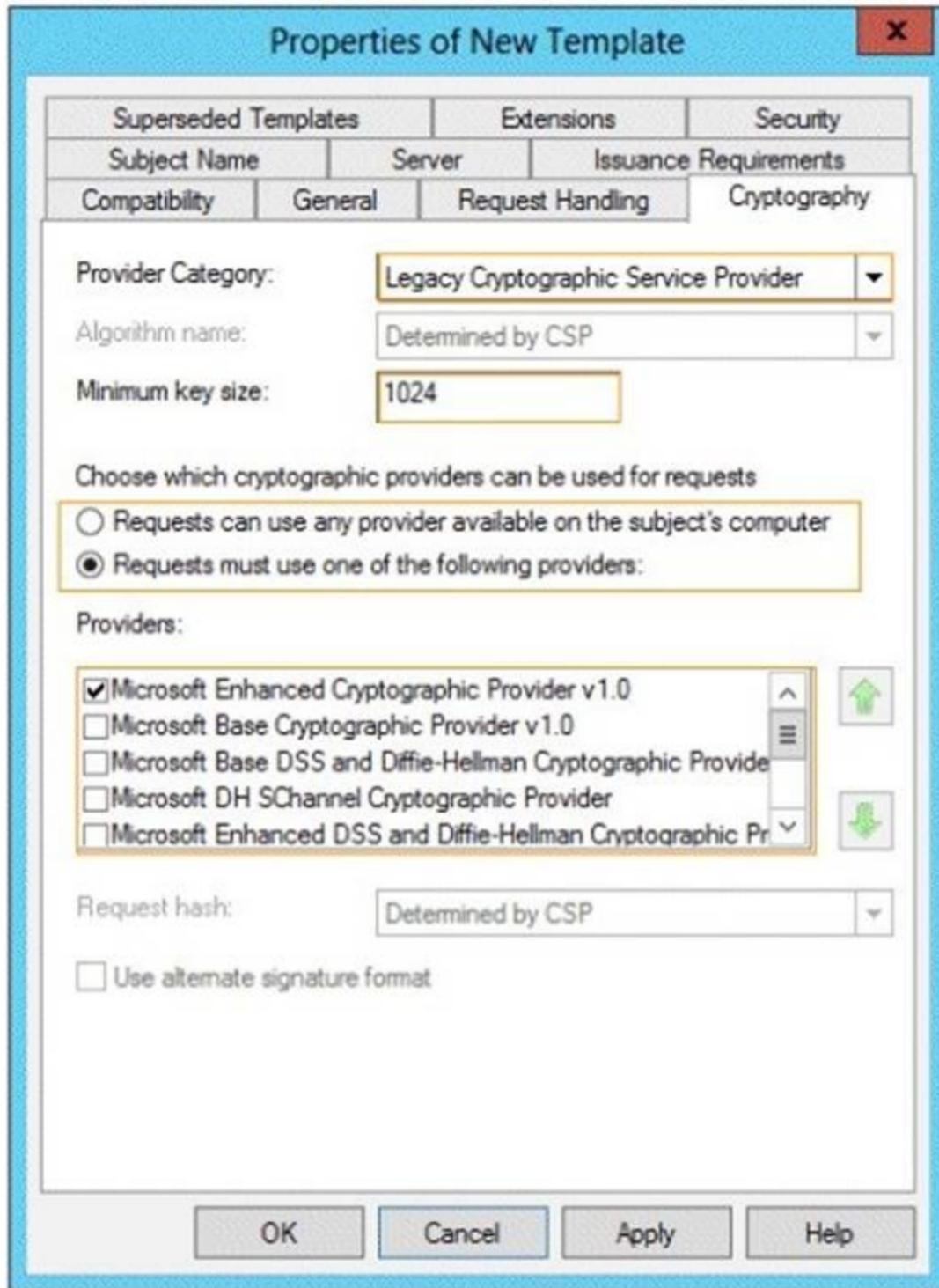
Answer:

Explanation: References:
http: //technet.microsoft.com/en-us/library/jj574173.aspx

NEW QUESTION 135
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.
You mount an Active Directory snapshot on DC1.
You need to expose the snapshot as an LDAP server. Which tool should you use?

A. Ldp
B. ADSI Edit
C. Dsamain
D. Ntdsutil

Answer: C

Explanation: dsamain /dbpath E:\$SNAP_200704181137_VOLUMED$\WINDOWS\NTDS\ntds. dit
/ldapport51389

Reference: http: //technet. microsoft. com/en-us/library/cc753609(v=ws. 10). aspx

NEW QUESTION 140
Your company has a main office and a branch office. The main office is located in Seattle. The branch office is located in Montreal. Each office is configured as an Active Directory site.
The network contains an Active Directory domain named adatum.com. The Seattle office contains a file server named Server1. The Montreal office contains a file server named Server2.
The servers run Windows Server 2012 R2 and have the File and Storage Services server role, the DFS Namespaces role service, and the DFS Replication role service installed.
Server1 and Server2 each have a share named Share1 that is replicated by using DFS Replication.
You need to ensure that users connect to the replicated folder in their respective office when they connect to \\contoso.com\Share1.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

A. Create a replication connection.
B. Create a namespace.
C. Share and publish the replicated folder.
D. Create a new topology.
E. Modify the Referrals settings.

Answer: BCE

Explanation: To share a replicated folder and publish it to a DFS namespace Click Start, point to Administrative Tools, and then click DFS Management. In the console tree, under the Replication node, click the replication group that contains the replicated folder you want to
share. In the details pane, on the Replicated Folders tab, right-click the replicated folder that you want to share, and then click Share and Publish in Namespace. In the Share and Publish Replicated Folder Wizard, click Share and publish the replicated folder in a namespace, and then follow the steps in the wizard.
Note that: If you do not have an existing namespace, you can create one in the Namespace Path page in the Share and Publish Replicated Folder Wizard. To create the namespace, in the Namespace Path page, click Browse, and then click New Namespace.
To create a namespace
Click Start, point to Administrative Tools, and then click DFS Management.
In the console tree, right-click the Namespaces node, and then click New Namespace. Follow the instructions in the New Namespace Wizard.
To create a stand-alone namespace on a failover cluster, specify the name of a clustered file server instance on the Namespace Server page of the New Namespace Wizard.
Important
Do not attempt to create a domain-based namespace using the Windows Server 2008 mode unless the forest functional level is Windows Server 2003 or higher.
Doing so can result in a namespace for which you cannot delete DFS folders, yielding the following error message: "The folder cannot be deleted. Cannot

complete this function."
To share a replicated folder and publish it to a DFS namespace
1. Click Start, point to Administrative Tools, and then click DFS Management.
2. In the console tree, under the Replication node, click the replication group that contains the replicated folder you want to share.
3. In the details pane, on the Replicated Folders tab, right-click the replicated folder that you want to share, and then click Share and Publish in Namespace.
4. In the Share and Publish Replicated Folder Wizard, click Share and publish the replicated folder in a namespace, and then follow the steps in the wizard.
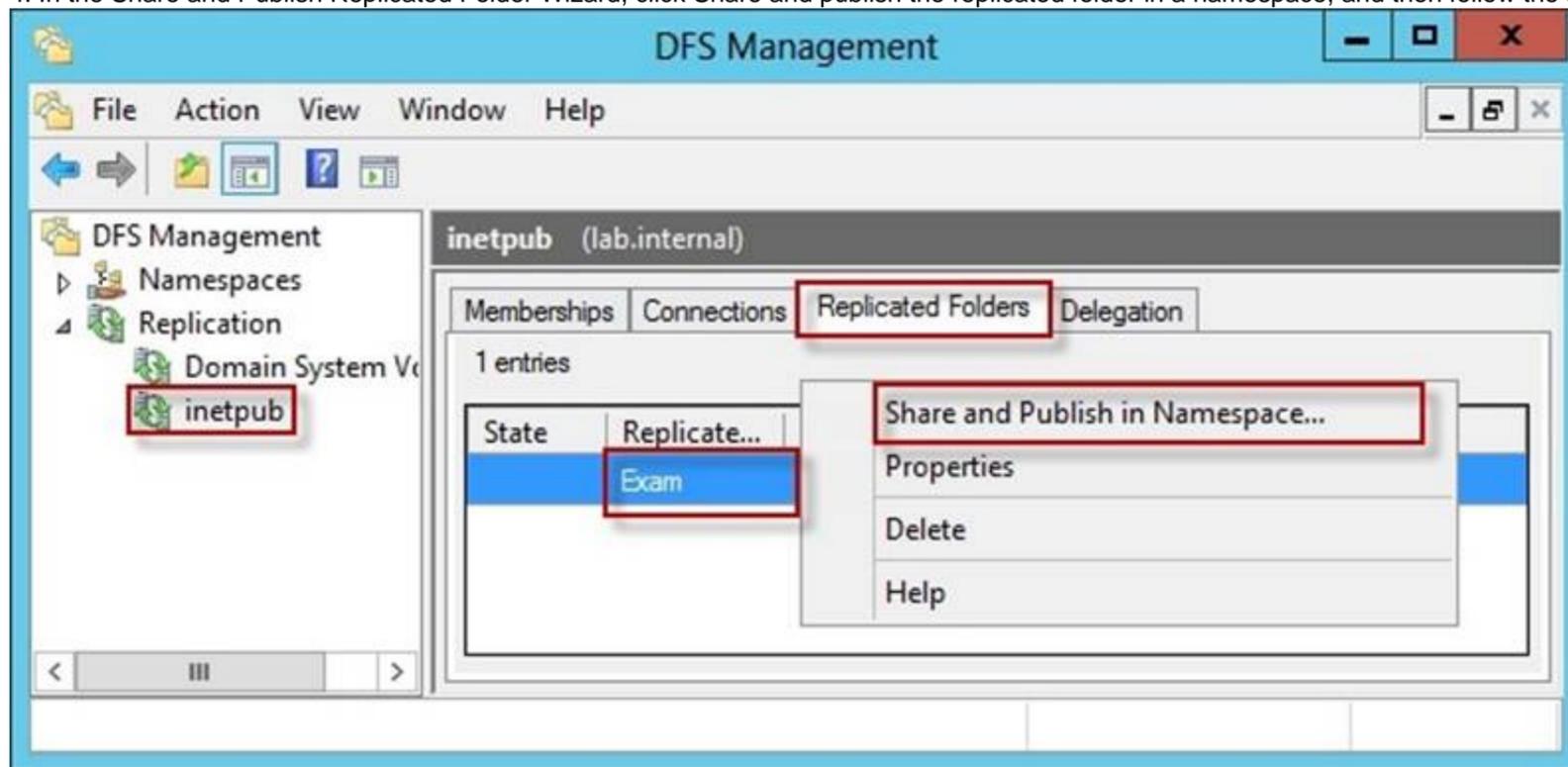
"You need to ensure that users connect to the replicated folder in their respective office when they connect to \\contoso.com\Share1."

Reference:
http: //technet. microsoft. com/en-us/library/cc731531. aspx
http: //technet. microsoft. com/en-us/library/cc772778%28v=ws. 10%29. aspx
http: //technet. microsoft. com/en-us/library/cc732414. aspx
http: //technet. microsoft. com/en-us/library/cc772379. aspx
http: //technet. microsoft. com/en-us/library/cc732863%28v=ws. 10%29. aspx
http: //technet. microsoft. com/en-us/library/cc725830. aspx
http: //technet. microsoft. com/en-us/library/cc771978. aspx
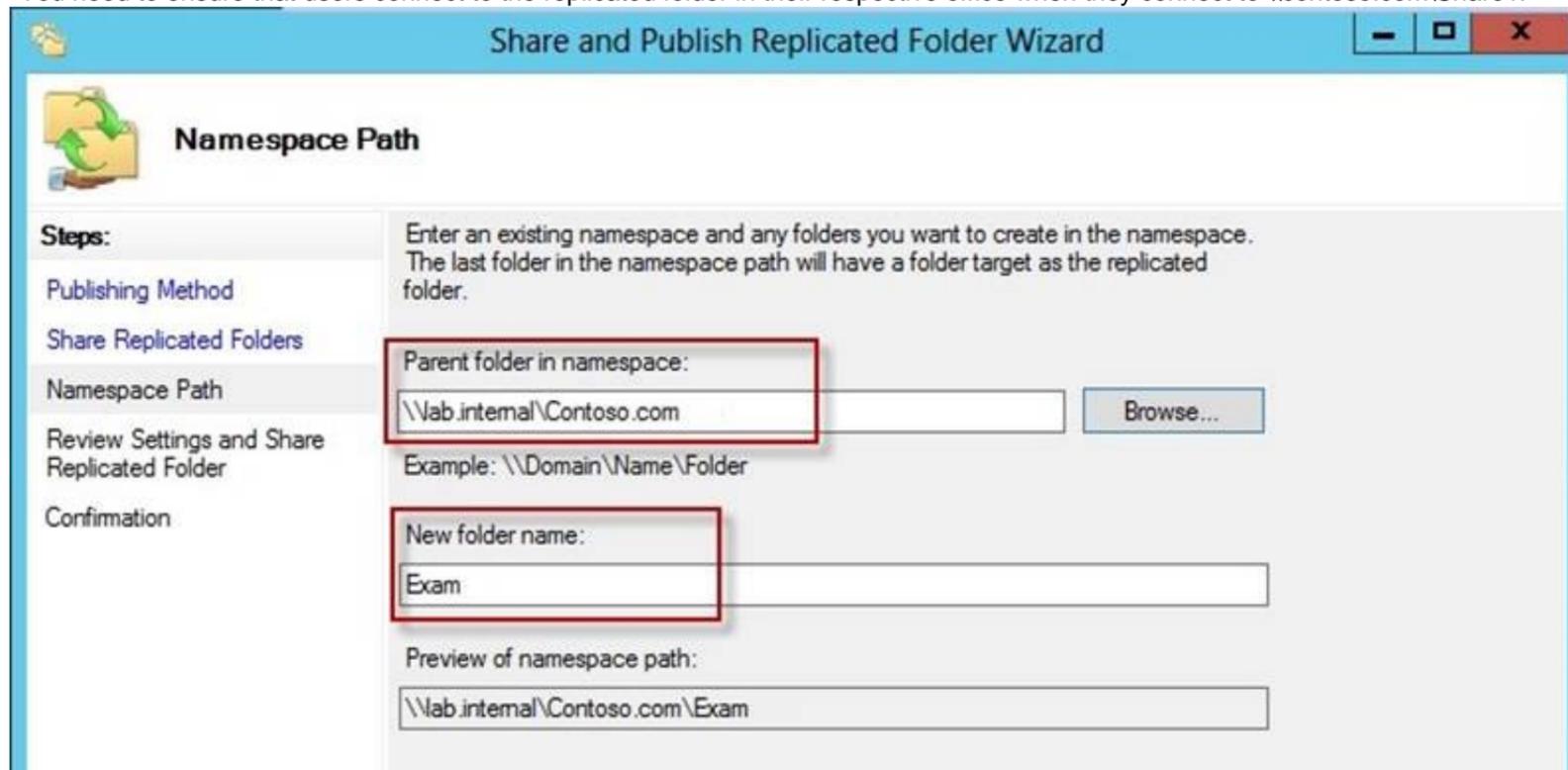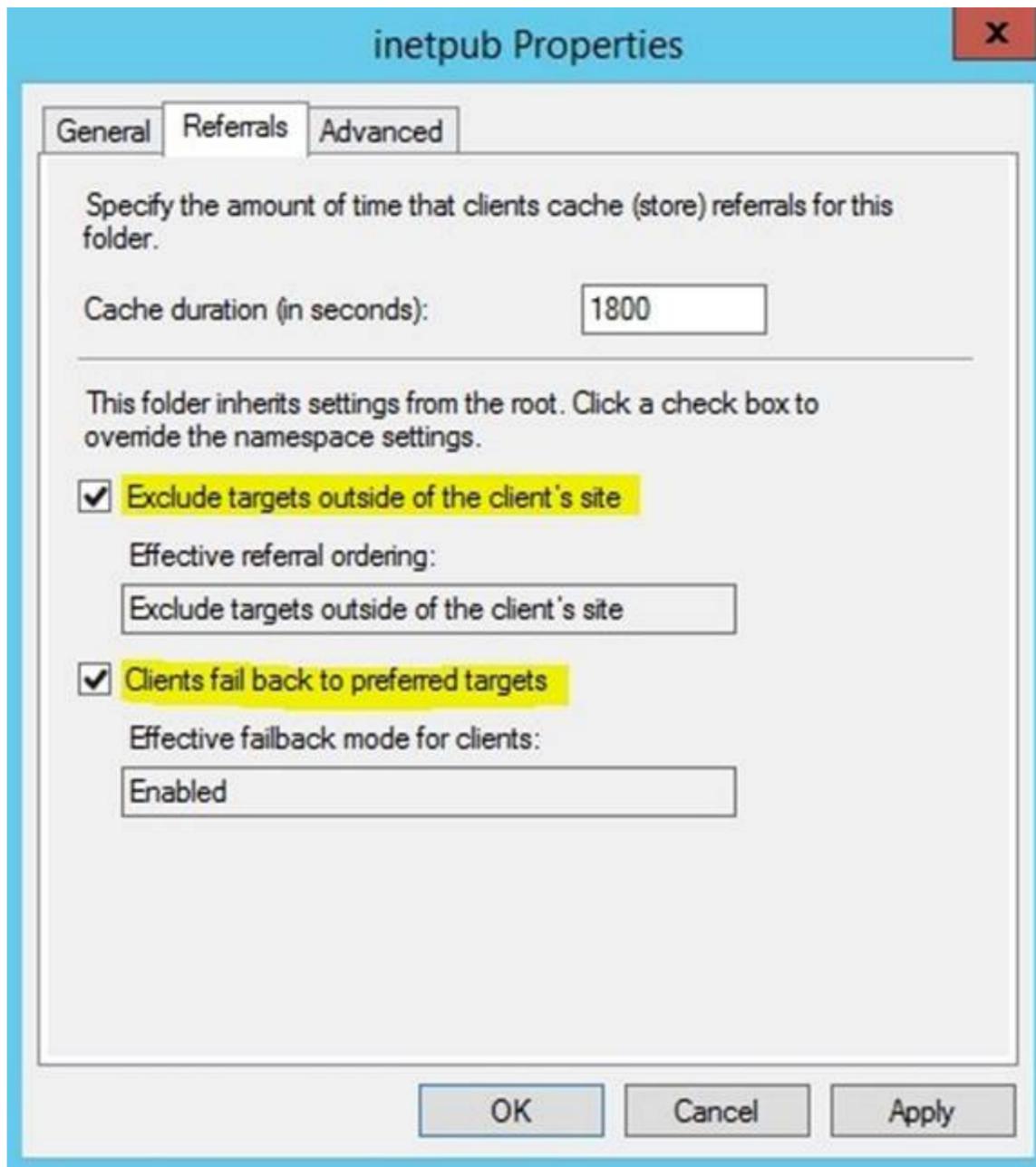
NEW QUESTION 142
Your network contains a domain controller named DC1 that runs Windows Server 2012 R2. You create a custom Data Collector Set (DCS) named DCS1.
You need to configure DCS1 to collect the following information:
? The amount of Active Directory data replicated between DC1 and the other domain controllers
? The current values of several registry settings
Which two should you configure in DCS1? (Each correct answer presents part of the solution. Choose two.)

A. Event trace data
B. A Performance Counter Alert
C. System configuration information
D. A performance counter

Answer: BC

Explanation: Automatically run a program when the amount of total free disk space on Server1 drops below 10 percent of capacity.
You can also configure alerts to start applications and performance logs Log the current values of several registry settings.
System configuration information allows you to record the state of, and changes to, registry keys.
Total free disk space

Registry settings

Performance Monitor

File   Action   View   Window   Help

Performance	Name	Type	Output
▲ Monitoring Tools	⚠ DataCollector01	Alert	
Performance Monitor			
▲ Data Collector Sets			
▲ User Defined			
New Data Collector Set			
Server Manager Perfor			
▷ System			
Event Trace Sessions			
Startup Event Trace Sessic			
▲ Reports			
▲ User Defined			
▷ New Data Collector Se			
▷ Server Manager Perfor			
▷ System			

Context menu:
- Start
- Stop
- Save Template...
- Data Manager...
- Latest Report
- New ▶ → Data Collector
- View ▶
- New Window from Here
- Delete
- Refresh
- Export List...
- Properties
- Help

Creates a new item in this container.

Create new Data Collector

What type of data collector would you like to create?

Name:

Registry Data Collector

○ Performance counter data collector
○ Event trace data collector
● Configuration data collector
○ Performance counter alert

Next   Finish   Cancel

Run a program on alert

Reference: http: //technet. microsoft. com/en-us/library/cc766404. aspx

NEW QUESTION 143
Your network contains an Active Directory domain named adatum.com. The domain contains 10 domain controllers that run Windows Server 2012 R2.
You plan to create a new Active Directory-integrated zone named contoso.com. You need to ensure that the new zone will be replicated to only four of the domain controllers.
What should you do first?

A. Create an application directory partition.
B. Create an Active Directory connection object.
C. Create an Active Directory site link.
D. Change the zone replication scope.

Answer: A

Explanation: Application directory partitions
An application directory partition is a directory partition that is replicated only to specific domain controllers. A domain controller that participates in the replication of a particular application directory partition hosts a replica of that partition. Only domain controllers running Windows Server 2003 can host a replica of an application directory partition.

NEW QUESTION 145
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains 30 user accounts that are used for network administration. The user accounts are members of a domain global group named Group1.
You identify the security requirements for the 30 user accounts as shown in the following table.

Security setting	Requirement
Minimum password length	20
Account is sensitive and cannot be delegated	Enabled
User cannot change password	Enabled
Password never expires	Enabled

You need to identify which settings must be implemented by using a Password Settings object (PSO) and which settings must be implemented by modifying the properties of the user accounts.

What should you identify? To answer, configure the appropriate settings in the dialog box in the answer area.

Answer Area

Security setting	Configured by using
Minimum password length	⌄
Account is sensitive and cannot be delegated	⌄
User cannot change password	⌄
Password never expires	⌄

Security setting	Configured by using
Minimum password length	⌄ PSO / User account properties
Account is sensitive and cannot be delegated	⌄ PSO / User account properties
User cannot change password	⌄ PSO / User account properties
Enforce password history	⌄ PSO / User account properties

Answer:

Explanation: Box 1: PSO
Box 2: User Account Properties Box 3: User Account Properties Box 4: PSO
Note:
* Password Setting Object (PSO) is another name for Fine Grain Password Policies.
* Here you can see all the settings that go into a PSO.
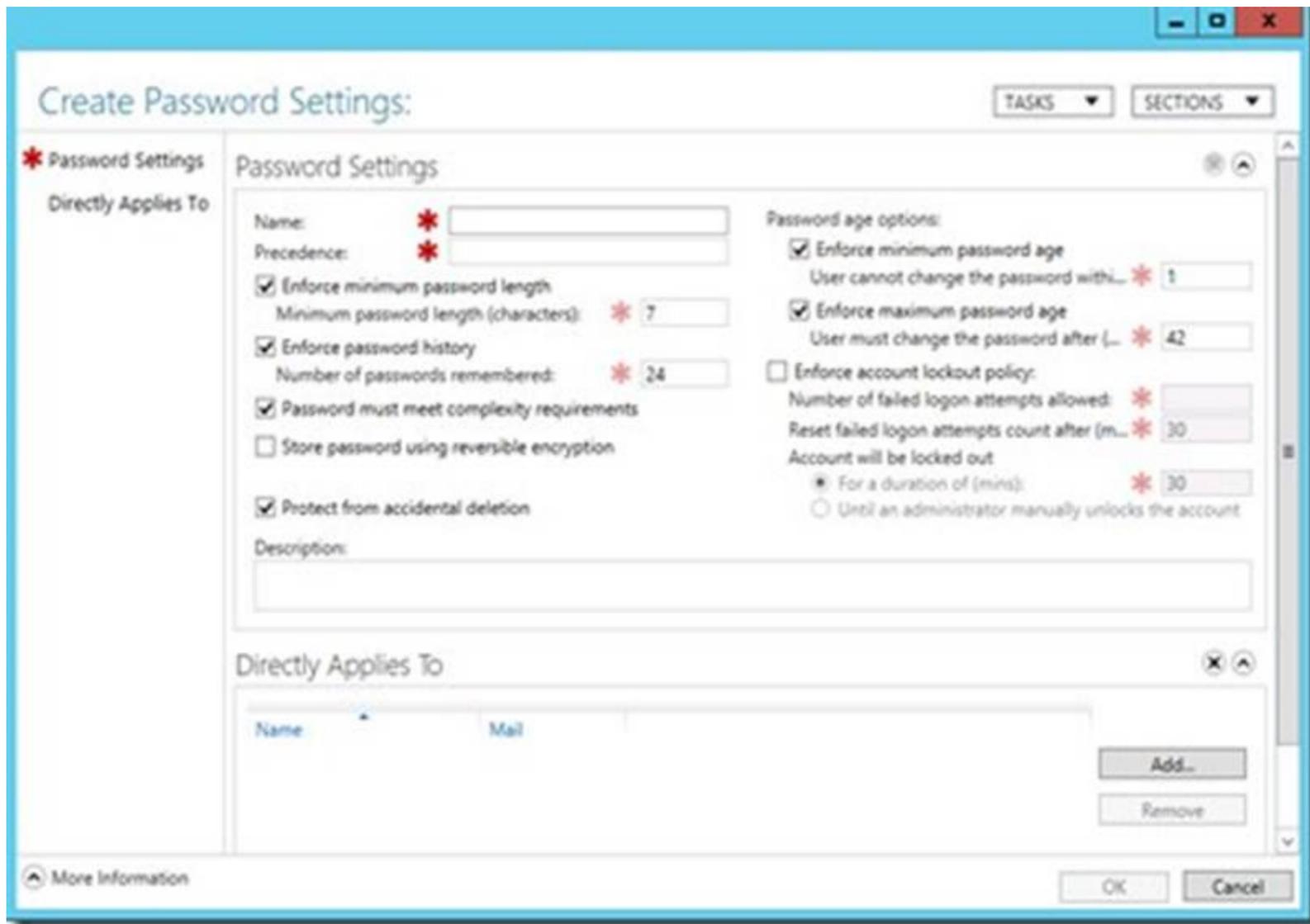
NEW QUESTION 147
Your network contains an Active Directory domain named contoso.com. The domain contains a RADIUS server named Server1 that runs Windows Server 2012 R2.
You add a VPN server named Server2 to the network. On Server1, you create several network policies.
You need to configure Server1 to accept authentication requests from Server2. Which tool should you use on Server1?

A. Server Manager
B. Routing and Remote Access
C. New-NpsRadiusClient
D. Connection Manager Administration Kit (CMAK)

Answer: C

Explanation: New-NpsRadiusClient -Name "NameOfMyClientGroup" -Address "10.1.0.0/16" - AuthAttributeRequired 0 -NapCompatible 0 -SharedSecret "SuperSharedSecretxyz" - VendorName "RADIUS Standard"

```
PS C:\Users\Administrator> New-NpsRadiusClient -Name "FromServer2" -Address "10.1.0.0/16" -AuthAttributeRequired 0 -NapC
ompatible 0 -SharedSecret "123" -VendorName "RADIUS Standard"


Name                  : FromServer2
Address               : 10.1.0.0/16
AuthAttributeRequired : False
NapCompatible         : False
SharedSecret          : 123
VendorName            : RADIUS Standard
Enabled               : True
```
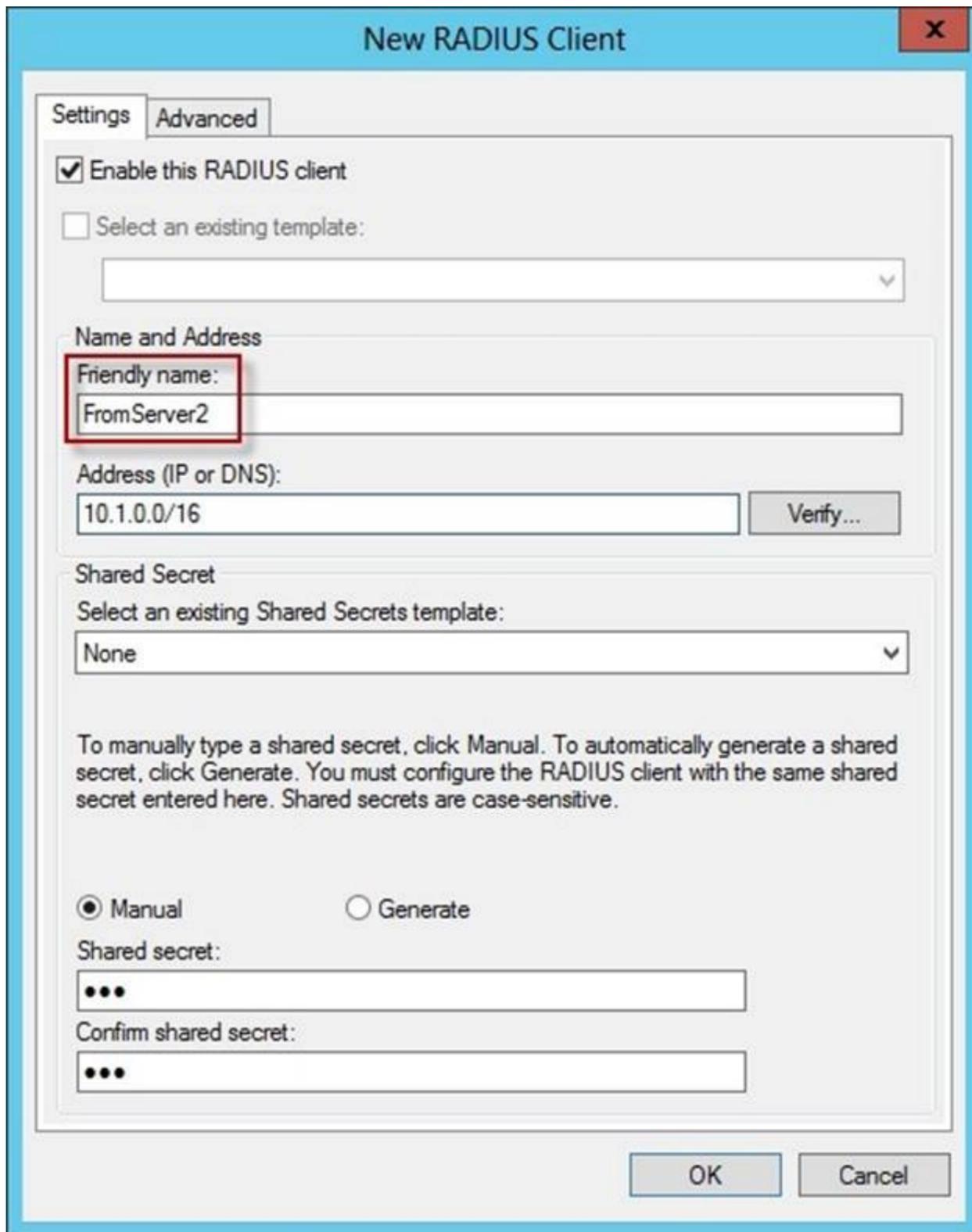
Reference:
http: //technet. microsoft. com/en-us/library/hh918425(v=wps. 620). aspx
http: //technet. microsoft. com/en-us/library/jj872740(v=wps. 620). aspx
http: //technet. microsoft. com/en-us/library/dd469790. aspx

NEW QUESTION 152
You have a server that runs Windows Server 2012 R2.
You have an offline image named Windows2012.vhd that contains an installation of Windows Server 2012 R2.
You plan to apply several updates to Windows2012.vhd. You need to mount Wmdows2012.vhd to D:\Mount. Which tool should you use?

A. Server Manager
B. Device Manager
C. Mountvol
D. Dism

Answer: D

Explanation: You can use the Deployment Image Servicing and Management (DISM) tool to mount a Windows image from a WIM or VHD file. Mounting an image maps the contents of the image to a directory so that you can service the image using DISM without booting into the image. You can also perform common file operations, such as copying, pasting, and editing on a mounted image.
To apply packages and updates to a Windows Embedded Standard 7 image, we recommend creating a configuration set and then using Deployment Imaging Servicing and Management (DISM) to install that configuration set. Although DISM can be used to install individual updates to an image, this method carries some additional risks and is not recommended.

NEW QUESTION 155
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 Network Policy Server server role installed.
You need to allow connections that use 802.1x. What should you create?

A. A network policy that uses Microsoft Protected EAP (PEAP) authentication

B. A network policy that uses EAP-MSCHAP v2 authentication
C. A connection request policy that uses EAP-MSCHAP v2 authentication
D. A connection request policy that uses MS-CHAP v2 authentication

Answer: C

Explanation: 802.1X uses EAP, EAP-TLS, EAP-MS-CHAP v2, and PEAP authentication methods:
? EAP (Extensible Authentication Protocol) uses an arbitrary authentication method, such as certificates, smart cards, or credentials.
? EAP-TLS (EAP-Transport Layer Security) is an EAP type that is used in certificate- based security environments, and it provides the strongest authentication and key determination method.
? EAP-MS-CHAP v2 (EAP-Microsoft Challenge Handshake Authentication Protocol version 2) is a mutual authentication method that supports password-based user or computer authentication.
? PEAP (Protected EAP) is an authentication method that uses TLS to enhance the security of other EAP authentication protocols.
Connection request policies are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User Service (RADIUS) servers perform the authentication and authorization of connection requests that the server running Network Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS servers are used for RADIUS accounting.
With connection request policies, you can use NPS as a RADIUS server or as a RADIUS proxy, based on factors such as the following:
? The time of day and day of the week
? The realm name in the connection request
? The type of connection being requested
? The IP address of the RADIUS client

NEW QUESTION 156
HOTSPOT
You have a server named Server5 that runs Windows Server 2012 R2. Servers has the Windows Deployment Services server role installed.
You need to ensure that when client computers connect to Server5 by using PXE, the computers use an unattended file.
What should you configure?
To answer, select the appropriate tab in the answer area.
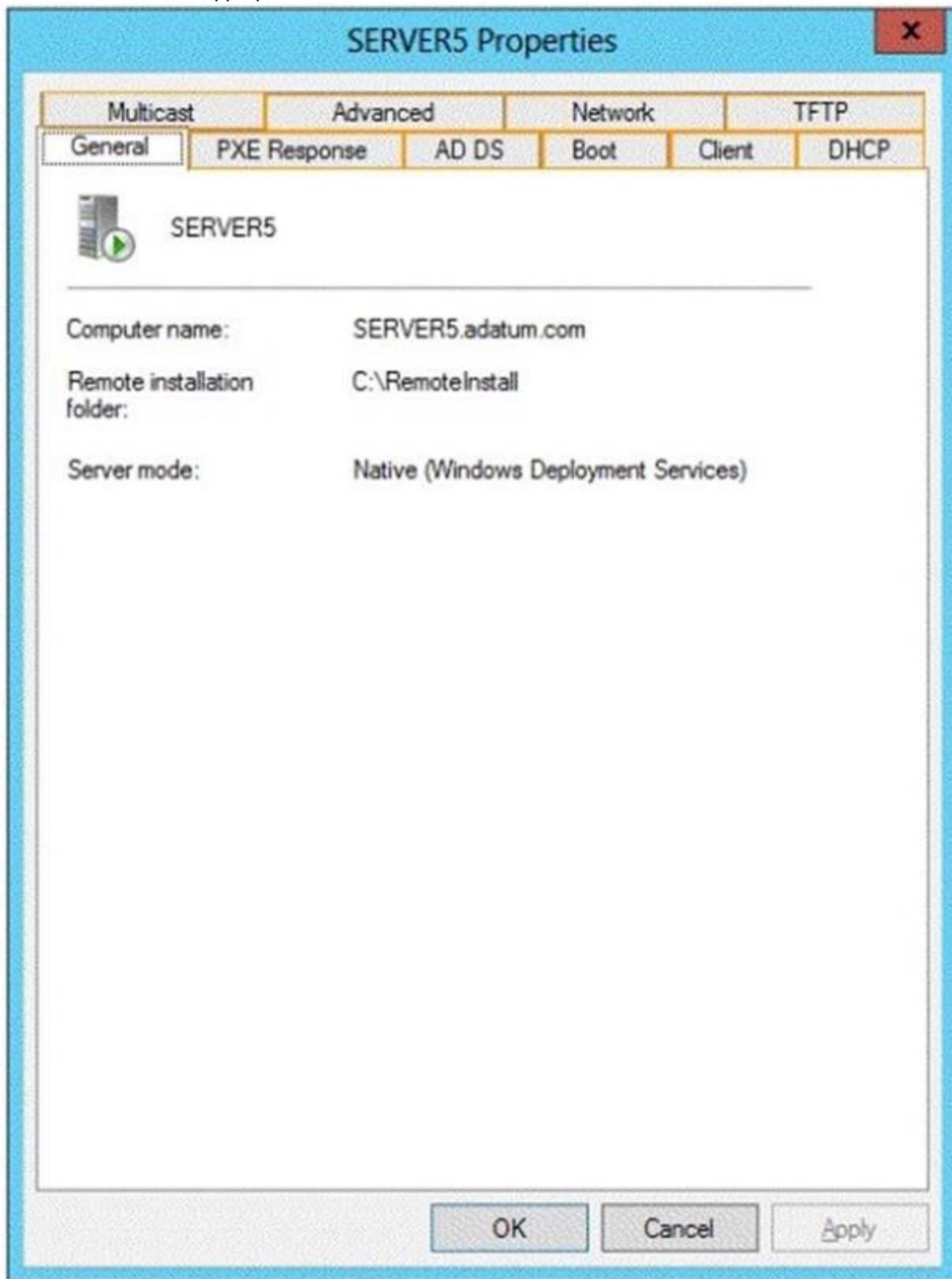
Answer:

Explanation:
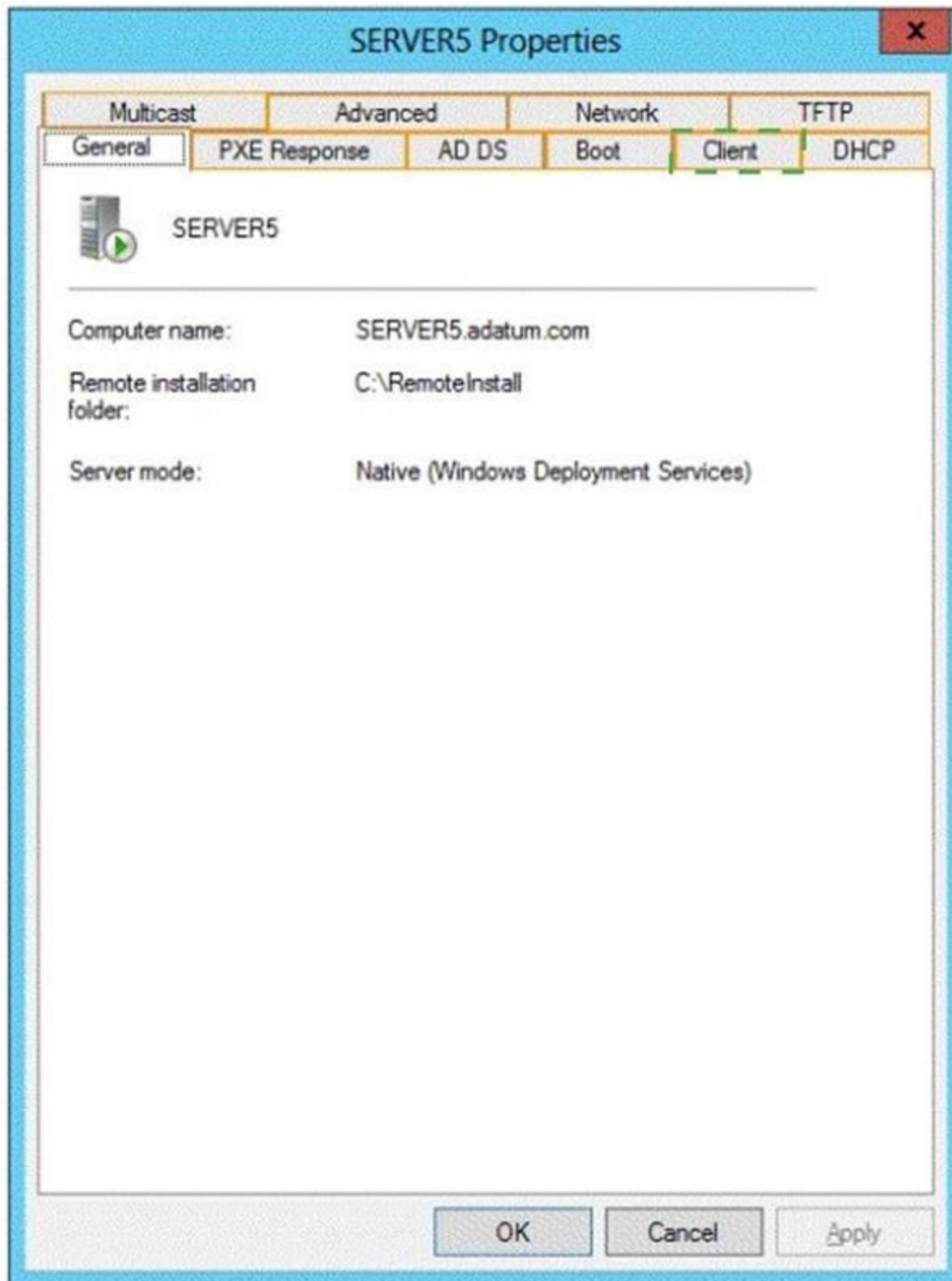
NEW QUESTION 161
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2.
You enable and configure Routing and Remote Access (RRAS) on Server1. You create a user account named User1.
You need to ensure that User1 can establish VPN connections to Server1. What should you do?

A. Modify the members of the Remote Management Users group.
B. Add a RADIUS client.
C. Modify the Dial-in setting of User1.
D. Create a connection request policy.

Answer: C

Explanation: Access permission is also granted or denied based on the dial-in properties of each user account.
http://technet.microsoft.com/en-us/library/cc772123.aspx

NEW QUESTION 166
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 Network Policy Server role service installed.
You plan to configure Server1 as a Network Access Protection (NAP) health policy server for VPN enforcement by using the Configure NAP wizard.
You need to ensure that you can configure the VPN enforcement method on Server1 successfully.
What should you install on Server1 before you run the Configure NAP wizard?

A. A system health validator (SHV)
B. The Host Credential Authorization Protocol (HCAP)
C. A computer certificate
D. The Remote Access server role

Answer: C

Explanation: Configure NAP enforcement for VPN
This checklist provides the steps required to deploy computers with Routing and Remote Access Service installed and configured as VPN servers with Network Policy Server (NPS) and Network Access Protection (NAP).

Task	Reference
If you want to perform authorization by group, create a user group in Active Directory® Domain Services (AD DS) that contains the users who are allowed to access the network through VPN servers.	Create a Group for a Network Policy
Determine the authentication method you want to use.	RADIUS Server for Dial-Up or VPN Connections and Certificate Requirements for PEAP and EAP
Autoenroll a server certificate to NPS and VPN servers or, if you are using PEAP-MS-CHAP v2 and you do not want to deploy your own CA, purchase a server certificate.	Deploy a CA and NPS Server Certificate and Obtaining and Installing a VeriSign WLAN Server Certificate for PEAP-MS-CHAP v2 Wireless Authentication (http://go.microsoft.com/fwlink/?LinkId=33675)
If you are using EAP-TLS or PEAP-TLS without smart cards, autoenroll user certificates, computer certificates, or both user and computer certificates, to domain member client computers.	Deploy Client Computer Certificates and Deploy User Certificates
In NPS, configure VPN servers as RADIUS clients and on the VPN server, configure the NPS server as the primary RADIUS server.	Add a New RADIUS Client; RADIUS Clients; and Routing and Remote Access Service documentation in Windows Server® 2008
If you are using the Windows Security Health Validator (WSHV) in your NAP deployment, enable Security Center on NAP-capable clients using Group Policy.	Enable Security Center in Group Policy
In NPS, if your NAP deployment requires it, configure the WSHV.	Windows Security Health Validator

If you are using non-Microsoft products that are compatible with NAP, deploy non-Microsoft system health agents (SHAs) on client computers and their corresponding system health validators (SHVs) on the NPS server.	System Health Validators and product documentation
If you want to provide client computers with automatic updates using autoremediation, deploy and configure Remediation Server Groups in NPS.	Configure Remediation Server Groups and Remediation Server Groups
On the NPS server, configure health policies, connection request policies, and network policies that enforce NAP for VPN connections.	Create NAP Policies with a Wizard
On client computers, manually configure a VPN connection to the VPN server or install a Connection Manager profile that you created with Connection Manager Administration Kit (CMAK).	Routing and Remote Access Service, Network and Sharing Center, and Connection Manager Administration Kit (CMAK) documentation in Windows Server 2008
On NAP-capable client computers, enable the Network Access Protection service and change the startup type to automatic.	Enable the Network Access Protection Service on Clients
On NAP-capable client computers, enable the Remote Access and EAP enforcement clients.	Enable and Disable NAP Enforcement Clients

NEW QUESTION 170
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Server Update Services server role installed.
You need to configure Windows Server Update Services (WSUS) to support Secure Sockets Layer (SSL).
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

A. From Internet Information Services (IIS) Manager, modify the connection strings of the WSUS website.
B. Install a server certificate.
C. Run the wsusutil.exe command.
D. Run the iisreset.exe command.
E. From Internet Information Services (IIS) Manager, modify the bindings of the WSUS website.

Answer: BCE

Explanation: Certificate needs to be installed to IIS, Bindings modifies and wsusutil run.
1. First we need to request a certificate for the WSUS web site, so open IIS, click the server name, then open Server Certificates.
On the Actions pane click Create Domain Certificate.
2. To add the signing certificate to the WSUS Web site in IIS 7.0
On the WSUS server, open Internet Information Services (IIS) Manager. Expand Sites, right-click the WSUS Web site, and then click Edit Bindings.
In the Site Binding dialog box, select the https binding, and click Edit to open the Edit Site Binding dialog box.
Select the appropriate Web server certificate in the SSL certificate box, and then click OK. Click Close to exit the Site Bindings dialog box, and then click OK to close Internet Information Services (IIS) Manager.
3. WSUSUtil.exe configuressl<FQDN of the software update point site system> (the name in your certificate)
WSUSUtil.exe configuressl<Intranet FQDN of the software update point site system>.
4. The next step is to point your clients to the correct url, by modifying the existing GPO or creating a new one. Open the policy Specify intranet Microsoft update service location and type the new url in the form https: //YourWSUSserver.
The gpupdate /force command will just download all the GPO's and re-apply them to the client, it won't force the client to check for updates. For that you need to use wuauclt
/resetauthorization /detectnow followed by wuauclt /reportnow
References:
http: //technet. microsoft. com/en-us/library/bb680861. aspx http: //technet. microsoft. com/en-us/library/bb633246. aspx http: //www. vkernel. ro/blog/configure-wsus-to-use-ssl

NEW QUESTION 172
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.
Each time a user receives an access-denied message after attempting to access a folder on Server1, an email notification is sent to a distribution list named DL1.
You create a folder named Folder1 on Server1, and then you configure custom NTFS permissions for Folder 1.
You need to ensure that when a user receives an access-denied message while attempting to access Folder1, an email notification is sent to a distribution list named DL2. The solution must not prevent DL1 from receiving notifications about other access-denied messages.
What should you do?

A. From File Explorer, modify the Classification tab of Folder1.
B. From the File Server Resource Manager console, modify the Email Notifications settings.

C. From the File Server Resource Manager console, set a folder management property.
D. From File Explorer, modify the Customize tab of Folder1.

Answer: C

Explanation: When using the email model each of the file shares, you can determine whether access requests to each file share will be received by the administrator, a distribution list that represents the file share owners, or both.
You can use the File Server Resource Manager console to configure the owner distribution list by editing the management properties of the classification properties.
Reference: http://technet.microsoft.com/en-us/library/jj574182.aspx#BKMK_12

NEW QUESTION 176
HOTSPOT
Your network contains a DNS server named Server1 that runs Windows Server 2012 R2. Server1 has a zone named contoso.com. The network contains a server named Server2 that runs Windows Server 2008 R2. Server1 and Server2 are members of an Active Directory domain named contoso.com.
You change the IP address of Server2.
Several hours later, some users report that they cannot connect to Server2.
On the affected users' client computers, you flush the DNS client resolver cache, and the users successfully connect to Server2.
You need to reduce the amount of time that the client computers cache DNS records from contoso.com.
Which value should you modify in the Start of Authority (SOA) record? To answer, select the appropriate setting in the answer area.

Answer:

Explanation: The Default TTL, is just that a default for newly created records. Once the records are created their TTL is independent of the Default TTL on the SOA. Microsoft DNS implementation copies the Default TTL setting to all newly created records their by giving them all independent TTL settings.
SOA Minimum Field: The SOA minimum field has been overloaded in the past to have three different meanings, the minimum TTL value of all RRs in a zone, the default TTL of RRs which did not contain a TTL value and the TTL of negative responses.
Despite being the original defined meaning, the first of these, the minimum TTL value of all RRs in a zone, has never in practice been used and is hereby deprecated. The second, the default TTL of RRs which contain no explicit TTL in the master zone file, is relevant only at
the primary server. After a zone transfer all RRs have explicit TTLs and it is impossible to determine whether the TTL for a record was explicitly set or derived from the default after a zone transfer. Where a server does not require RRs to include the TTL value explicitly, it should provide a mechanism, not being the value of the MINIMUM field of the SOA record, from which the missing TTL values are obtained. How this is done is implementation dependent.

TTLs also occur in the Domain Name System (DNS), where they are set by an authoritative name server for a particular resource record. When a caching (recursive) nameserver queries the authoritative nameserver for a resource record, it will cache that record for the time (in seconds) specified by the TTL. If a stub resolver queries the caching nameserver for the same record before the TTL has expired, the caching server will simply reply with the already cached resource record rather than retrieve it from the authoritative nameserver again.

Shorter TTLs can cause heavier loads on an authoritative nameserver, but can be useful when changing the address of critical services like Web servers or MX records, and therefore are often lowered by the DNS administrator prior to a service being moved, in order to minimize disruptions.

contoso.com Properties

WINS | Zone Transfers | Security
General | Start of Authority (SOA) | Name Servers

Serial number: 234 [Increment]

Primary server: server1.contoso.com. [Browse...]

Responsible person: hostmaster.contoso.com [Browse...]

Refresh interval: 1 days
Retry interval: 1 days
Expires after: 1 days
Minimum (default) TTL: 20 minutes

TTL for this record: 1 :0 :0 :0 (DDDDD:HH.MM.SS)

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

```
C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

    dc1
    ----------------------------------------
    Record Name . . . . . : dc1.home.local
    Record Type . . . . . : 1
    Time To Live  . . . . : 1196
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.1.10
```

```
> set type=soa
> dc1
Server:  dc1.home.local
Address:  192.168.1.10

home.local
        primary name server = dc1.home.local
        responsible mail addr = hostmaster.home.local
        serial  = 281
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 300 (5 mins)
        default TTL = 1200 (20 mins)
dc1.home.local  internet address = 192.168.1.10
```

NEW QUESTION 181
HOTSPOT
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012 R2 and are configured as DNS servers. All DNS zones are Active Directory-integrated. Active Directory Recycle Bin is enabled.
You need to modify the amount of time deleted objects are retained in the Active Directory Recycle Bin.
Which naming context should you use? To answer, select the appropriate naming context in the answer area.
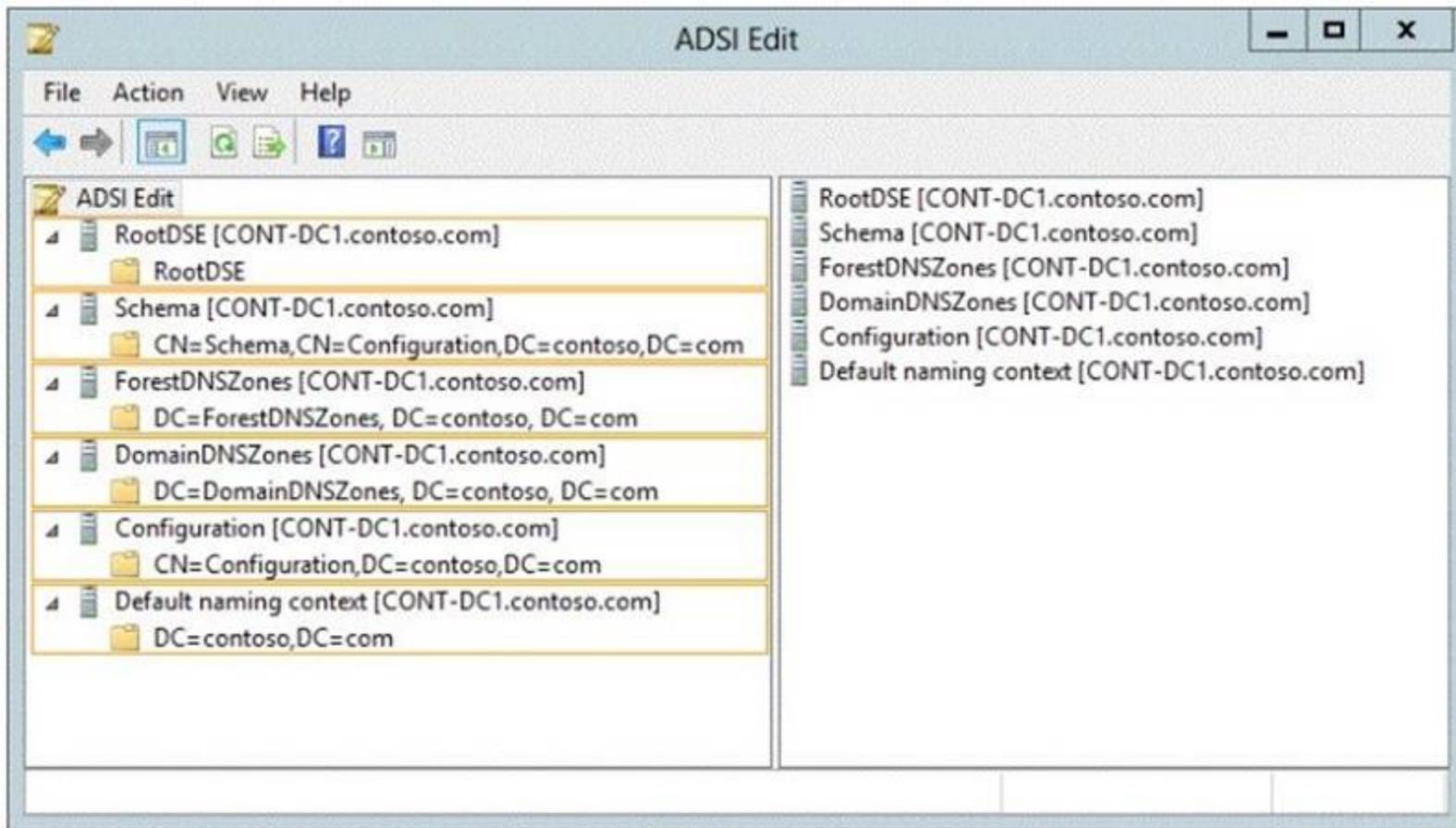
Answer:

Explanation: Starting in Windows Server 2008 R2, Active Directory now implements a true recycle bin. No longer will you need an authoritative restore to recover deleted users, groups, OU's, or other objects. Instead, it is now possible to use PowerShell commands to bring back objects with all their attributes, backlinks, group memberships, and metadata.

The amount of time that an object can be recovered is controlled by the Deleted Object Lifetime (DOL). This time range can be set on the msDS-deletedObjectLifetime attribute. By default, it will be the same number of days as the Tombstone Lifetime (TSL). The TSL set for a new forest since Windows Server 2003 SP1 has been 180 days*, and since by default DOL = TSL, the default number of days that an object can be restored is therefore 180 days. If tombstoneLifetime is NOT SET or NULL, the tombstone lifetime is that of the Windows default: 60 days. This is all configurable by the administrator.

Set-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=contoso,DC=com" -Partition "CN=Configuration,DC=contoso,DC=com" -Replace: @("msDS-DeletedObjectLifetime" = 365)

msDS-deletedObjectLifetime New to Windows Server 2008 R2

Is set on the "CN=Directory Service,CN=Windows NT, CN=Services, CN=Configuration, DC=COMPANY,DC=COM" container

Describes how long a deleted object will be restorable To modify the deleted object lifetime by using Ldp.exe

To open Ldp.exe, click Start, click Run, and then type ldp.exe.

To connect and bind to the server hosting the forest root domain of your Active Directory environment, under Connections, click Connect, and then click Bind.

In the console tree, right-click the CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration container, and then click Modify.

In the Modify dialog box, in Edit Entry Attribute, type msDS-DeletedObjectLifeTime.

In the Modify dialog box, in Values, type the number of days that you want to set for the tombstone lifetime value. (The minimum is 3 days.)

In the Modify dialog box, under Operation click Replace, click Enter, and then click Run.

References:

http://technet. microsoft. com/en-us/library/dd392260%28v=ws. 10%29. aspx

http://blogs. technet. com/b/askds/archive/2009/08/27/the-ad-recycle-bin-understanding- implementing-best-practices-and-troubleshooting. aspx

NEW QUESTION 182

Your network is configured as shown in the exhibit. (Click the Exhibit button.)
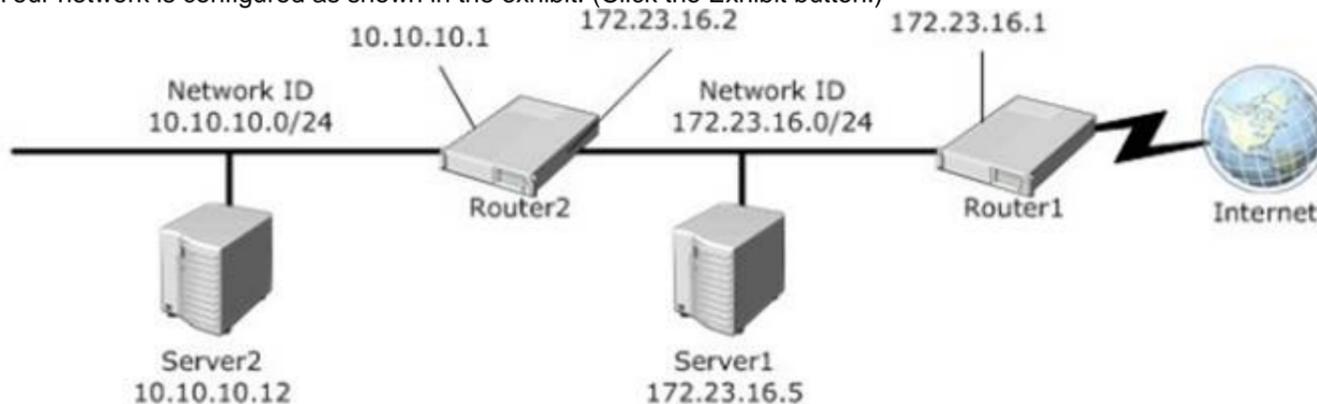
Server1 regularly accesses Server2.

You discover that all of the connections from Server1 to Server2 are routed through Router1.

You need to optimize the connection path from Server1 to Server2. Which route command should you run on Server1?

A. Route add -p 10.10.10.0 MASK 255.255.255.0 172.23.16.2 METRIC 100
B. Route add -p 10.10.10.0 MASK 255.255.255.0 10.10.10.1 METRIC 50
C. Route add -p 10.10.10.12 MASK 255.255.255.0 10.10.10.1 METRIC 100
D. Route add -p 10.10.10.12 MASK 255.255.255.0 10.10.10.0 METRIC 50

Answer: A

Explanation: Destination - specifies either an IP address or host name for the network or host. subnetmask - specifies a subnet mask to be associated with this route entry. If subnetmask
is not specified, 255.255.255.255 is used.
gateway - specifies either an IP address or host name for the gateway or router to use when forwarding.
costmetric - assigns an integer cost metric (ranging from 1 through 9,999) to be used in calculating the fastest, most reliable, and/or least expensive routes. If costmetric is not specified, 1 is used.
interface - specifies the interface to be used for the route that uses the interface number. If an interface is not specified, the interface to be used for the route is determined from the gateway IP address.
References:
http: //support. microsoft. com/kb/299540/en-us
http: //technet. microsoft. com/en-us/library/cc757323%28v=ws. 10%29. aspx

NEW QUESTION 183
Your network contains an Active Directory domain named contoso.com. Network Access Protection (NAP) is deployed to the domain.
You need to create NAP event trace log files on a client computer. What should you run?

A. logman
B. Register-ObjectEvent
C. tracert
D. Register-EngineEvent

Answer: A

Explanation: You can enable NAP client tracing by using the command line. On computers running Windows Vista®, you can enable tracing by using the NAP Client Configuration console. NAP client tracing files are written in Event Trace Log (ETL) format. These are binary files representing trace data that must be decoded by Microsoft support personnel. Use the –o option to specify the directory to which they are written. In the following example, files are written to %systemroot%\tracing\nap. For more information, see Logman (http: //go. microsoft.com/fwlink/?LinkId=143549).
To create NAP event trace log files on a client computer
? Open a command line as an administrator.
? Type
logman start QAgentRt -p {b0278a28-76f1-4e15-b1df-14b209a12613} 0xFFFFFFFF 9 -o
%systemroot%\tracing\nap\QAgentRt. etl –ets.
Note: To troubleshoot problems with WSHA, use the following GUID: 789e8f15-0cbf-4402- b0ed-0e22f90fdc8d.
? Reproduce the scenario that you are troubleshooting.
? Type logman stop QAgentRt -ets.
? Close the command prompt window.
References:
http: //technet. microsoft. com/en-us/library/dd348461%28v=ws. 10%29. aspx

NEW QUESTION 187
You have a server named Server1 that runs Windows Server 2012 R2. You create a custom Data Collector Set (DCS) named DCS1.
You need to configure Server1 to start DCS1 automatically when the network usage exceeds 70 percent.
Which type of data collector should you create?

A. A performance counter alert
B. A configuration data collector
C. A performance counter data collector
D. An event trace data collector

Answer: A

Explanation: Performance alerts notify you when a specified performance counter exceeds your configured threshold by logging an event to the event log. But rather than notifying you immediately when the counter exceeds the threshold, you can configure a time period over which the counter needs to exceed the threshold, to avoid unnecessary alerts.
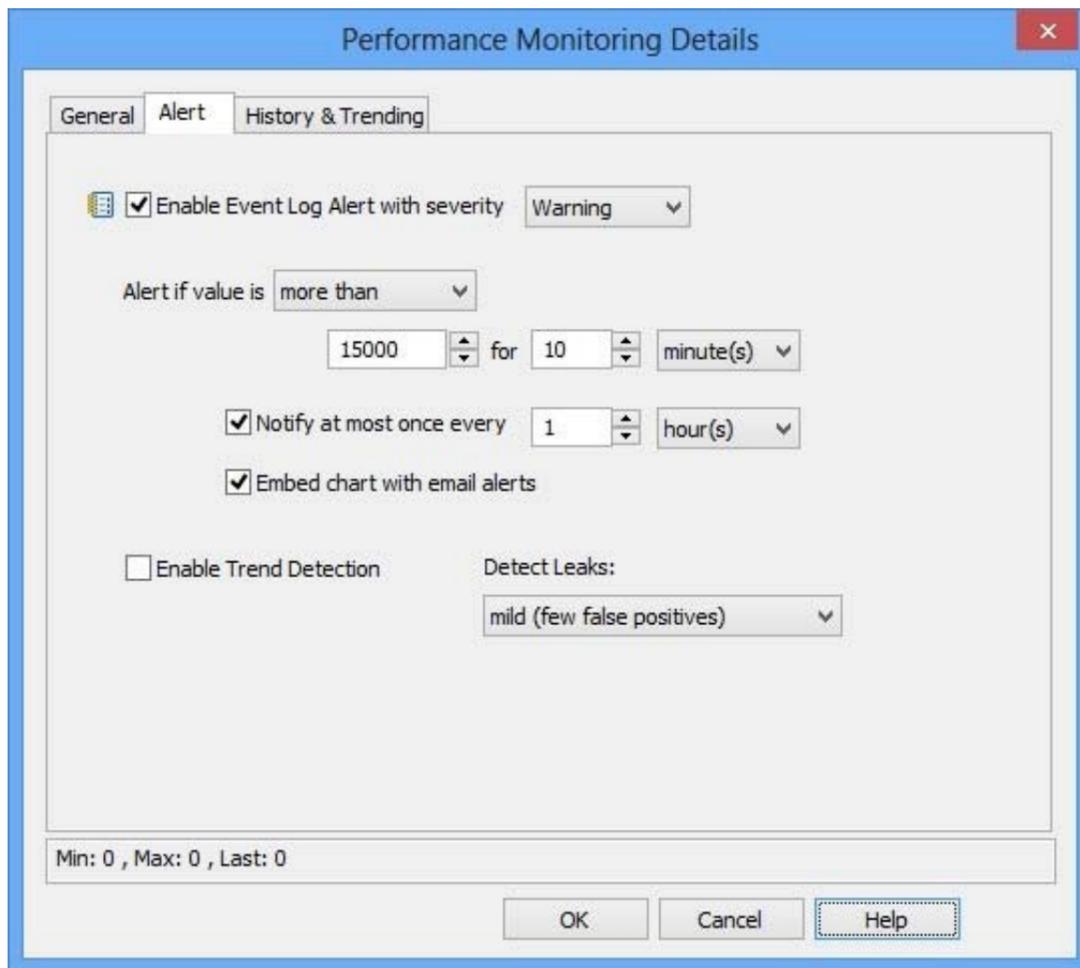
NEW QUESTION 192
HOTSPOT
You have a server named Server1 that has the Network Policy and Access Services server role installed.
You plan to configure Network Policy Server (NPS) on Server1 to use certificate-based authentication for VPN connections.
You obtain a certificate for NPS.
You need to ensure that NPS can perform certificate-based authentication. To which store should you import the certificate?
To answer, select the appropriate store in the answer area.
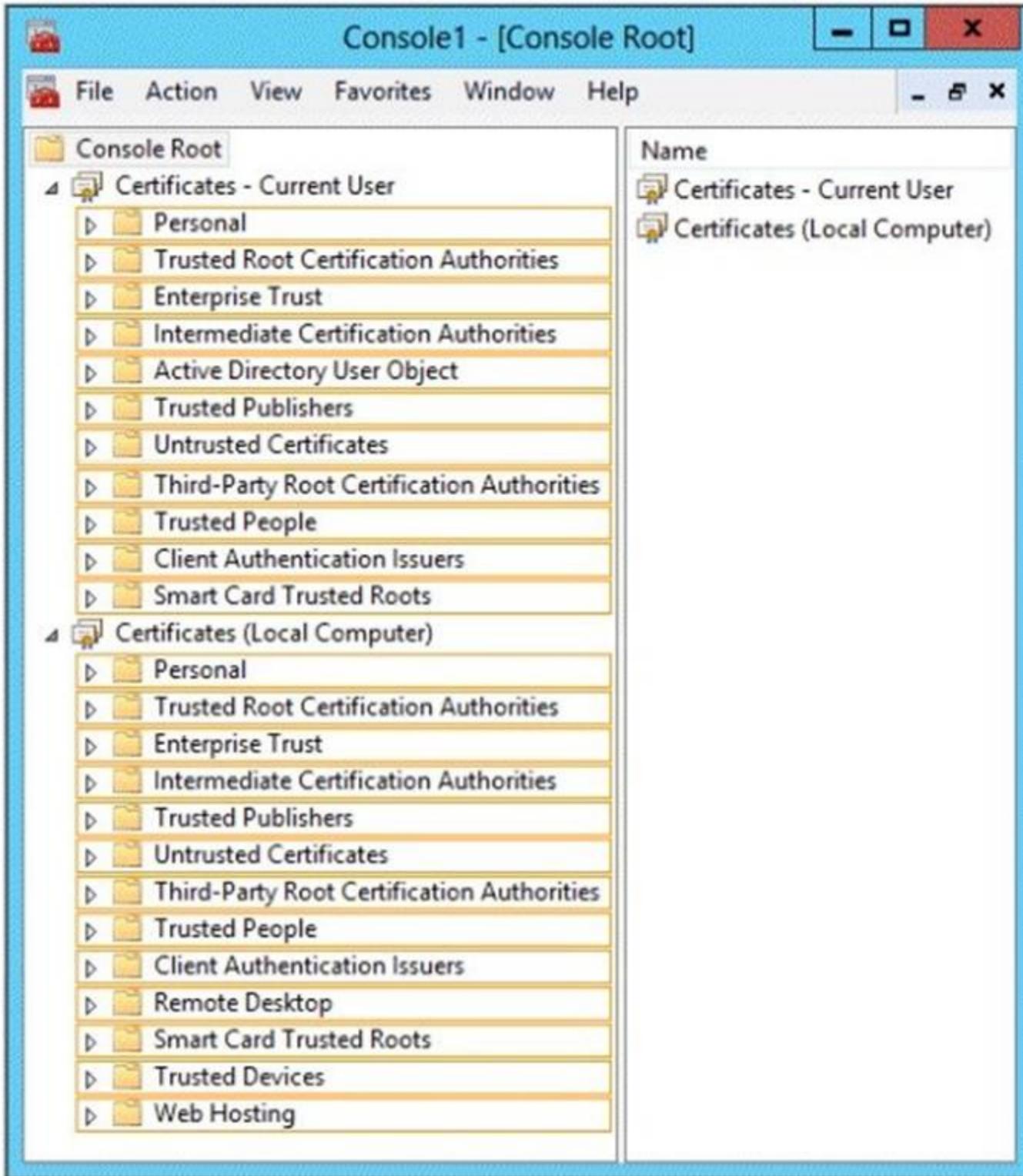
Answer:

Explanation: When organizations deploy their own public key infrastructure (PKI) and install a private trusted root CA, their CA automatically sends its certificate to all domain member computers in the organization. The domain member client and server computers store the CA certificate in the Trusted Root Certification Authorities certificate store. After this occurs, the domain member computers trust certificates that are issued by the organization trusted root CA.

For example, if you install AD CS, the CA sends its certificate to the domain member computers in your organization and they store the CA certificate in the Trusted Root Certification Authorities certificate store on the local computer. If you also configure and autoenroll a server certificate for your NPS servers and then deploy PEAP-MS-CHAP v2 for wireless connections, all domain member wireless client computers can successfully authenticate your NPS servers using the NPS server certificate because they trust the CA that issued the NPS server certificate.

On computers that are running the Windows operating system, certificates that are installed on the computer are kept in a storage area called the certificate store. The certificate store is accessible using the Certificates Microsoft Management Console (MMC) snap-in.

This store contains multiple folders, where certificates of different types are stored. For example, the certificate store contains a Trusted Root Certification Authorities folder where the certificates from all trusted root CAs are kept.

When your organization deploys a PKI and installs a private trusted root CA using AD CS, the CA automatically sends its certificate to all domain member computers in the organization. The domain member client and server computers store the CA certificate in the Trusted Root Certification Authorities folder in the Current User and the Local Computer certificate stores. After this occurs, the domain member computers trust certificates that are issued by the trusted root CA.

Similarly, when you autoenroll computer certificates to domain member client computers, the certificate is kept in the Personal certificate store for the Local Computer. When you autoenroll certificates to users, the user certificate is kept in the Personal certificate store for the Current User.

References:
http: //technet. microsoft. com/en-us/library/cc730811. aspx http: //technet. microsoft. com/en-us/library/cc730811. aspx
http: //technet. microsoft. com/en-us/library/cc772401%28v=ws. 10%29. aspx http: //technet. microsoft. com/en-us/library/ee407543%28v=ws. 10%29. aspx

NEW QUESTION 194
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

70-411 Practice Exam Features:

* 70-411 Questions and Answers Updated Frequently

* 70-411 Practice Questions Verified by Expert Senior Certified Staff

* 70-411 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 70-411 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 70-411 Practice Test Here