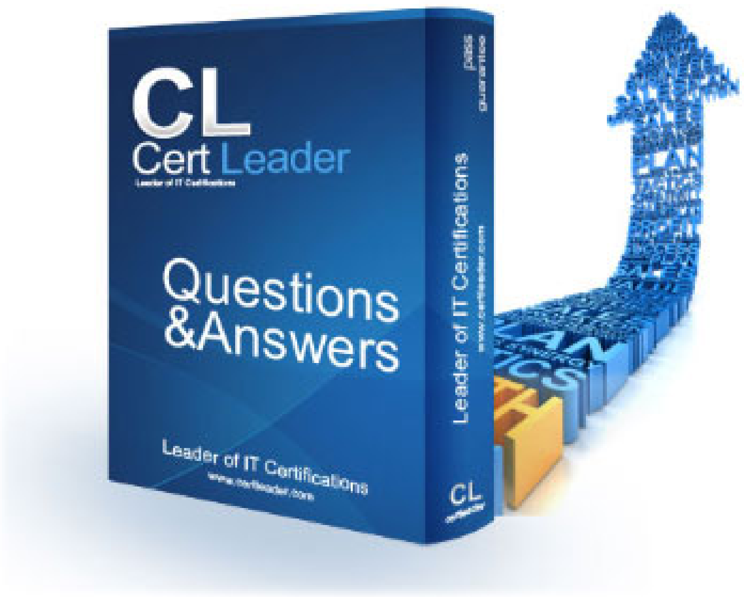
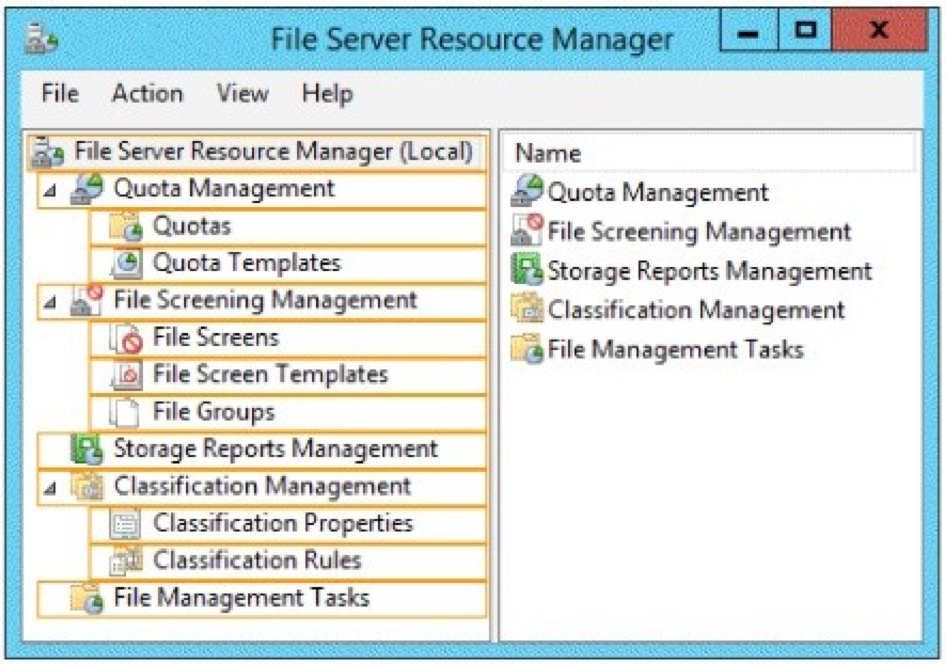
70-411 Dumps

Administering Windows Server 2012

https://www.certleader.com/70-411-dumps.html



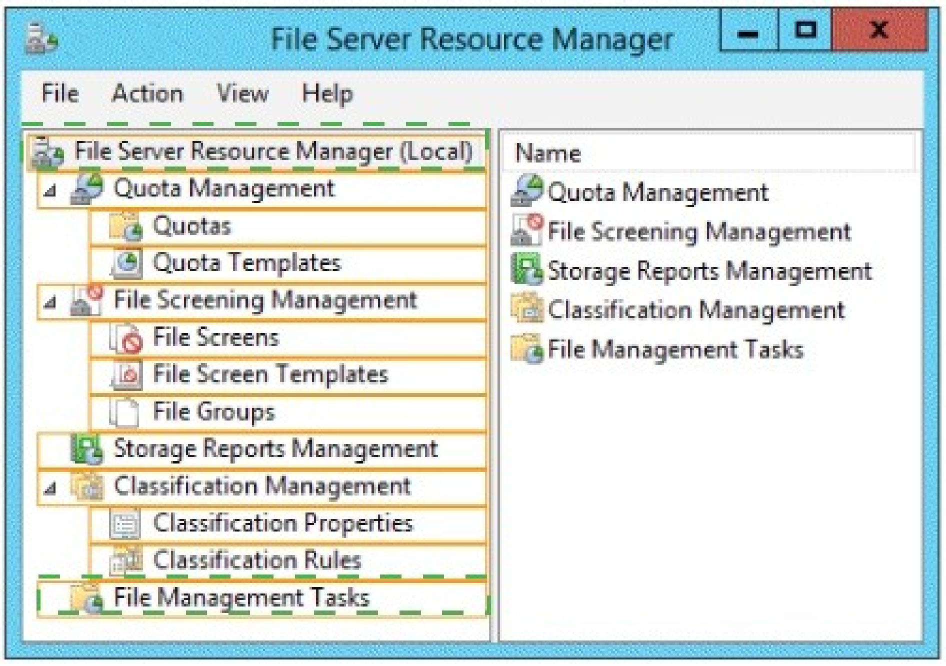
NEW QUESTION 1
HOTSPOT - (Topic 1)
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.
You need to configure Server1 to meet the following requirements:
? Ensure that old files in a folder named Folder1 are archived automatically to a folder named Archive1.
? Ensure that all storage reports are saved to a network share.
Which two nodes should you configure? To answer, select the appropriate two nodes in the answer area.


File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
File Screens
File Screen Templates
File Groups
Storage Reports Management
Classification Management
Classification Properties
Classification Rules
File Management Tasks
Name
Quota Management
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks

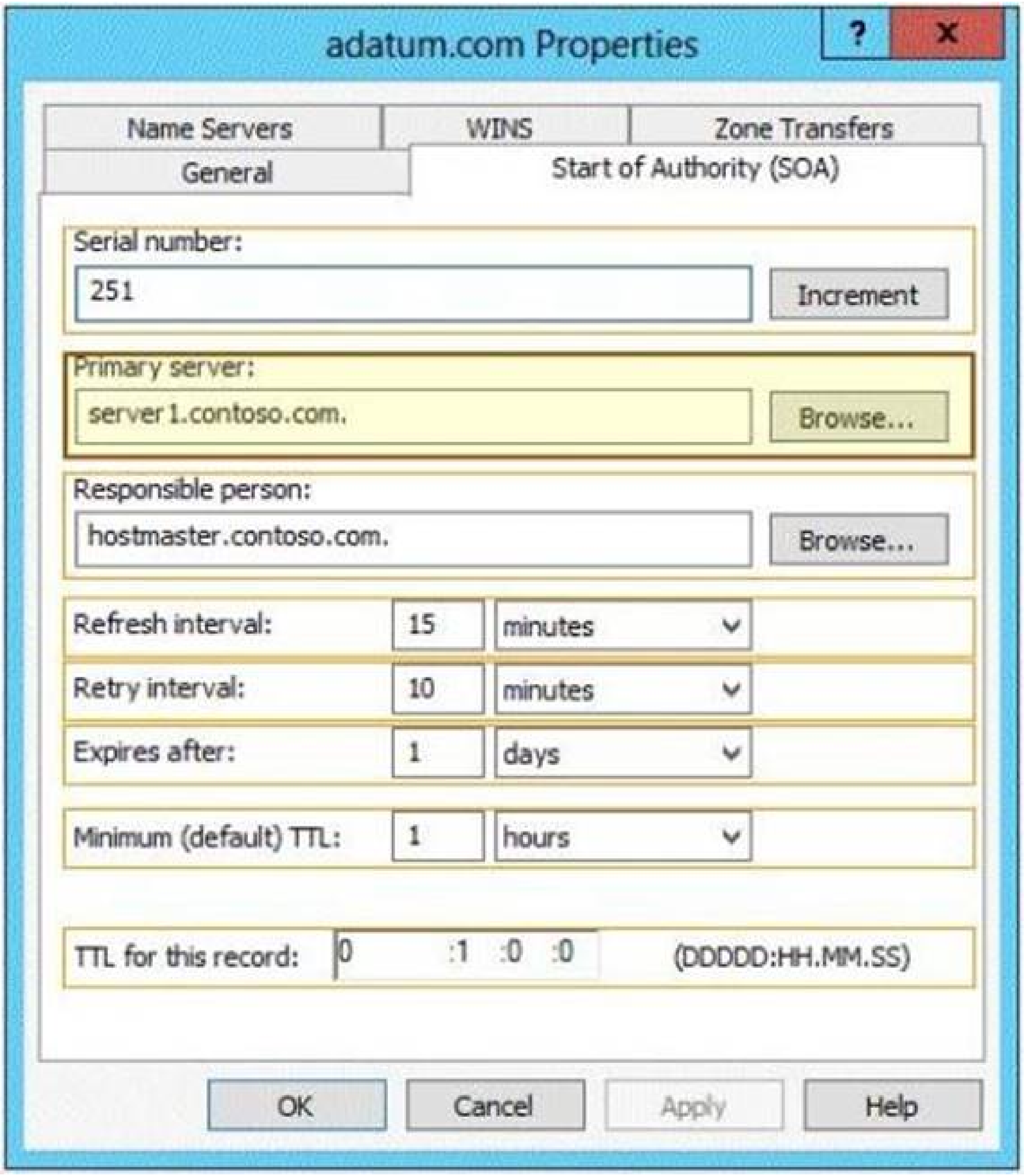
A. Mastered
B. Not Mastered

Answer: A

Explanation:


File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
File Screens
File Screen Templates
File Groups
Storage Reports Management
Classification Management
Classification Properties
Classification Rules
File Management Tasks
Name
Quota Management
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks

NEW QUESTION 2
HOTSPOT - (Topic 1)
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.



adatum.com Properties

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

Serial number: 251 [Increment]

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

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

Refresh interval: 15 minutes

Retry interval: 10 minutes

Expires after: 1 days

Minimum (default) TTL: 1 hours

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

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

A. Mastered
B. Not Mastered

Answer: A

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.

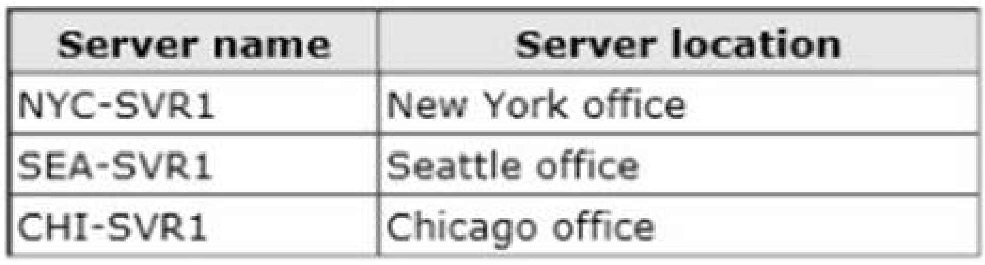
NEW QUESTION 3
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.
DC1 is backed up daily.
The domain has the Active Directory Recycle Bin enabled.
During routine maintenance, you delete 500 inactive user accounts and 100 inactive groups. One of the deleted groups is named Group1. Some of the deleted user accounts are members of some of the deleted groups.
For documentation purposes, you must provide a list of the members of Group1 before the group was deleted.
You need to identify the names of the users who were members of Group1 prior to its deletion.
You want to achieve this goal by using the minimum amount of administrative effort. What should you do first?

A. Mount the most recent Active Directory backup.
B. Reactivate the tombstone of Group1.
C. Perform an authoritative restore of Group1.
D. Use the Recycle Bin to restore Group1.

Answer: A

Explanation:
The Active Directory Recycle Bin does not have the ability to track simple changes to objects.
If the object itself is not deleted, no element is moved to the Recycle Bin for possible recovery in the future. In other words, there is no rollback capacity for changes to object properties, or, in other words, to the values of these properties.

NEW QUESTION 4
- (Topic 1)
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.



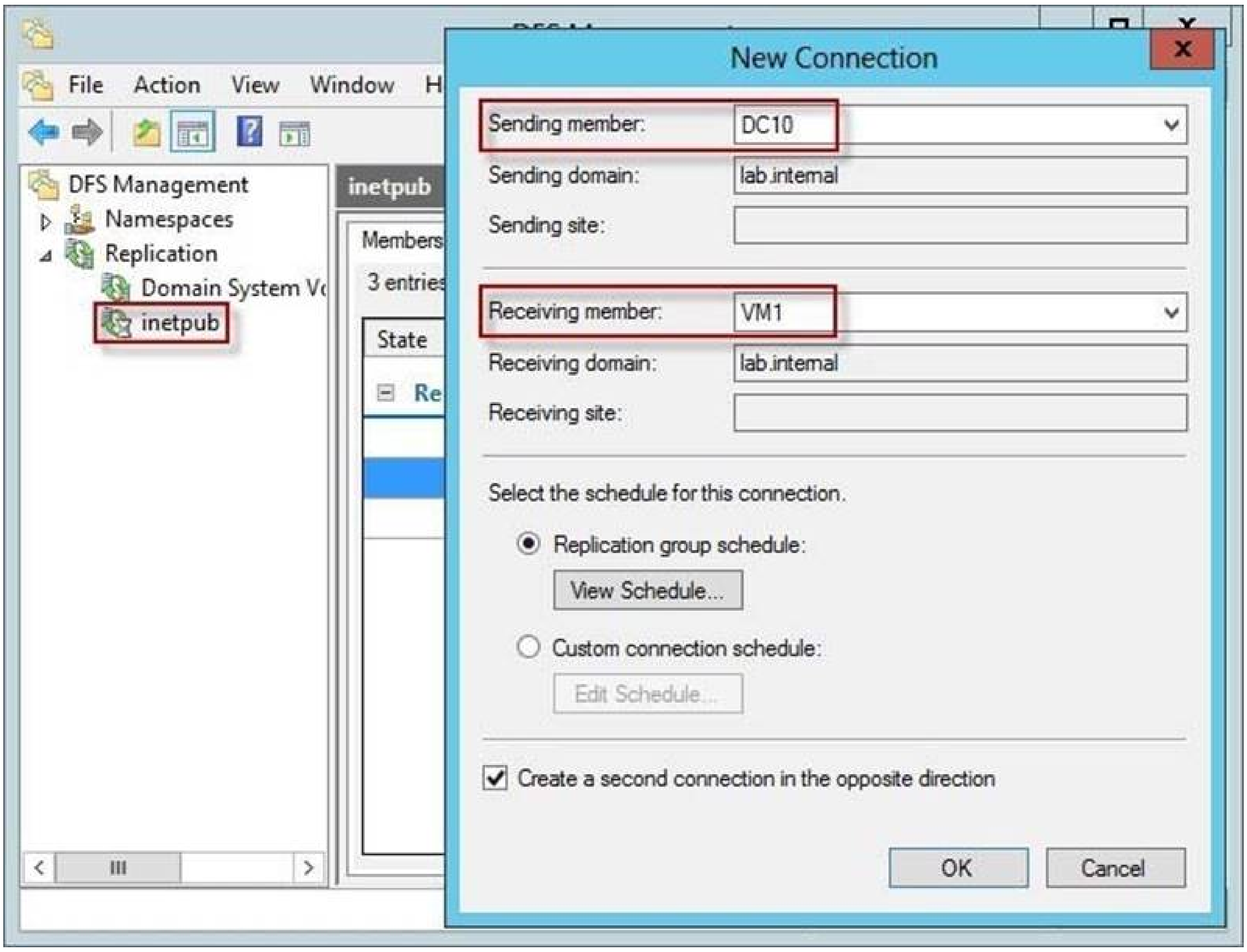
Server name	Server location
NYC-SVR1	New York office
SEA-SVR1	Seattle office
CHI-SVR1	Chicago office

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:



New Connection

Sending member: DC10
Sending domain: lab.internal
Sending site:

Receiving member: VM1
Receiving domain: lab.internal
Receiving site:

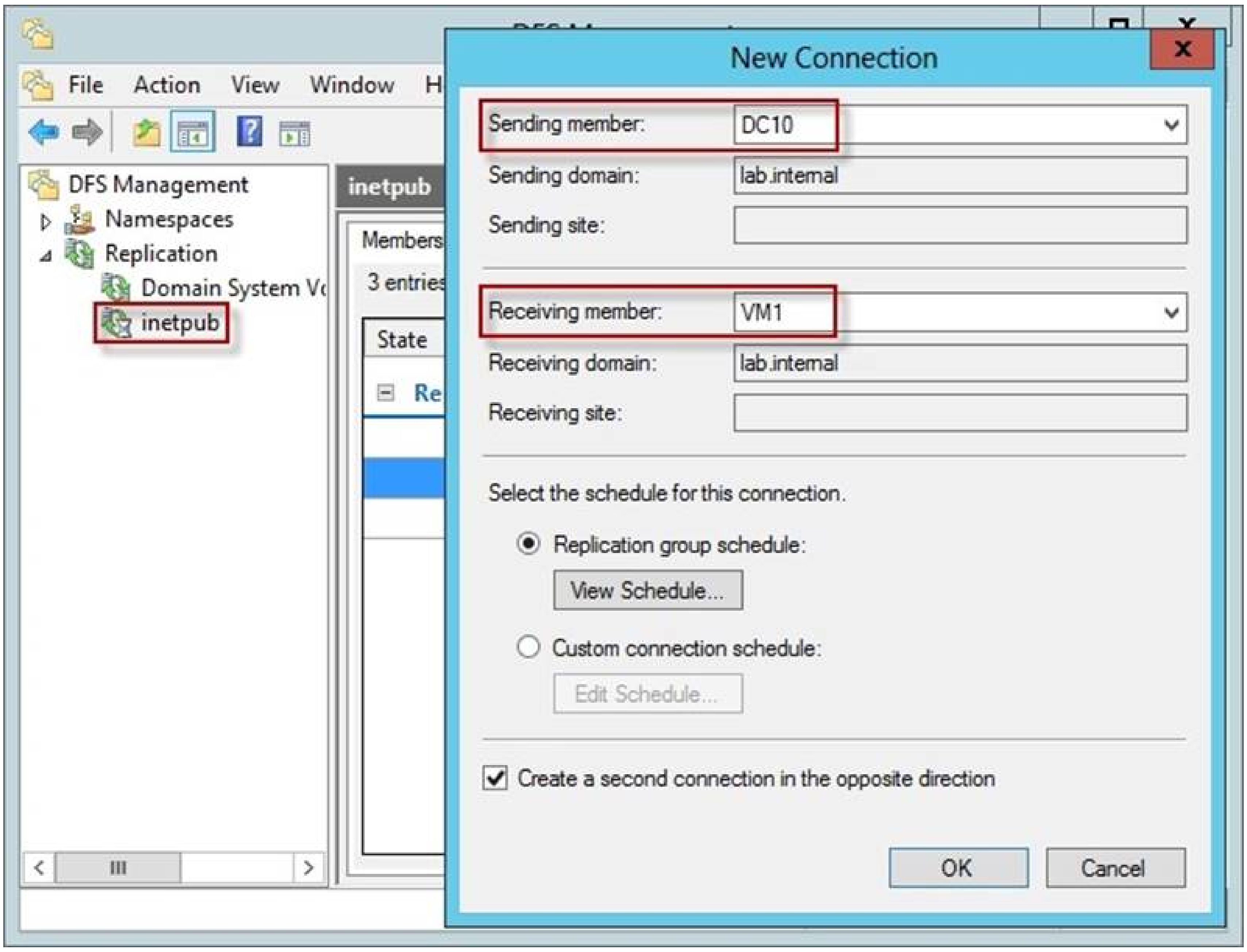
Select the schedule for this connection.

● Replication group schedule:
View Schedule...
○ Custom connection schedule:
Edit Schedule...

☑ Create a second connection in the opposite direction

OK Cancel

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.”



Sending member: DC10
Sending domain: lab.internal
Sending site:
Receiving member: VM1
Receiving domain: lab.internal
Receiving site:

Select the schedule for this connection.

● Replication group schedule:

View Schedule...

○ Custom connection schedule:

Edit Schedule...

☑ Create a second connection in the opposite direction

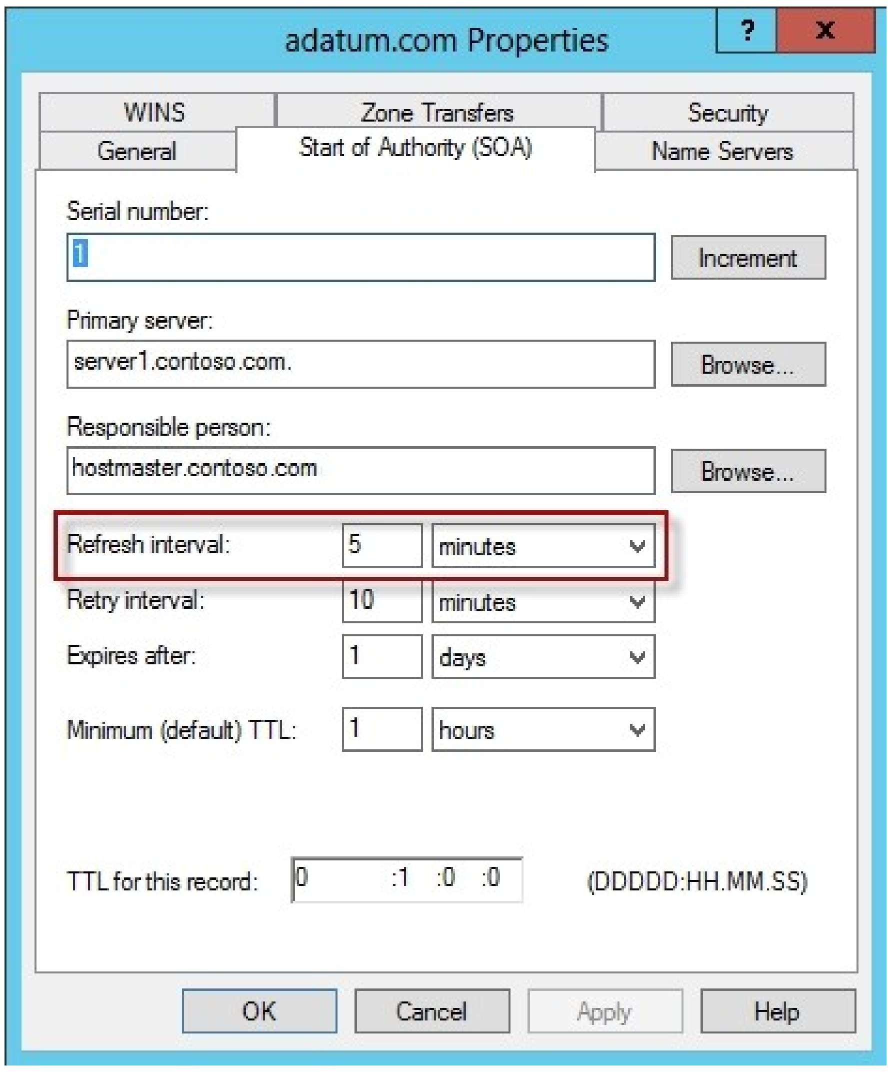
Reference:
http: //faultbucket. ca/2012/08/fixing-a-dfsr-connection-problem/
http: //faultbucket. ca/2012/08/fixing-a-dfsr-connection-problem/
http: //technet. microsoft. com/en-us/library/cc771941. aspx

NEW QUESTION 5
- (Topic 1)
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.



Serial number: 1

Primary server: server1.contoso.com.

Responsible person: hostmaster.contoso.com

Refresh interval: 5 minutes

Retry interval: 10 minutes

Expires after: 1 days

Minimum (default) TTL: 1 hours

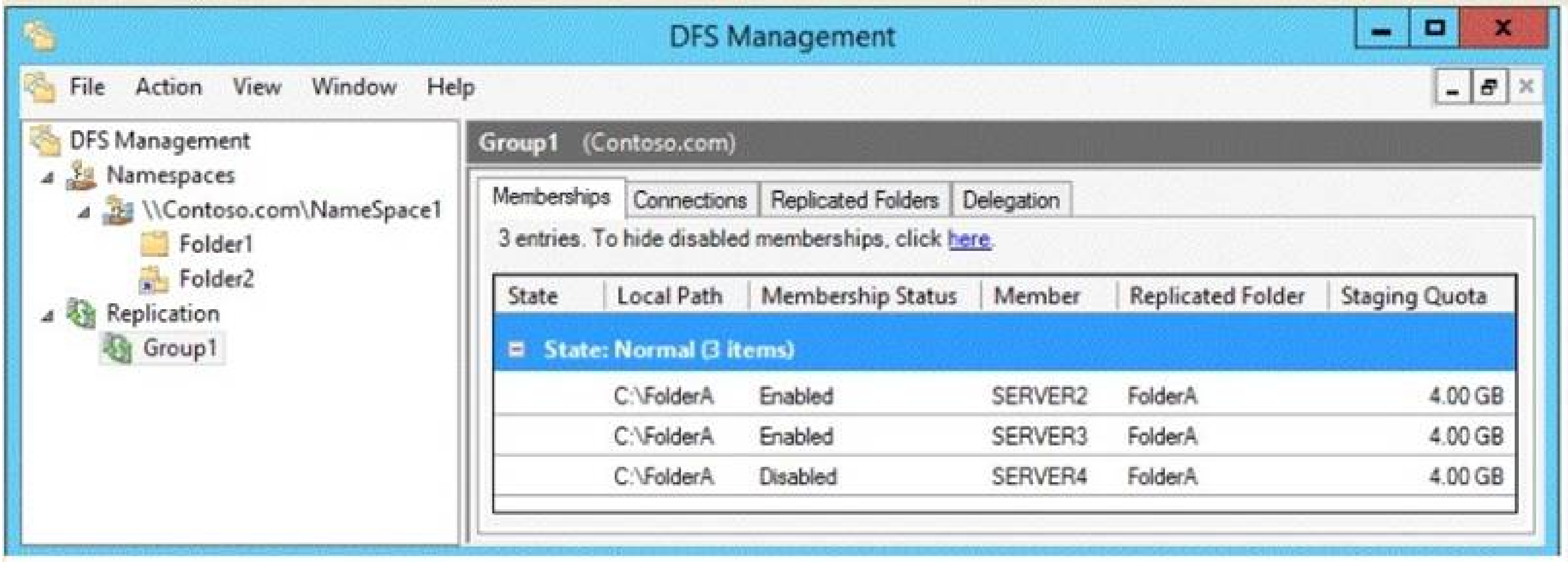
TTL for this record: 0 :1 :0 :0 (DDDDD:HH.MM.SS)

NEW QUESTION 6

HOTSPOT - (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains three servers named Server2, Server3, and Server4. Server2 and Server4 host a Distributed File System (DFS) namespace named Namespace1.

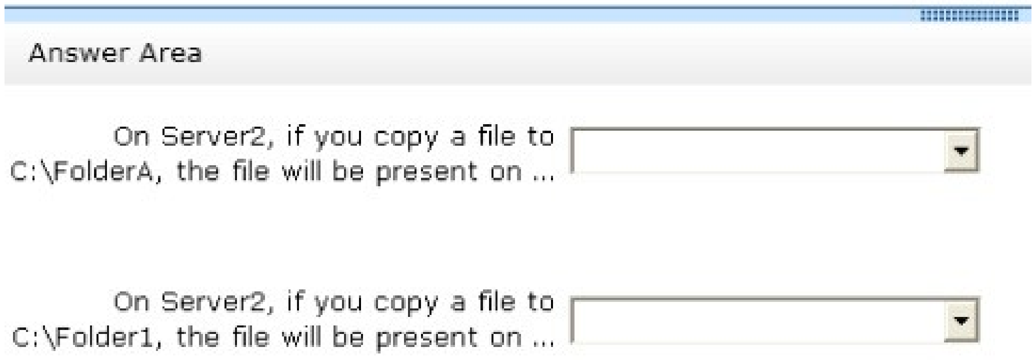
You open the DFS Management console as shown in the exhibit. (Click the Exhibit button.)



3 entries. To hide disabled memberships, click here.

State	Local Path	Membership Status	Member	Replicated Folder	Staging Quota
⊟ State: Normal (3 items)					
	C:\FolderA	Enabled	SERVER2	FolderA	4.00 GB
	C:\FolderA	Enabled	SERVER3	FolderA	4.00 GB
	C:\FolderA	Disabled	SERVER4	FolderA	4.00 GB

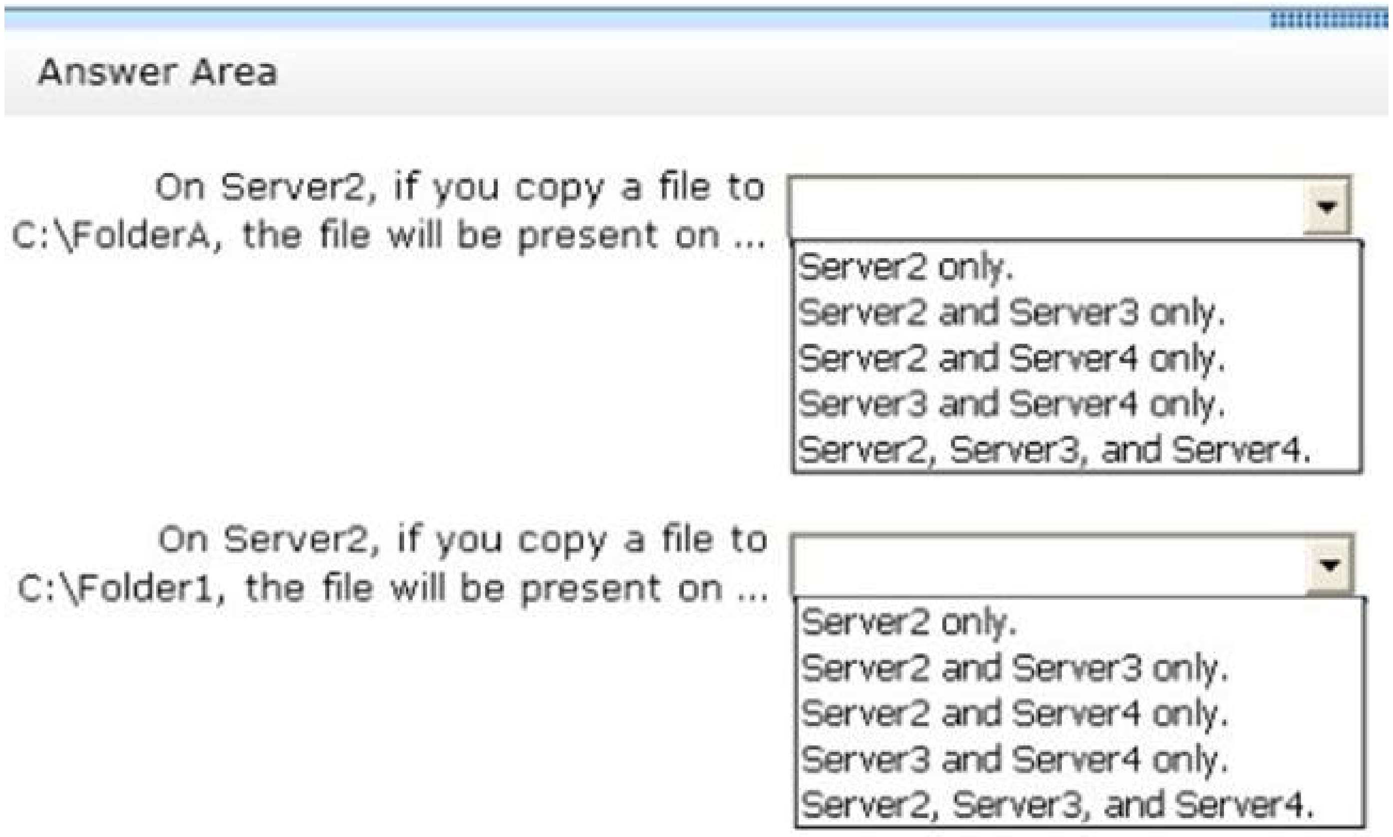
To answer, complete each statement according to the information presented in the exhibit. Each correct selection is worth one point.



Answer Area

On Server2, if you copy a file to C:\FolderA, the file will be present on ... [▾]

On Server2, if you copy a file to C:\Folder1, the file will be present on ... [▾]



Answer Area

On Server2, if you copy a file to C:\FolderA, the file will be present on ...

- Server2 only.
- Server2 and Server3 only.
- Server2 and Server4 only.
- Server3 and Server4 only.
- Server2, Server3, and Server4.

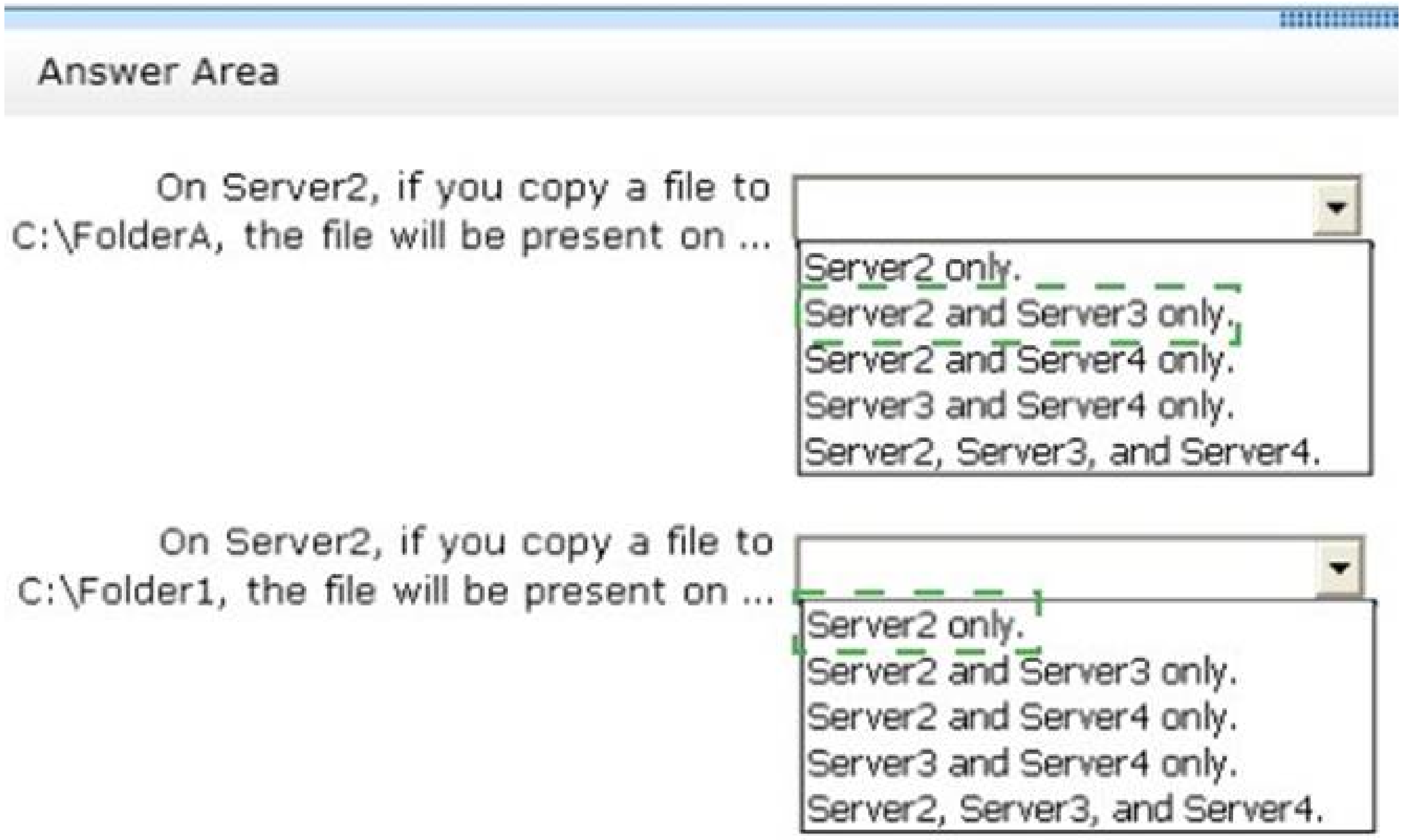
On Server2, if you copy a file to C:\Folder1, the file will be present on ...

- Server2 only.
- Server2 and Server3 only.
- Server2 and Server4 only.
- Server3 and Server4 only.
- Server2, Server3, and Server4.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

On Server2, if you copy a file to C:\FolderA, the file will be present on ...

- Server2 only.
- [✓ Server2 and Server3 only.]
- Server2 and Server4 only.
- Server3 and Server4 only.
- Server2, Server3, and Server4.

On Server2, if you copy a file to C:\Folder1, the file will be present on ...

- [✓ Server2 only.]
- Server2 and Server3 only.
- Server2 and Server4 only.
- Server3 and Server4 only.
- Server2, Server3, and Server4.

NEW QUESTION 7
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. The domain contains a Web server named www.contoso.com. The Web server is available on the Internet.
You implement DirectAccess by using the default configuration.
You need to ensure that users never attempt to connect to www.contoso.com by using DirectAccess. The solution must not prevent the users from using DirectAccess to access other resources in contoso.com.
Which settings should you configure in a Group Policy object (GPO)?

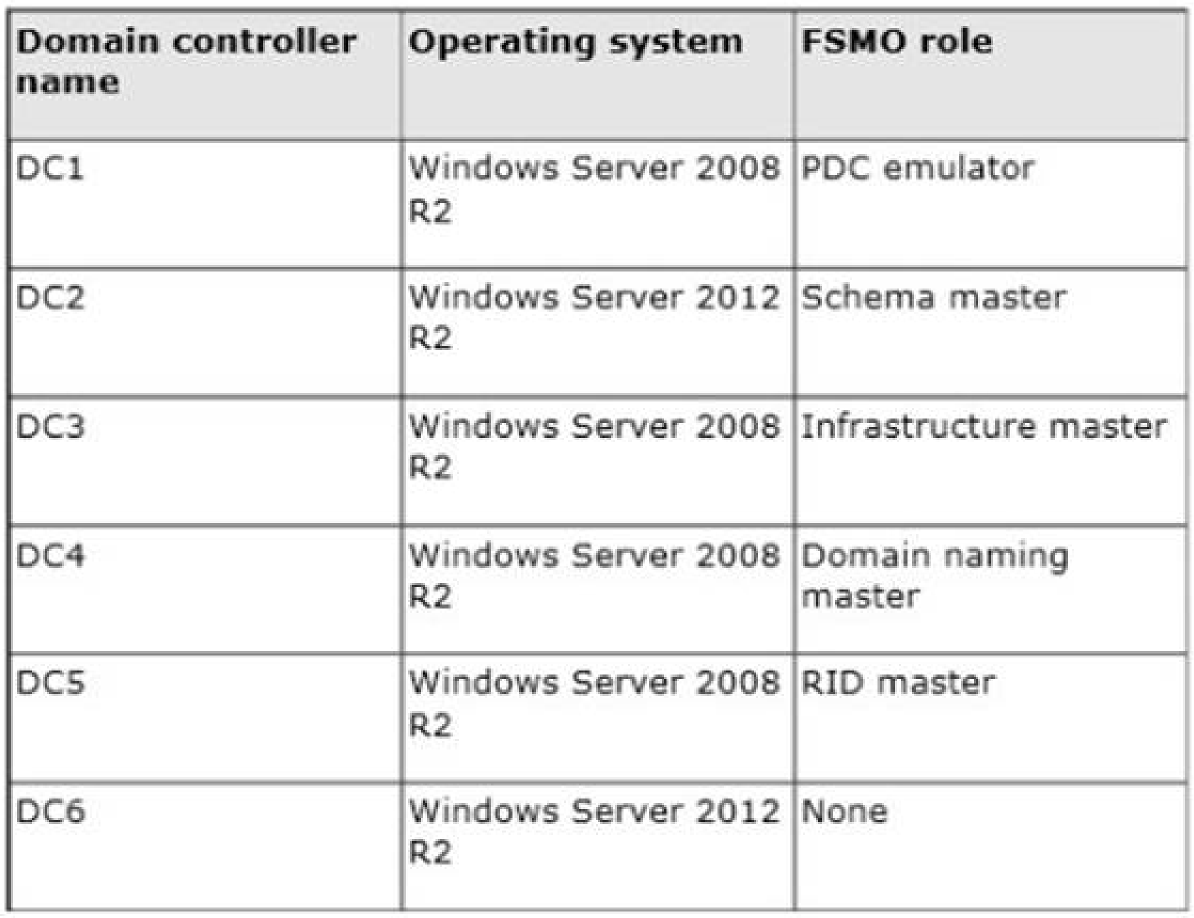
A. DirectAccess Client Experience Settings
B. DNS Client
C. Name Resolution Policy
D. Network Connections

Answer: C

Explanation:
For DirectAccess, the NRPT must be configured with the namespaces of your intranet with a leading dot (for example, internal.contoso.com or . corp.contoso.com). For a DirectAccess client, any name request that matches one of these namespaces will be sent to the specified intranet Domain Name System (DNS) servers.
Include all intranet DNS namespaces that you want DirectAccess client computers to access.
There are no command line methods for configuring NRPT rules. You must use Group Policy settings. To configure the NRPT through Group Policy, use the

Group Policy add-in at Computer Configuration \Policies\Windows Settings\Name Resolution Policy in the Group Policy object for DirectAccess clients. You can create a new NRPT rule and edit or delete existing rules. For more information, see Configure the NRPT with Group Policy.

NEW QUESTION 8
- (Topic 1)
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

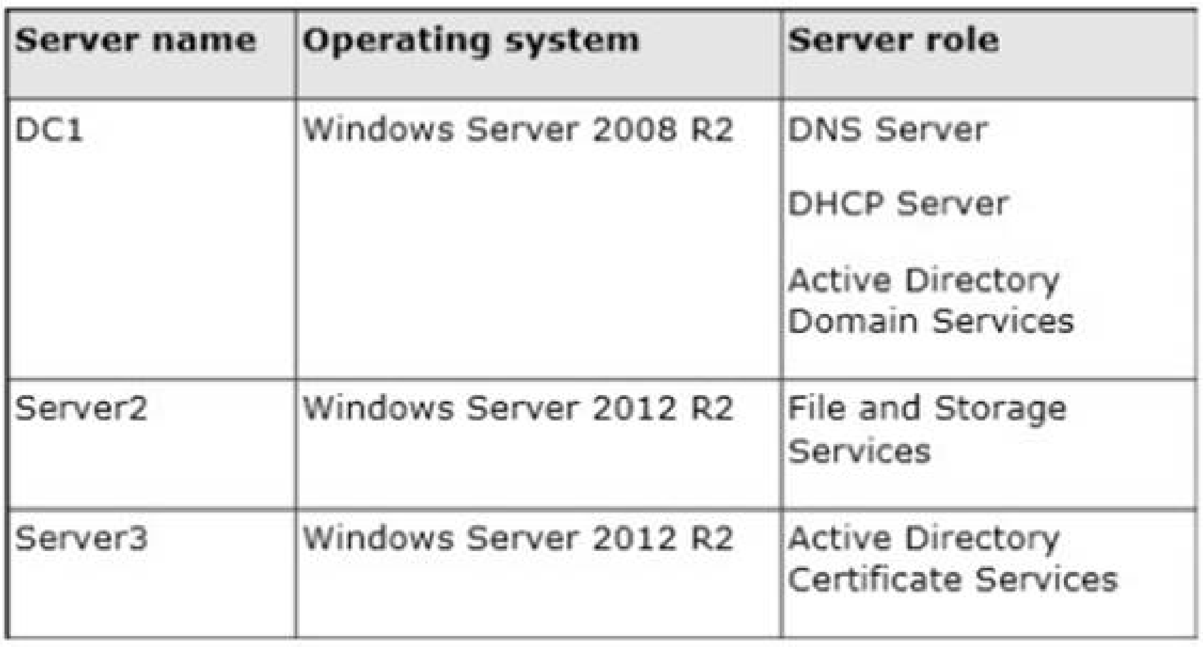
The network contains a server named Server1 that has the Hyper-v server role installed. DC6 is a virtual machine that is hosted on Server1.
You need to ensure that you can clone DC6. Which FSMO role should you transfer to DC2?

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 9
- (Topic 1)
Your network contains an Active Directory forest named contoso.com.
The domain contains three servers. The servers are configured as shown in the following table.



Server name	Operating system	Server role
DC1	Windows Server 2008 R2	DNS Server DHCP Server Active Directory Domain Services
Server2	Windows Server 2012 R2	File and Storage Services
Server3	Windows Server 2012 R2	Active Directory Certificate Services

You need to identify which server role must be deployed to the network to support the planned implementation.
Which role should you identify?

A. Network Policy and Access Services
B. Volume Activation Services
C. Windows Deployment Services
D. Active Directory Rights Management Services

Answer: C

Explanation:
Windows Deployment Services (WDS) is a server role that enables you to remotely deploy Windows operating systems. You can use it to set up new computers by using a network- based installation. This means that you do not have to install each operating system directly from a CD, USB drive or DVD. To use Windows Deployment Services, you should have a working knowledge of common desktop deployment technologies and networking components, including Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Active Directory Domain Services (AD DS). It is also helpful to understand the Preboot execution Environment (also known as Pre-Execution Environment).

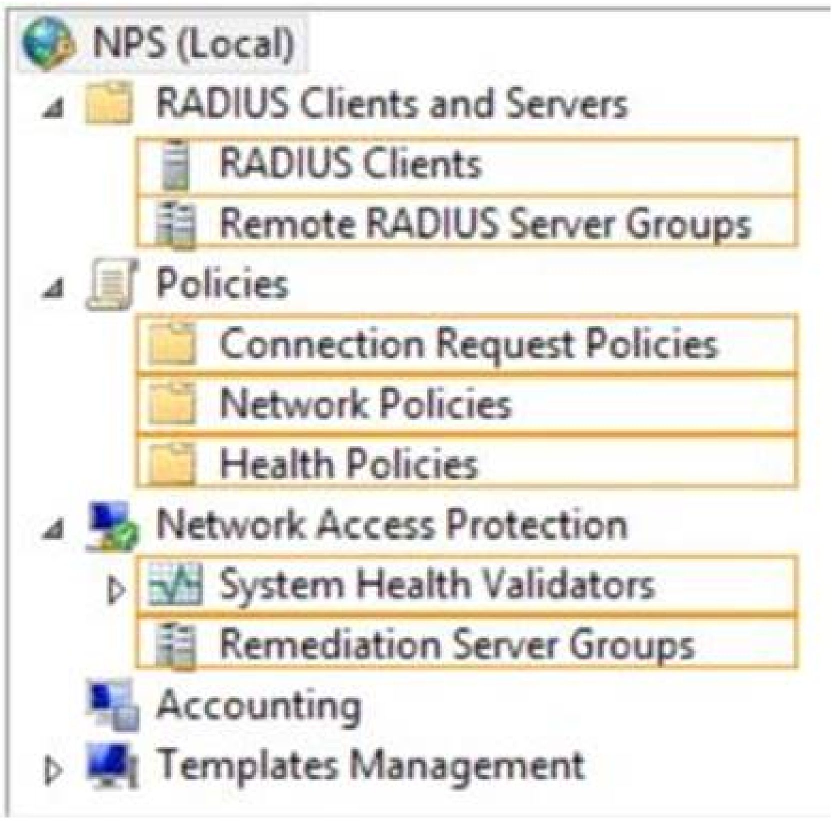
NEW QUESTION 10
- (Topic 1)
Your network contains two Active Directory forests named contoso.com and dev.contoso.com. The contoso.com forest contains a domain controller named DC1. The dev.contoso.com forest contains a domain controller named DC2. Each domain contains an organizational unit (OU) named 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

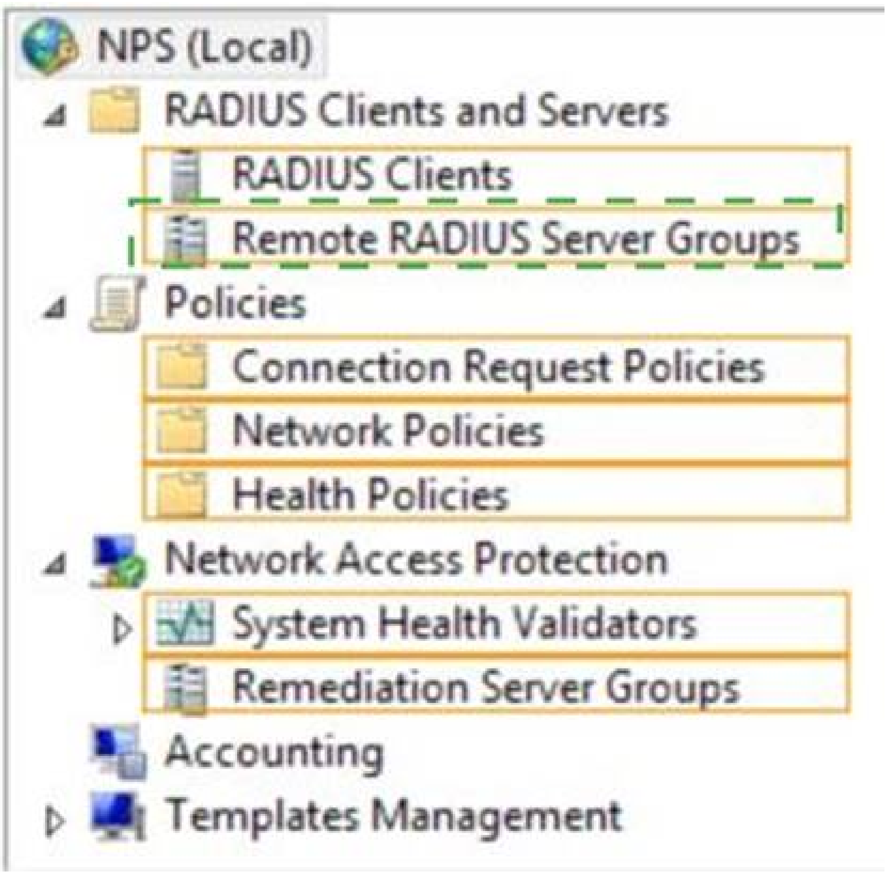
NEW QUESTION 10
HOTSPOT - (Topic 1)
Your network contains a RADIUS server named Server1.
You install a new server named Server2 that runs Windows Server 2012 R2 and has Network Policy Server (NPS) installed.
You need to ensure that all accounting requests for Server2 are forwarded to Server1.
On Server2, 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

A. Mastered
B. Not Mastered

Answer: A

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 15

- (Topic 1)

You have Windows Server 2012 R2 installation media that contains a file named Install.wim. You need to identify the permissions of the mounted images in Install.wim.

What should you do?

A. Run dism.exe and specify the /get-mountedwiminfo parameter.
B. Run imagex.exe and specify the /verify parameter.
C. Run imagex.exe and specify the /ref parameter.
D. Run dism.exe and specify the/get-imageinfo parameter.

Answer: A

Explanation:

/Get-MountedWimInfo Lists the images that are currently mounted and information about the mounted image such as read/write permissions, mount location, mounted file path, and mounted image index.

References:

http: //technet. microsoft. com/en-us/library/cc749447(v=ws. 10). aspx http: //technet. microsoft. com/en-us/library/dd744382(v=ws. 10). aspx http: //technet. microsoft. com/en-us/library/hh825224. aspx

NEW QUESTION 19

- (Topic 1)

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 create an Active Directory snapshot of DC1 each day.

You need to view the contents of an Active Directory snapshot from two days ago. What should you do first?

A. Run the dsamain.exe command.
B. Stop the Active Directory Domain Services (AD DS) service.
C. Start the Volume Shadow Copy Service (VSS).
D. Run the ntdsutil.exe command.

Answer: A

Explanation:

Dsamain.exe exposes Active Directory data that is stored in a snapshot or backup as a Lightweight Directory Access Protocol (LDAP) server.

Reference: http://technet.microsoft.com/en-us/library/cc772168.aspx

NEW QUESTION 21

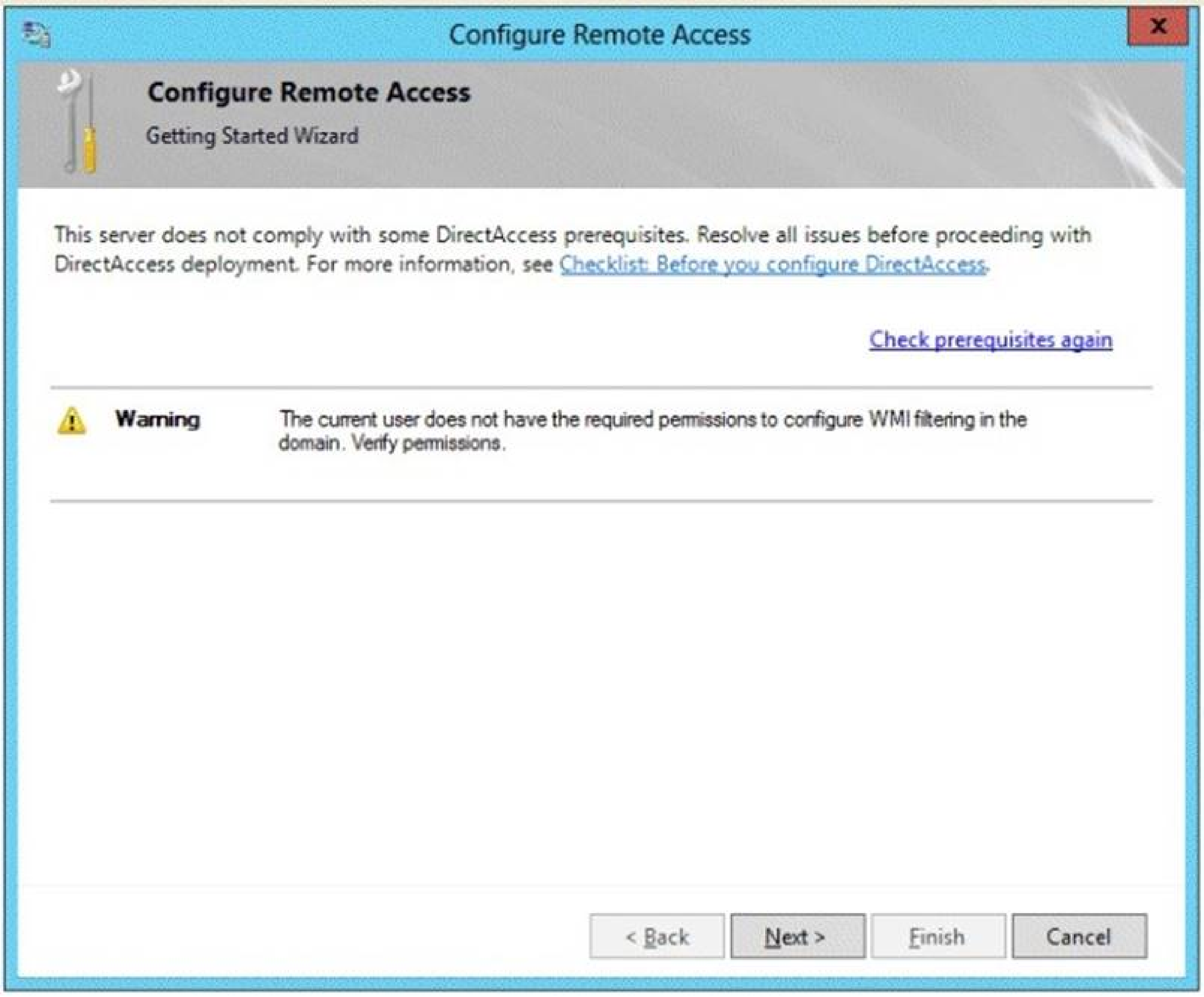
- (Topic 1)

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.)



This server does not comply with some DirectAccess prerequisites. Resolve all issues before proceeding with DirectAccess deployment. For more information, see Checklist: Before you configure DirectAccess.

Warning The current user does not have the required permissions to configure WMI filtering in the domain. Verify permissions.

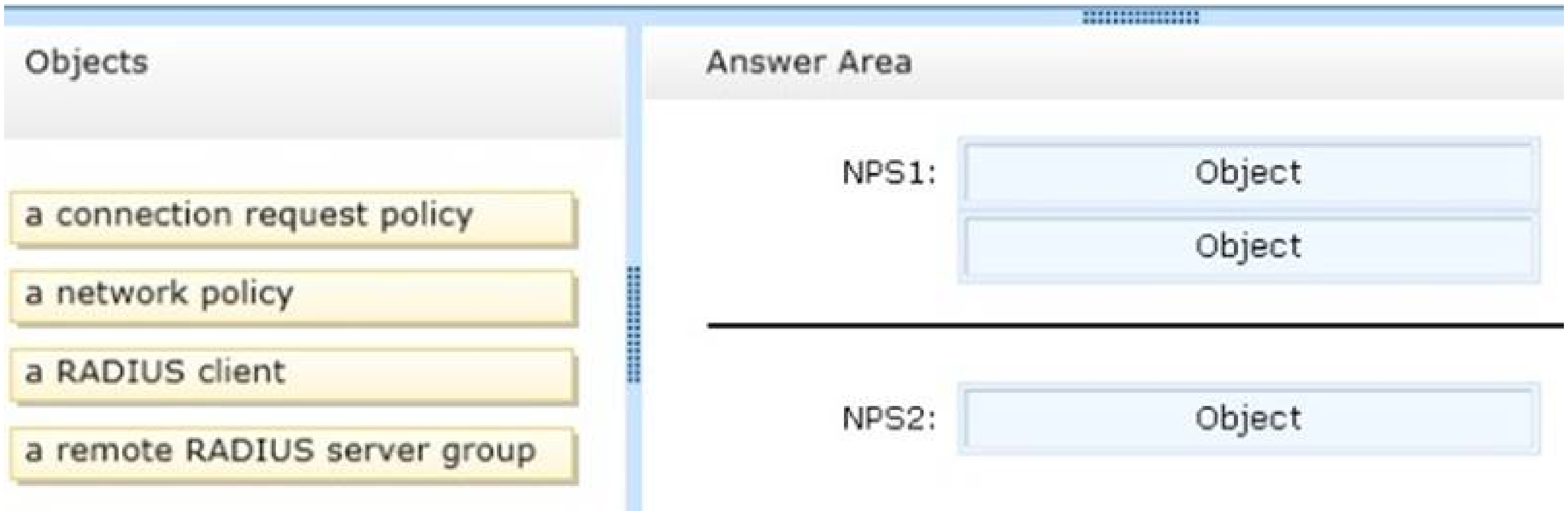
You need to ensure that you can configure DirectAccess successfully. The solution must minimize the number of permissions assigned to User2.
To which group should you add User2?

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 24
DRAG DROP - (Topic 1)
Your network contains an Active Directory forest named contoso.com. The forest contains a Network Policy Server (NPS) server named NPS1 and a VPN server named VPN1. VPN1 forwards all authentication requests to NPS1.
A partner company has an Active Directory forest named adatum.com. The adatum.com forest contains an NPS server named NPS2.
You plan to grant users from adatum.com VPN access to your network. You need to authenticate the users from adatum.com on VPN1.
What should you create on each NPS server?
To answer, drag the appropriate objects to the correct NPS servers. Each object may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Objects

- a connection request policy
- a network policy
- a RADIUS client
- a remote RADIUS server group

Answer Area

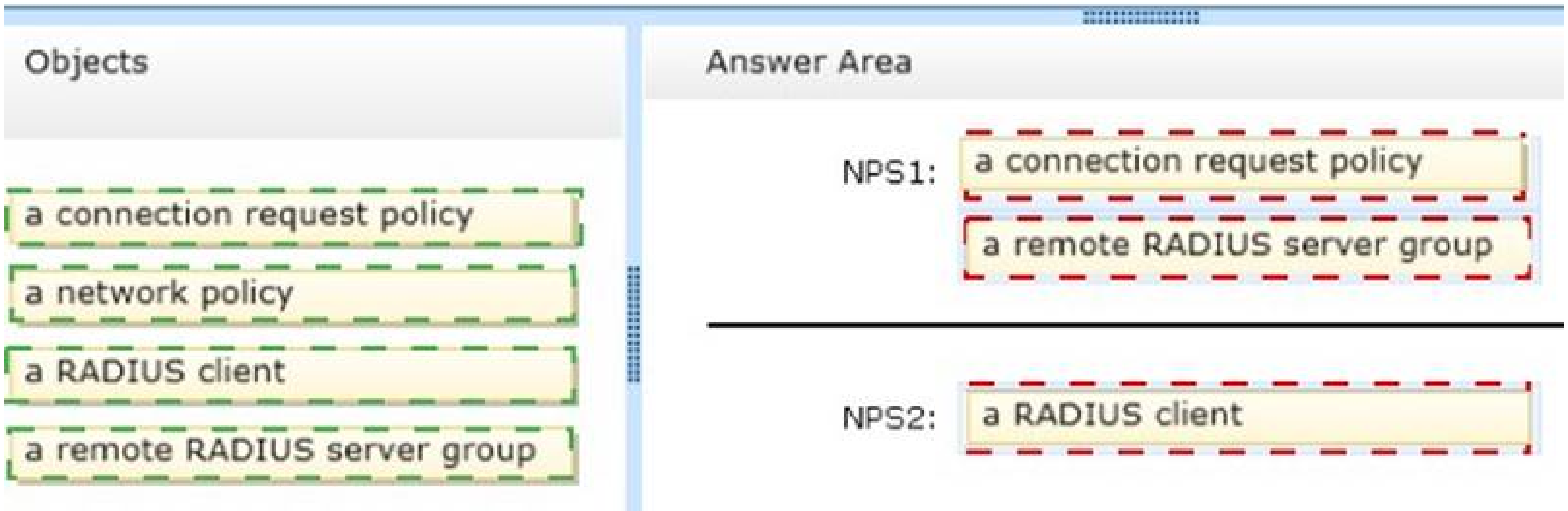
NPS1: Object
Object

NPS2: Object

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Objects

- a connection request policy
- a network policy
- a RADIUS client
- a remote RADIUS server group

Answer Area

NPS1: a connection request policy
a remote RADIUS server group

NPS2: a RADIUS client

NEW QUESTION 26
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. The Active Directory Recycle bin is enabled for contoso.com.
A support technician accidentally deletes a user account named User1. You need to restore the User1 account.
Which tool should you use?

A. Ldp
B. Esentutl
C. Active Directory Administrative Center
D. Ntdsutil

Answer: C

NEW QUESTION 30
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
The domain contains 200 Group Policy objects (GPOs).
An administrator named Admin1 must be able to add new WMI filters from the Group Policy Management Console (GPMC).
You need to delegate the required permissions to Admin1. The solution must minimize the number of permissions assigned to Admin1.
What should you do?

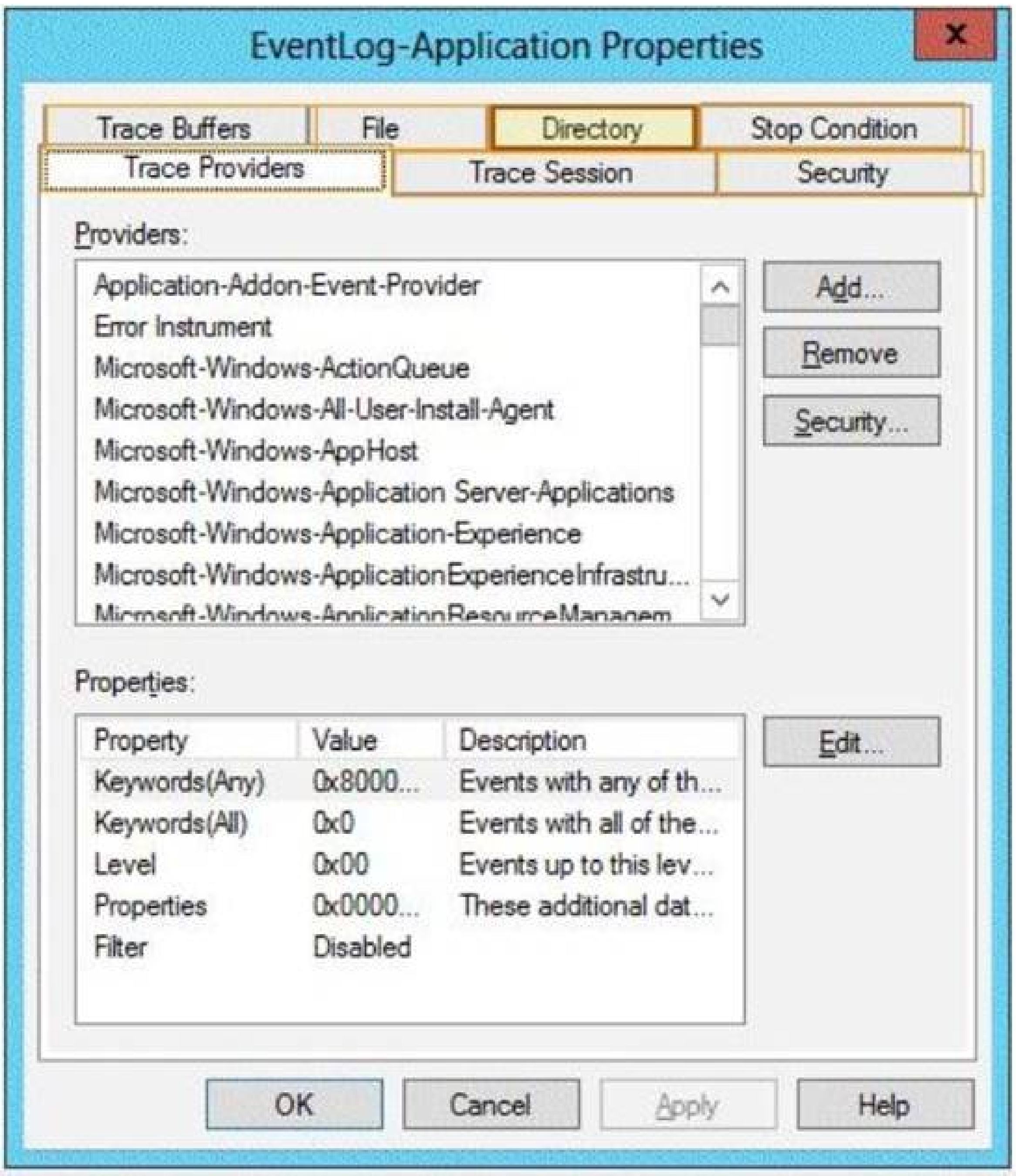
A. From Active Directory Users and Computers, add Admin1 to the WinRMRemoteWMIUsers group.
B. From Group Policy Management, assign Creator Owner to Admin1 for the WMI Filters container.
C. From Active Directory Users and Computers, add Admin1 to the Domain Admins group.
D. From Group Policy Management, assign Full control to Admin1 for the WMI Filters container.

Answer: D

Explanation:
Users with Full control permissions can create and control all WMI filters in the domain, including WMI filters created by others.
Users with Creator owner permissions can create WMI filters, but can only control WMI filters that they create.
Reference: http://technet.microsoft.com/en-us/library/cc757429(v=ws.10).aspx

NEW QUESTION 35
HOTSPOT - (Topic 1)
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 runs Windows Server 2012 R2.

You enable the EventLog-Application event trace session.
You need to set the maximum size of the log file used by the trace session to 10 MB. From which tab should you perform the configuration? To answer, select the appropriate
tab in the answer area.



Providers:

Application-Addon-Event-Provider
Error Instrument
Microsoft-Windows-ActionQueue
Microsoft-Windows-All-User-Install-Agent
Microsoft-Windows-AppHost
Microsoft-Windows-Application Server-Applications
Microsoft-Windows-Application-Experience
Microsoft-Windows-ApplicationExperienceInfrastru...
Microsoft-Windows-ApplicationResourceManagem

Properties:

Property	Value	Description
Keywords(Any)	0x8000...	Events with any of th...
Keywords(All)	0x0	Events with all of the...
Level	0x00	Events up to this lev...
Properties	0x0000...	These additional dat...
Filter	Disabled	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Note: By default, logging stops only if you set an expiration date as part of the logging schedule. Using the options on the Stop Condition tab, you can configure the log file to stop automatically after a specified period of time, such as seven days, or when the log file is full (if you've set a maximum size limit).

NEW QUESTION 36
- (Topic 1)
Your network contains an Active Directory domain named contoso.com.
All user accounts for the marketing department reside in an organizational unit (OU) named OU1. All user accounts for the finance department reside in an organizational unit (OU) named OU2.
You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU2. You configure the Group Policy preference of GPO1 to add a shortcut named Link1 to the desktop.
You discover that when a user signs in, the Link1 is not added to the desktop. You need to ensure that when a user signs in, Link1 is added to the desktop. What should you do?

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

Answer: D

Explanation:
Security filtering is a way of refining which users and computers will receive and apply the settings in a Group Policy object (GPO). Using security filtering, you can specify that only certain security principals within a container where the GPO is linked apply the GPO. Security group filtering determines whether the GPO as a whole applies to groups, users, or computers; it cannot be used selectively on different settings within a GPO.

NEW QUESTION 39
- (Topic 1)
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 8.1 Enterprise and Microsoft Office 2013.
You implement a Group Policy central store.

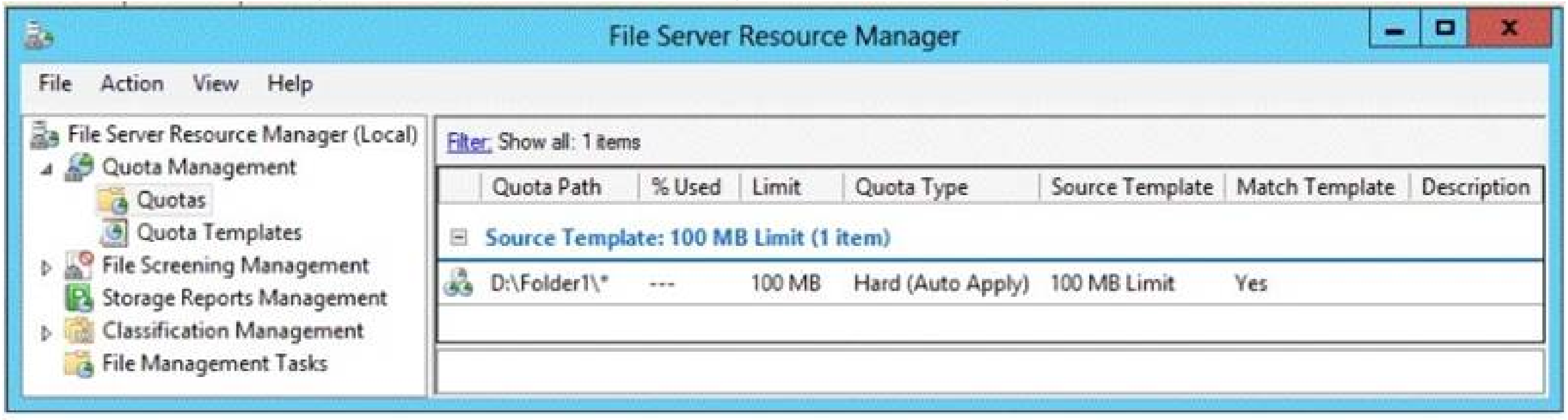
You need to modify the default Microsoft Office 2013 Save As location for all client computers. The solution must minimize administrative effort.
What should you configure in a Group Policy object (GPO)?

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

Answer: A

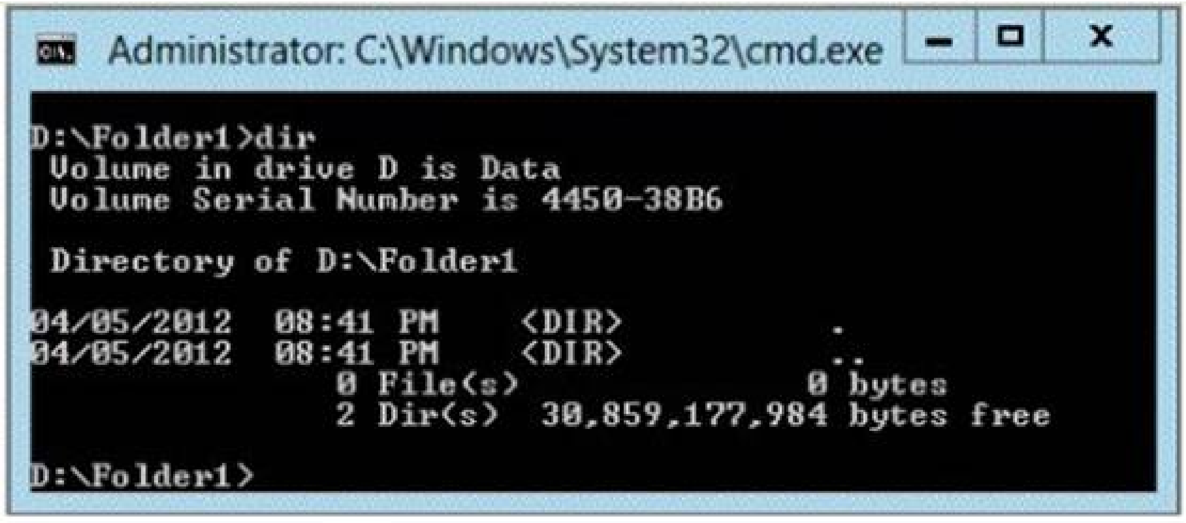
Explanation:
Group Policy preferences provide the means to simplify deployment and standardize configurations. They add to Group Policy a centralized system for deploying preferences (that is, settings that users can change later). You can also use Group Policy preferences to configure applications that 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.
Reference: http://technet.microsoft.com/en-us/library/dn581922.aspx

NEW QUESTION 43
- (Topic 1)
You have a server named Server1 that runs Windows Server 2012 R2.
An administrator creates a quota as shown in the Quota exhibit. (Click the Exhibit button.)


File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks
Filter: Show all: 1 items

Quota Path	% Used	Limit	Quota Type	Source Template	Match Template	Description
Source Template: 100 MB Limit (1 item)						
D:\Folder1*	---	100 MB	Hard (Auto Apply)	100 MB Limit	Yes	

You run the dir command as shown in the Dir exhibit. (Click the Exhibit button.)



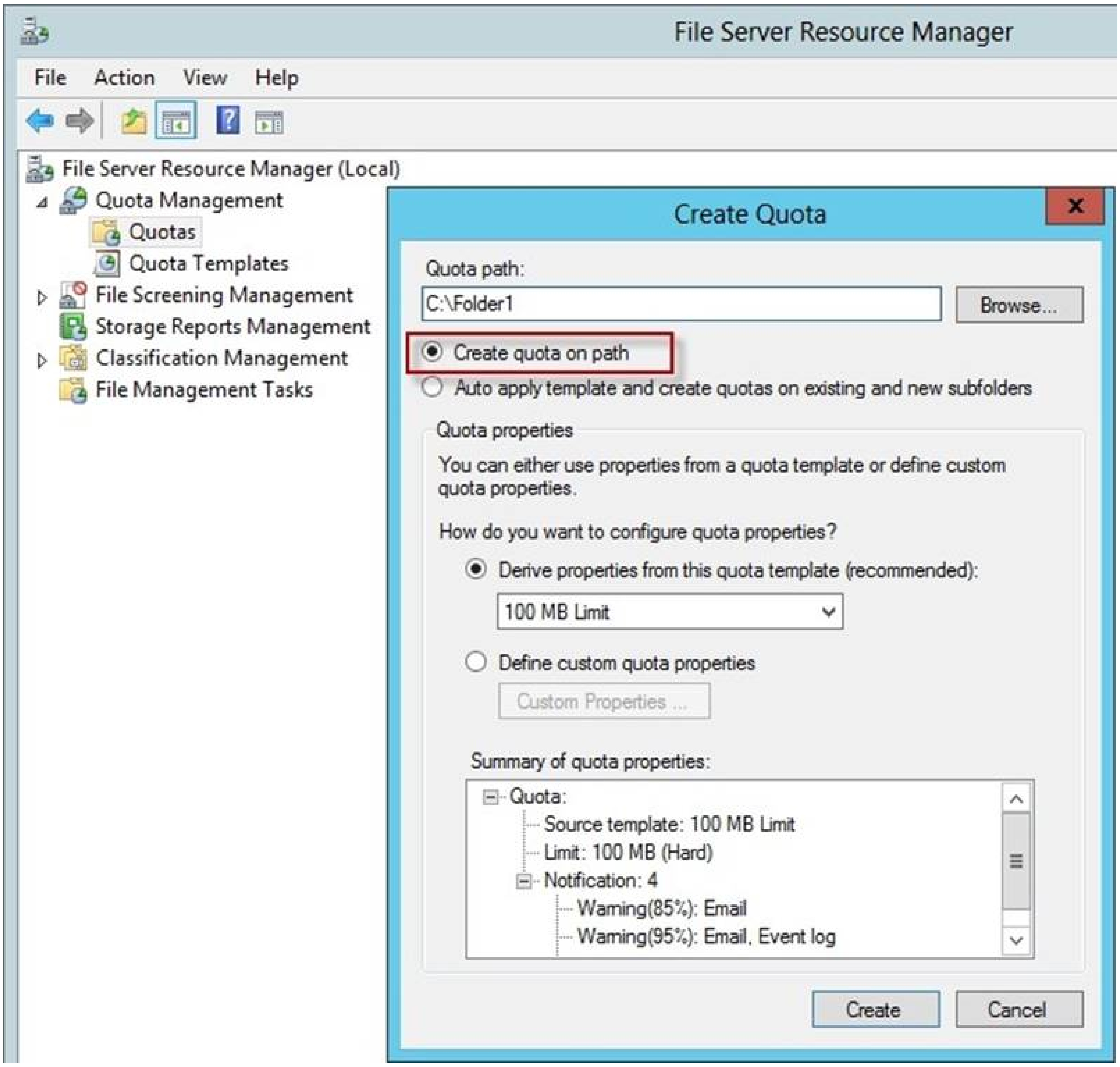
```
D:\Folder1>dir
 Volume in drive D is Data
 Volume Serial Number is 4450-38B6

 Directory of D:\Folder1

04/05/2012  08:41 PM    <DIR>          .
04/05/2012  08:41 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  30,859,177,984 bytes free

D:\Folder1>
```

You need to ensure that D:\Folder1 can only consume 100 MB of disk space. What should you do?

A. From File Server Resource Manager, create a new quota.
B. From File Server Resource Manager, edit the existing quota.
C. From the Services console, set the Startup Type of the Optimize drives service to Automatic.
D. From the properties of drive D, enable quota management.

Answer: A

Explanation:
1. In Quota Management, click the Quota Templates node.
2. In the Results pane, select the template on which you will base your new quota.
3. Right-click the template and click Create Quota from Template (or select Create Quota from Template from the Actions pane). This opens the Create Quota dialog box with the summary properties of the quota template displayed.
4. Under Quota path, type or browse to the folder that the quota will apply to.
5. Click the Create quota on path option. Note that the quota properties will apply to the entire folder.
Note: To create an auto apply quota, click the Auto apply template and create quotas on existing and new subfolders option. For more information about auto apply quotas, see Create an Auto Apply Quota.
6. Under Drive properties from this quota template, the template you used in step 2 to create your new quota is preselected (or you can select another template from the list). Note that the template's properties are displayed under Summary of quota properties.
7. Click Create.
Create a new Quota on path, without using the auto apply template and create quota on existing and new subfolders.


File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks
Create Quota
Browse...
Custom Properties ...
Create
Cancel

Quota path: C:\Folder1

● Create quota on path

○ Auto apply template and create quotas on existing and new subfolders

Quota properties

You can either use properties from a quota template or define custom quota properties.

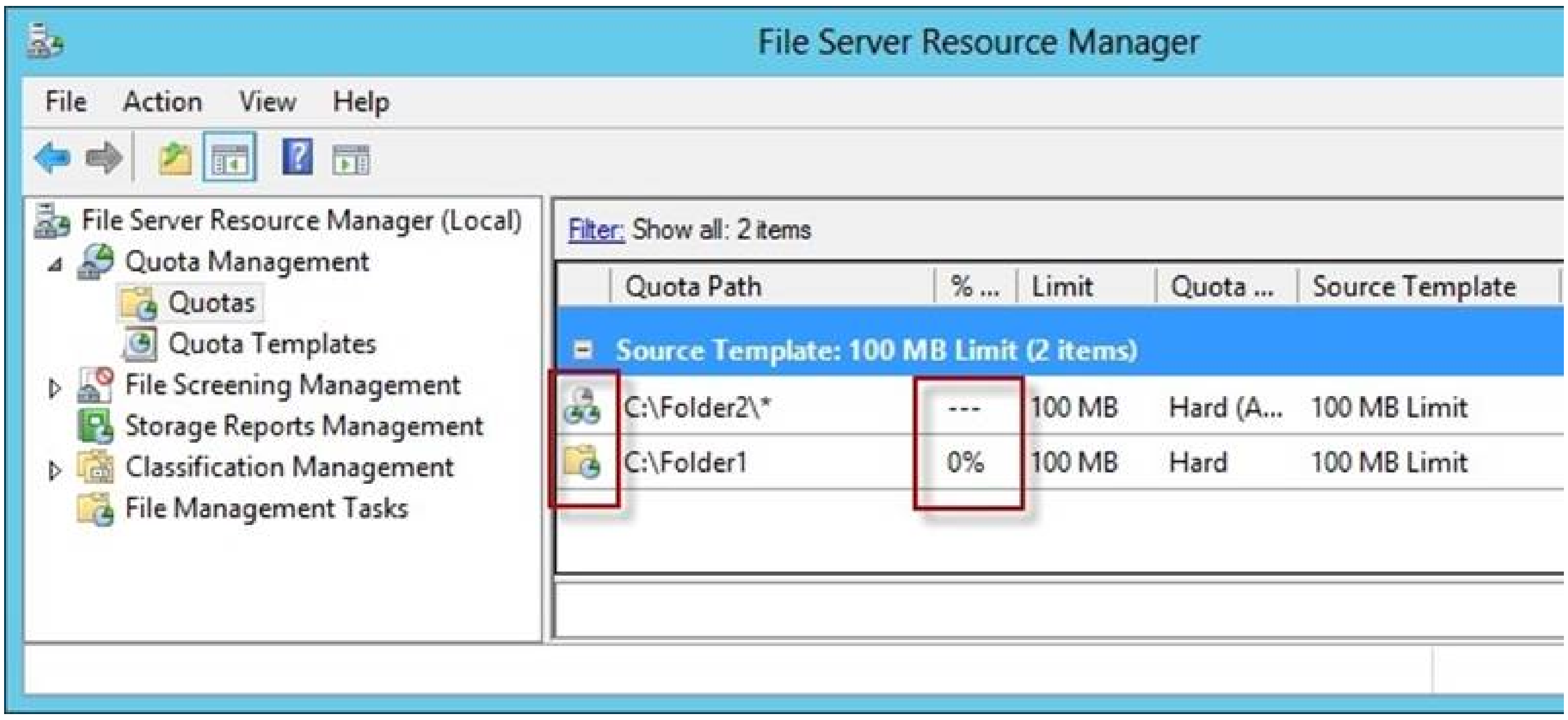
How do you want to configure quota properties?

● Derive properties from this quota template (recommended): 100 MB Limit

○ Define custom quota properties

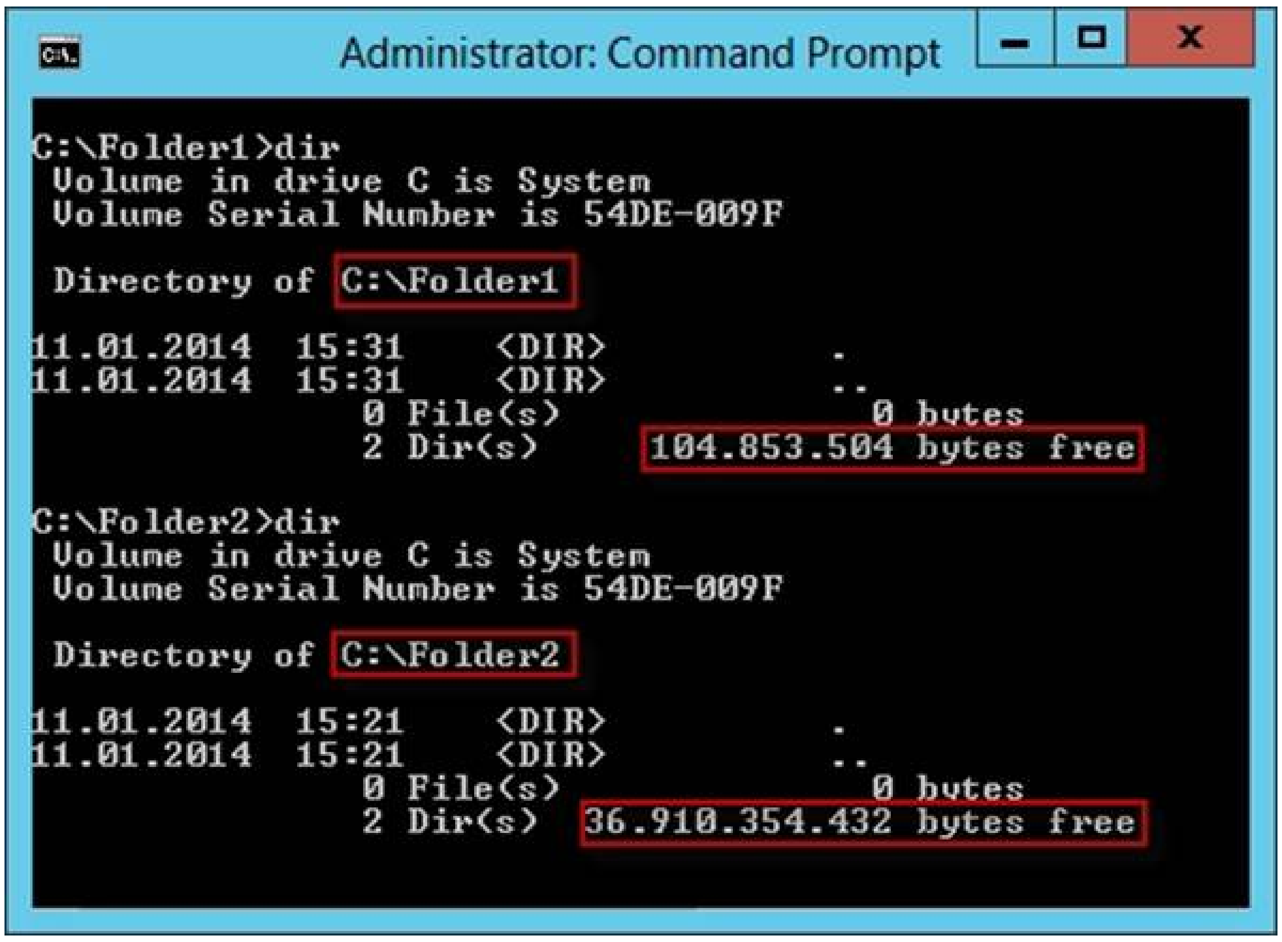
Summary of quota properties:

```
⊟ Quota:
    Source template: 100 MB Limit
    Limit: 100 MB (Hard)
  ⊟ Notification: 4
      Warning(85%): Email
      Warning(95%): Email, Event log
```


File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks

Filter: Show all: 2 items

Quota Path	% ...	Limit	Quota ...	Source Template
Source Template: 100 MB Limit (2 items)				
C:\Folder2\*	---	100 MB	Hard (A...	100 MB Limit
C:\Folder1	0%	100 MB	Hard	100 MB Limit



Administrator: Command Prompt

```
C:\Folder1>dir
 Volume in drive C is System
 Volume Serial Number is 54DE-009F

 Directory of C:\Folder1

11.01.2014  15:31    <DIR>          .
11.01.2014  15:31    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)     104.853.504 bytes free

C:\Folder2>dir
 Volume in drive C is System
 Volume Serial Number is 54DE-009F

 Directory of C:\Folder2

11.01.2014  15:21    <DIR>          .
11.01.2014  15:21    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  36.910.354.432 bytes free
```

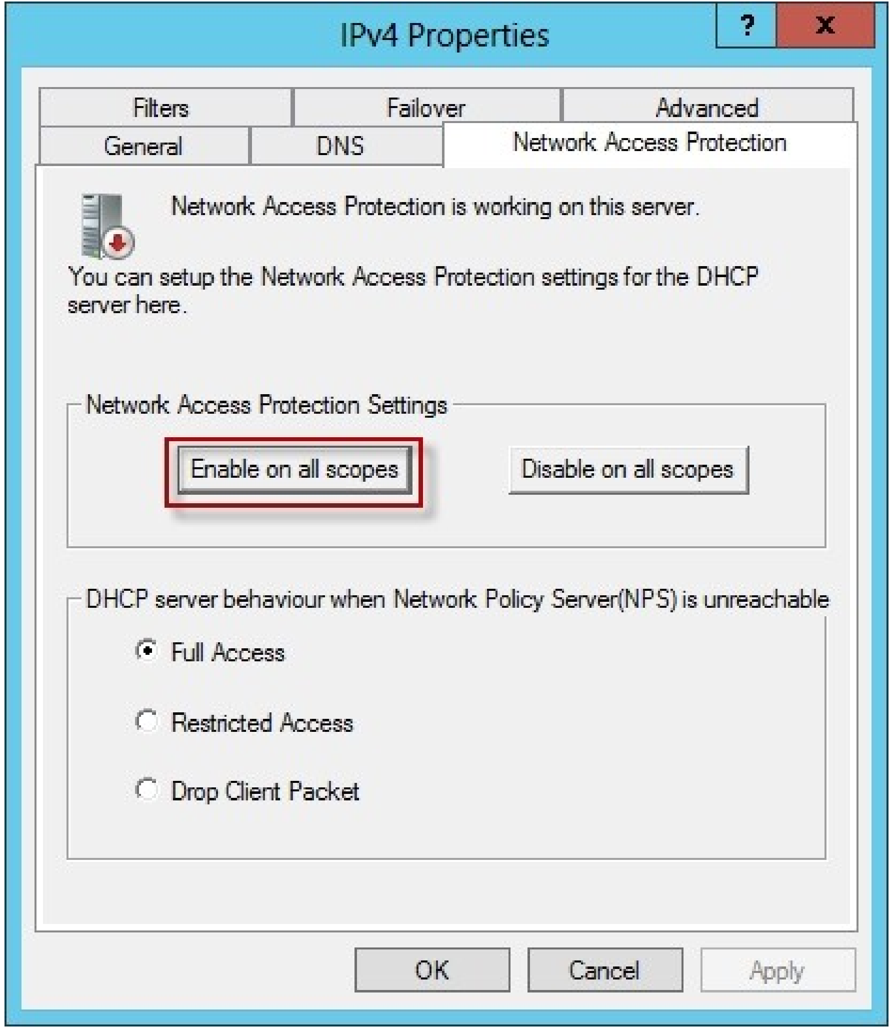
Reference: http: //technet.microsoft.com/en-us/library/cc755603(v=ws.10).aspx

NEW QUESTION 48
- (Topic 1)
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:



IPv4 Properties

Network Access Protection is working on this server.

You can setup the Network Access Protection settings for the DHCP server here.

Network Access Protection Settings

DHCP server behaviour when Network Policy Server(NPS) is unreachable

● Full Access

○ Restricted Access

○ Drop Client Packet

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 52
- (Topic 1)
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 55
- (Topic 1)
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

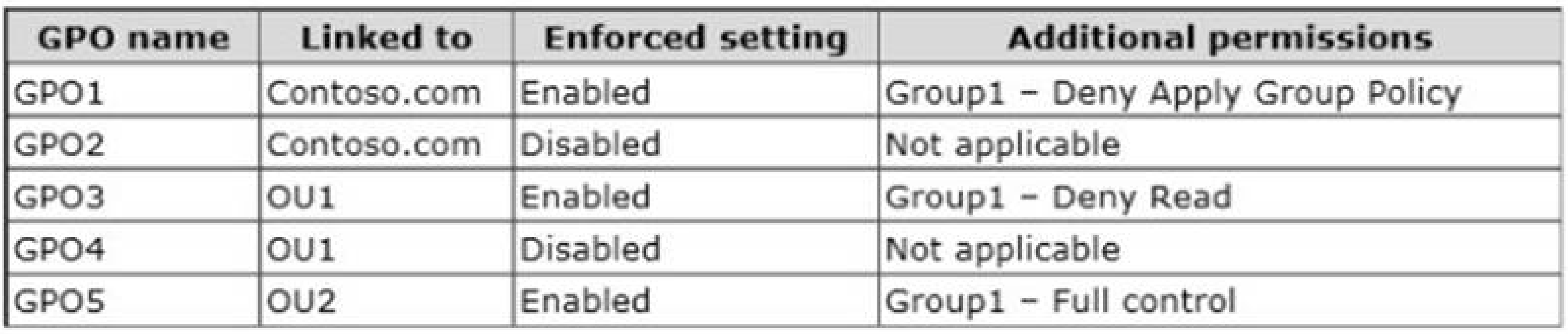
NEW QUESTION 60
- (Topic 1)
You have a DNS server named DN51 that runs Windows Server 2012 R2. On DNS1, you create a standard primary DNS zone named adatum.com.
You need to change the frequency that secondary name servers will replicate the zone from DNS1.
Which type of DNS record should you modify?

A. Name server (NS)
B. Start of authority (SOA)
C. Host information (HINFO)
D. Service location (SRV)

Answer: B

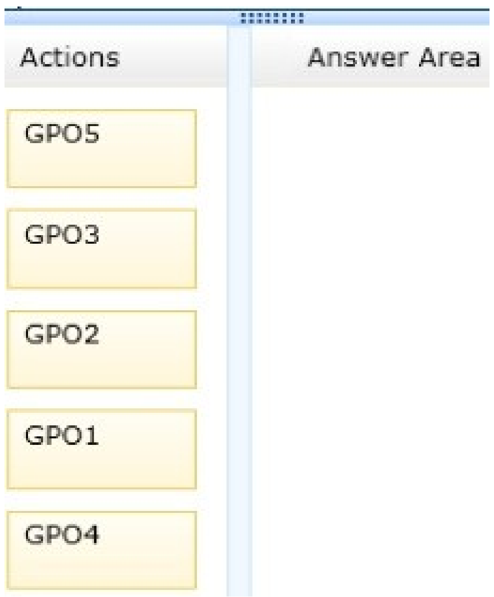
Explanation:
The time to live is specified in the Start of Authority (SOA) record
Note: TTL (time to live) - The number of seconds a domain name is cached locally before expiration and return to authoritative nameservers for updated information.

NEW QUESTION 62
DRAG DROP - (Topic 1)
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.

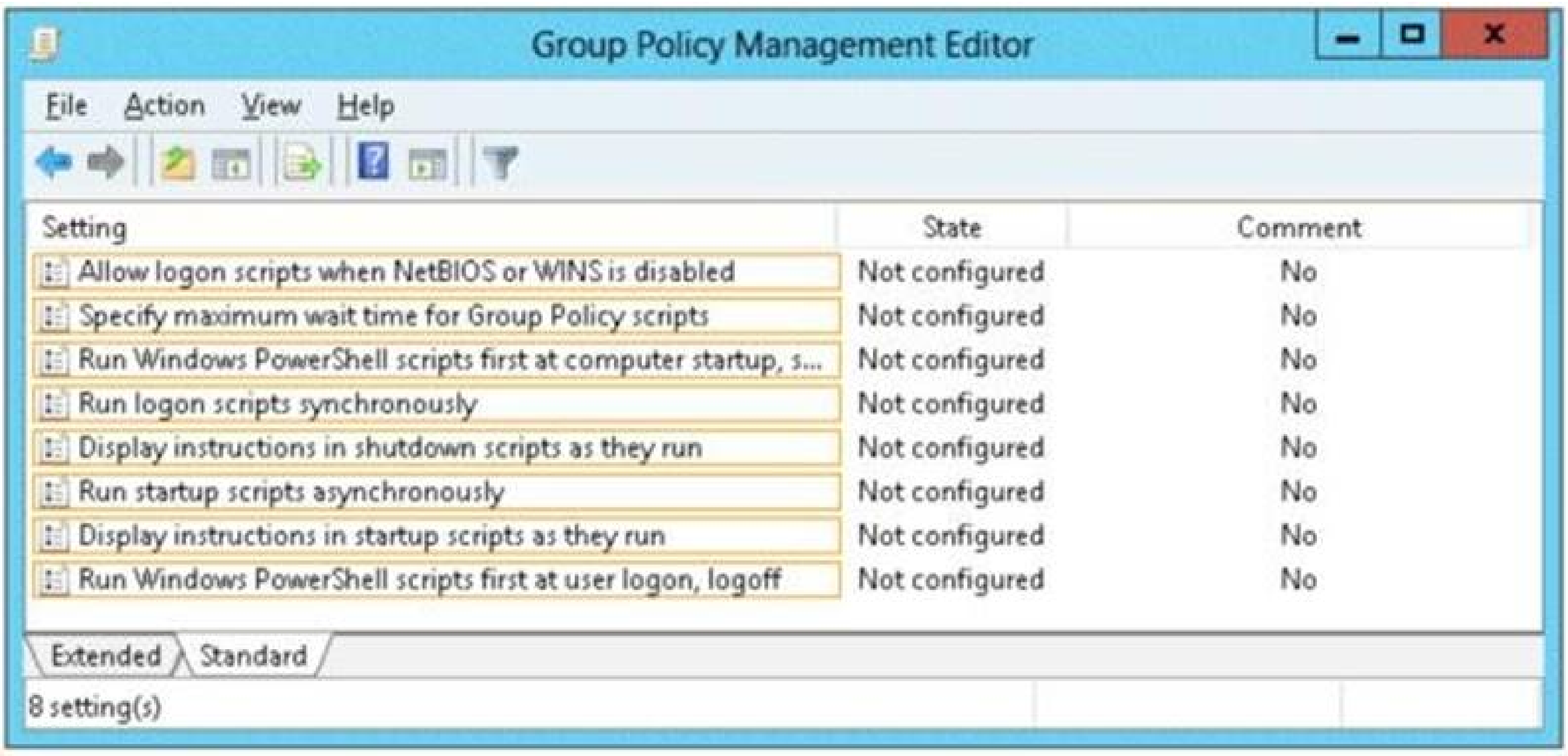


A. Mastered
B. Not Mastered

Answer: A

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 66
HOTSPOT - (Topic 1)
Your network contains an Active Directory domain named contoso.com.
You have several Windows PowerShell scripts that execute when client computers start. When a client computer starts, you discover that it takes a long time before users are
prompted to log on.
You need to reduce the amount of time it takes for the client computers to start. The solution must not prevent scripts from completing successfully.
Which setting should you configure? To answer, select the appropriate setting in the answer area.



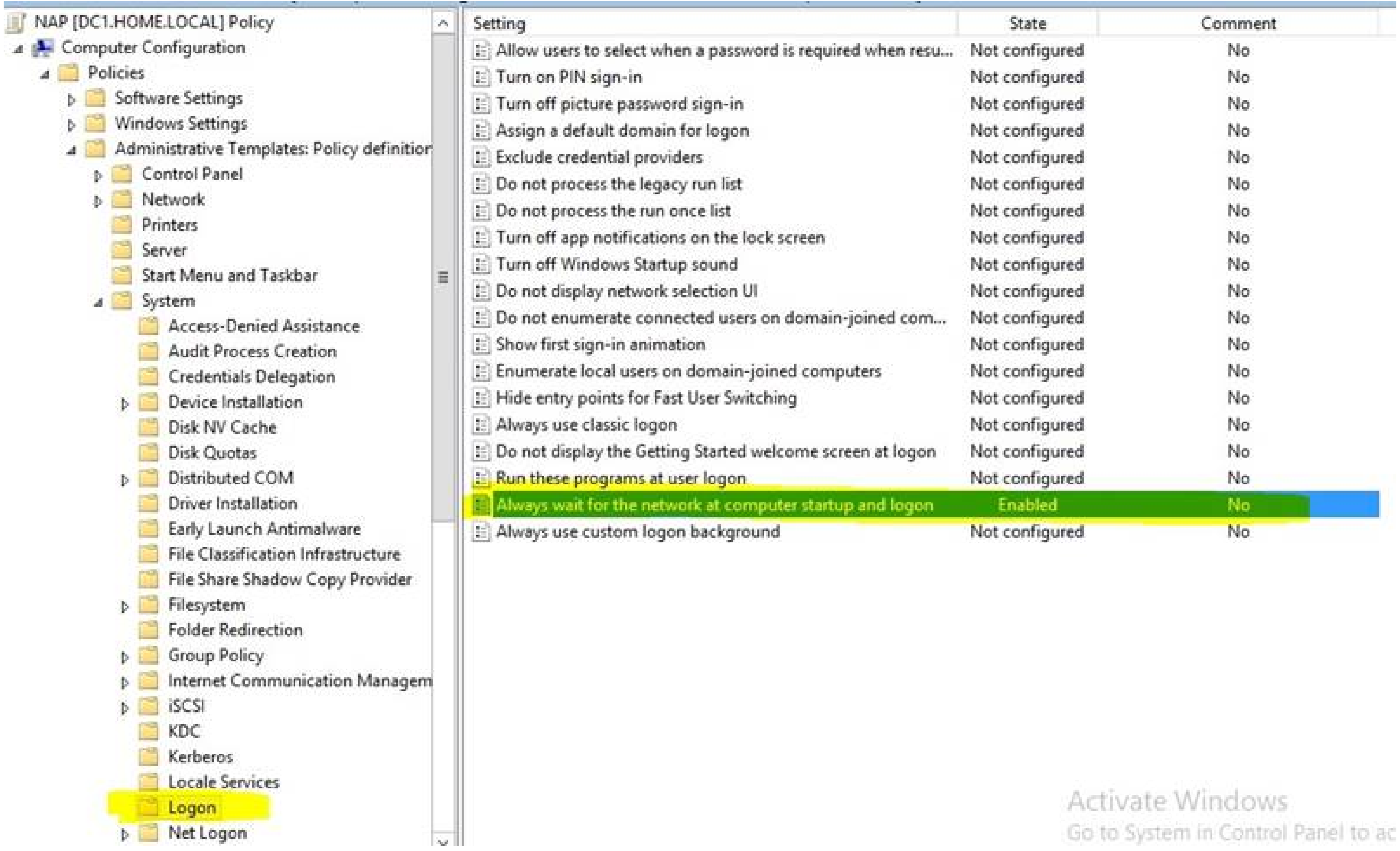
Setting	State	Comment
Allow logon scripts when NetBIOS or WINS is disabled	Not configured	No
Specify maximum wait time for Group Policy scripts	Not configured	No
Run Windows PowerShell scripts first at computer startup, s...	Not configured	No
Run logon scripts synchronously	Not configured	No
Display instructions in shutdown scripts as they run	Not configured	No
Run startup scripts asynchronously	Not configured	No
Display instructions in startup scripts as they run	Not configured	No
Run Windows PowerShell scripts first at user logon, logoff	Not configured	No

8 setting(s)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Lets the system run startup scripts simultaneously rather than waiting for each to finish http: //technet. microsoft. com/en-us/library/cc939423. aspx
Directs the system to wait for logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop.
If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.
If you disable this policy or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously.
This policy appears in the Computer Configuration and User Configuration folders. The policy set in Computer Configuration takes precedence over the policy set in User
Configuration.
By default, the Fast Logon Optimization feature is set for both domain and workgroup members. This setting causes policy to be applied asynchronously when the computer starts and the user logs on. The result is similar to a background refresh. The advantage is that it can reduce the amount of time it takes for the logon dialog box to appear and the amount of time it takes for the desktop to become available to the user. Of course, it also means that the user may log on and start working before the absolute latest policy settings have been applied to the system.
Depending on your environment, you may want to disable Fast Logon Optimization. You can do this with Group Policy, using the Always wait for the network at computer startup and logon policy setting.



Setting	State	Comment
Allow users to select when a password is required when resu...	Not configured	No
Turn on PIN sign-in	Not configured	No
Turn off picture password sign-in	Not configured	No
Assign a default domain for logon	Not configured	No
Exclude credential providers	Not configured	No
Do not process the legacy run list	Not configured	No
Do not process the run once list	Not configured	No
Turn off app notifications on the lock screen	Not configured	No
Turn off Windows Startup sound	Not configured	No
Do not display network selection UI	Not configured	No
Do not enumerate connected users on domain-joined com...	Not configured	No
Show first sign-in animation	Not configured	No
Enumerate local users on domain-joined computers	Not configured	No
Hide entry points for Fast User Switching	Not configured	No
Always use classic logon	Not configured	No
Do not display the Getting Started welcome screen at logon	Not configured	No
Run these programs at user logon	Not configured	No
Always wait for the network at computer startup and logon	Enabled	No
Always use custom logon background	Not configured	No

Refernces:
http: //technet. microsoft. com/en-us/magazine/gg486839. aspx http: //technet. microsoft. com/en-us/magazine/gg486839. aspx http: //technet. microsoft. com/en-us/library/cc958585. aspx

NEW QUESTION 71
- (Topic 1)

Your network contains an Active Directory domain named adatum.com. The domain contains a member server named Server1 and 10 web servers. All of the web servers are
in an organizational unit (OU) named WebServers_OU. All of the servers run Windows Server 2012 R2.
On Server1, you need to collect the error events from all of the web servers. The solution must ensure that when new web servers are added to WebServers_OU, their error events are collected automatically on Server1.
What should you do?

A. On Server1, create a source computer initiated subscriptio
B. From a Group Policy object (GPO), configure the Configure target Subscription Manager setting.
C. On Server1, create a source computer initiated subscriptio
D. From a Group Policy object (GPO), configure the Configure forwarder resource usage setting.
E. On Server1, create a collector initiated subscriptio
F. From a Group Policy object (GPO), configure the Configure forwarder resource usage setting.
G. On Server1, create a collector initiated subscriptio
H. From a Group Policy object (GPO), configure the Configure target Subscription Manager setting.

Answer: A

Explanation:
Source-initiated subscriptions allow you to define a subscription on an event collector computer without defining the event source computers, and then multiple remote event source computers can be set up (using a group policy setting) to forward events to the event collector computer. This differs from a collector initiated subscription because in the collector initiated subscription model, the event collector must define all the event sources in the event subscription.
1. Run the following command from an elevated privilege command prompt on the Windows Server domain controller to configure Windows Remote Management: winrm qc –q.
2. Start group policy by running the following command:
%SYSTEMROOT%\System32\gpedit. msc.
3. Under the Computer Configuration node, expand the Administrative Templates node, then expand the Windows Components node, then select the Event Forwarding node.
4. Right-click the SubscriptionManager setting, and select Properties. Enable the SubscriptionManager setting, and click the Show button to add a server address to the setting. Add at least one setting that specifies the event collector computer. The SubscriptionManager Properties window contains an Explain tab that describes the syntax for the setting.
5. After the SubscriptionManager setting has been added, run the following command to ensure the policy is applied: gpupdate /force.
If you want to configure a source computer-initiated subscription, you need to configure the following group policies on the computers that will act as the event forwarders:
* (A) Configure Target Subscription Manager This policy enables you to set the location of the collector computer.

NEW QUESTION 75
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 8.1.
The network contains a shared folder named FinancialData that contains five files.
You need to ensure that the FinancialData folder and its contents are copied to all of the client computers.
Which two Group Policy preferences should you configure? (Each correct answer presents part of the solution. Choose two.)

A. Shortcuts
B. Network Shares
C. Environment
D. Folders
E. Files

Answer: DE

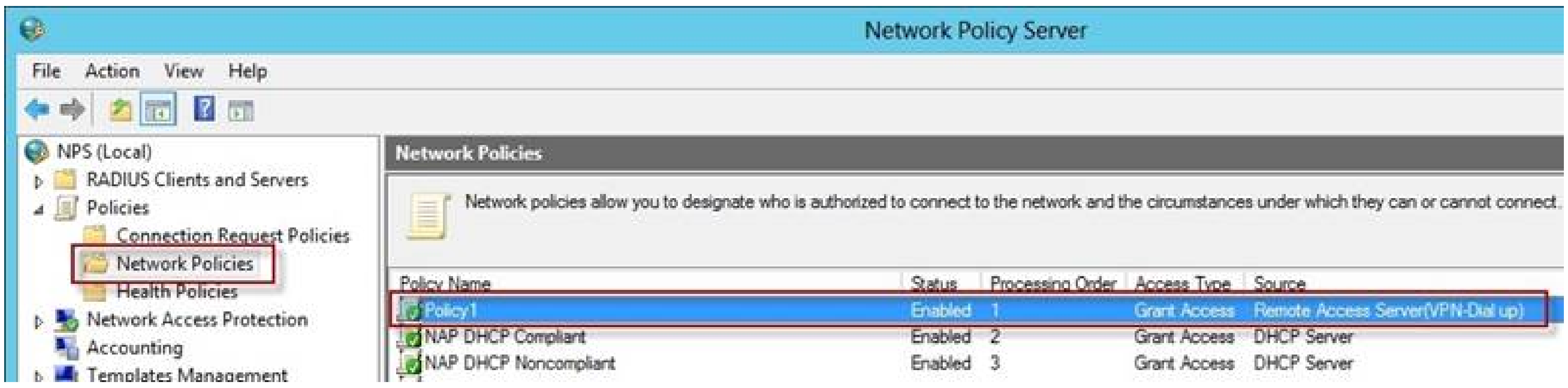
Explanation:
Folder preference items allow you to create, update, replace, and delete folders and their contents. (To configure individual files rather than folders, see Files Extension.) Before you create a Folder preference item, you should review the behavior of each type of action possible with this extension.
File preference items allow you to copy, modify the attributes of, replace, and delete files. (To configure folders rather than individual files, see Folders Extension.) Before you create a File preference item, you should review the behavior of each type of action possible with this extension.

NEW QUESTION 77
- (Topic 2)
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. Create a network policy.
B. Create a connection request policy.
C. Add a RADIUS client.
D. Modify the members of the Remote Management Users group.

Answer: A

Explanation:
Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Network policies can be viewed as rules. Each rule has a set of conditions and settings. Configure your VPN server to use Network Access Protection (NAP) to enforce health requirement policies.

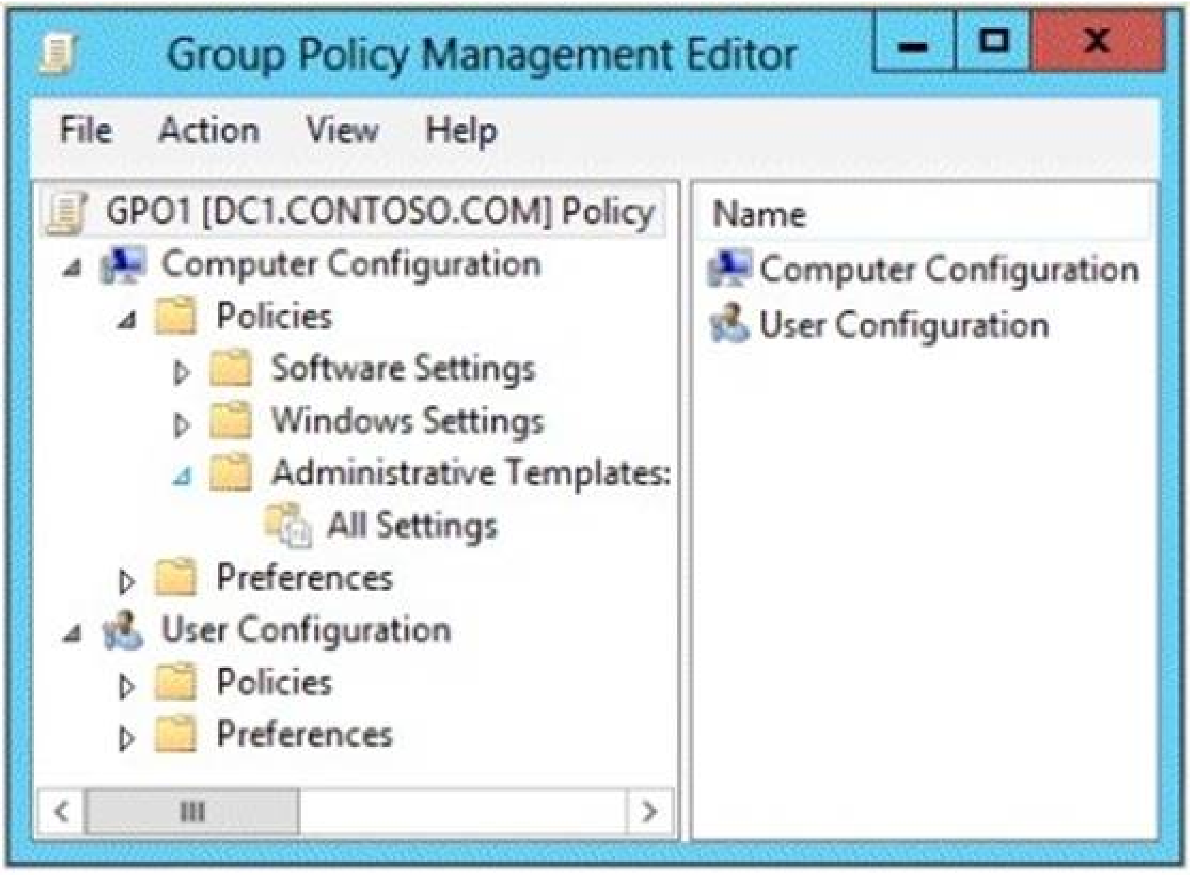


Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Policy1	Enabled	1	Grant Access	Remote Access Server(VPN-Dial up)
NAP DHCP Compliant	Enabled	2	Grant Access	DHCP Server
NAP DHCP Noncompliant	Enabled	3	Grant Access	DHCP Server

References:
http: //technet. microsoft. com/en-us/library/hh831683. aspx
http: //technet. microsoft. com/en-us/library/cc754107. aspx
http: //technet. microsoft. com/en-us/library/dd314165%28v=ws. 10%29. aspx
http: //technet. microsoft. com/en-us/windowsserver/dd448603. aspx
http: //technet. microsoft. com/en-us/library/dd314165(v=ws. 10). aspx
http: //technet. microsoft. com/en-us/library/dd469733. aspx
http: //technet. microsoft. com/en-us/library/dd469660. aspx
http: //technet. microsoft. com/en-us/library/cc753603. aspx
http: //technet. microsoft. com/en-us/library/cc754033. aspx
http: //technet. microsoft. com/en-us/windowsserver/dd448603. aspx

NEW QUESTION 82
- (Topic 2)
Your network contains an Active Directory domain named contoso.com.
A user named User1 creates a central store and opens the Group Policy Management Editor as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that the default Administrative Templates appear in GPO1. What should you do?

A. Link a WMI filter to GPO1.
B. Copy files from %Windir%\Policydefinitions to the central store.
C. Configure Security Filtering in GPO1.
D. Add User1 to the Group Policy Creator Owners group.

Answer: B

Explanation:
In earlier operating systems, all the default Administrative Template files are added to the ADM folder of a Group Policy object (GPO) on a domain controller. The GPOs are stored in the SYSVOL folder. The SYSVOL folder is automatically replicated to other domain controllers in the same domain. A policy file uses approximately 2 megabytes (MB) of hard disk space. Because each domain controller stores a distinct version of a policy, replication traffic is increased.
In Group Policy for Windows Server 2008 and Windows Vista, if you change Administrative template policy settings on local computers, Sysvol will not be automatically updated with the new .admX or .admL files. This change in behavior is implemented to reduce network load and disk storage requirements, and to prevent conflicts between .admX files and.admL files when edits to Administrative template policy settings are made across different locales. To make sure that any local updates are reflected in Sysvol, you must manually copy the updated .admX or .admL files from the PolicyDefinitions file on the local computer to the Sysvol\PolicyDefinitions folder on the appropriate domain controller.
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.
To create a Central Store for .admx and .adml files, create a folder that is named PolicyDefinitions in the following location:
\\FQDN\SYSVOL\FQDN\policies
Reference:
http: //support. microsoft. com/kb/929841

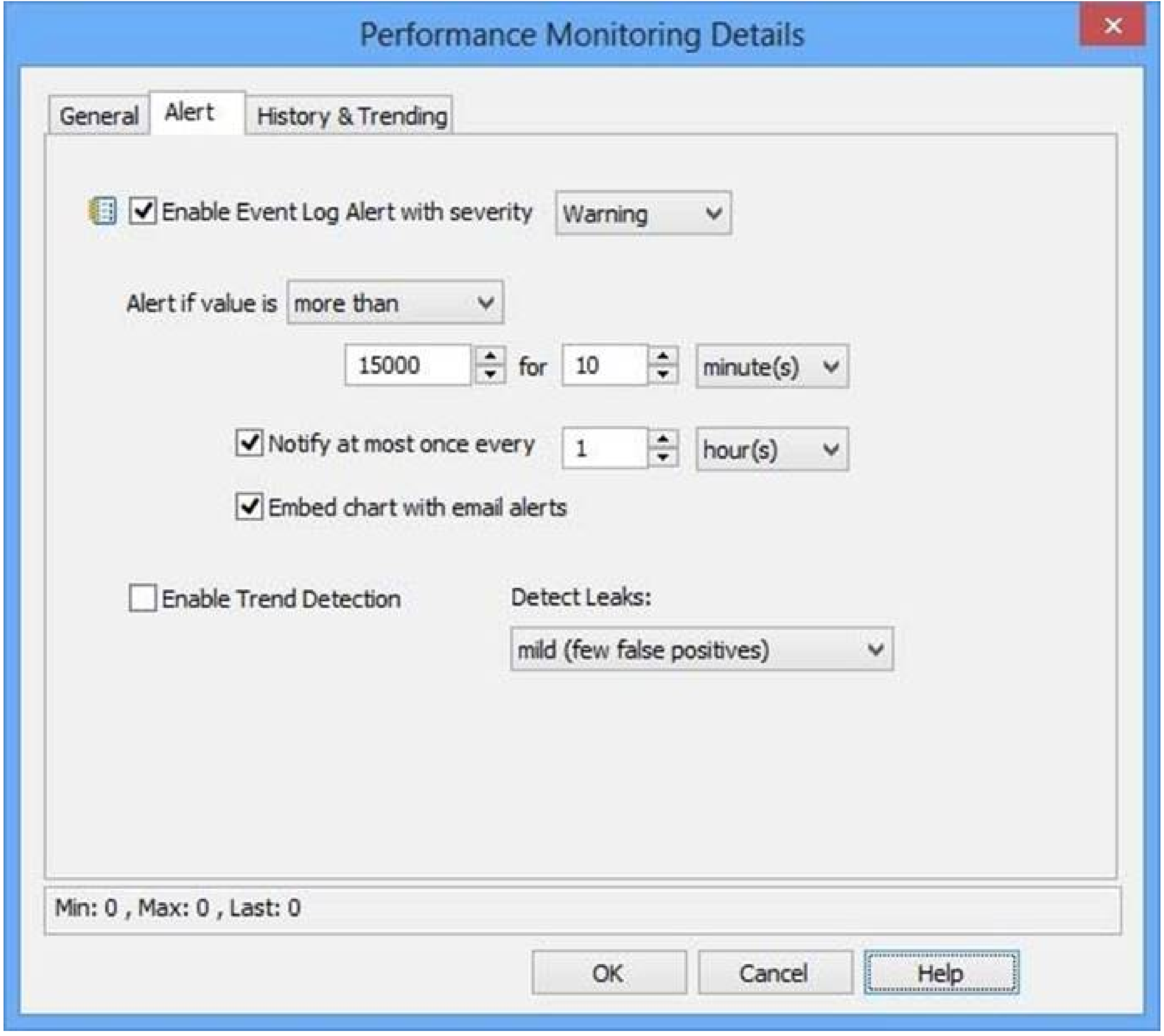
NEW QUESTION 83

- (Topic 2)
You have a server named Server1 that runs Windows Server 2012 R2.
You need to configure Server1 to create an entry in an event log when the processor usage exceeds 60 percent.
Which type of data collector should you create?

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

Answer: B

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.


Performance Monitoring Details

☑ Enable Event Log Alert with severity: Warning

Alert if value is: more than

15000 for 10 minute(s)

☑ Notify at most once every 1 hour(s)

☑ Embed chart with email alerts

□ Enable Trend Detection

Detect Leaks: mild (few false positives)

Min: 0 , Max: 0 , Last: 0

NEW QUESTION 84
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the Network Policy Server role service installed.
You need to enable trace logging for Network Policy Server (NPS) on Server1. Which tool should you use?

A. The tracert.exe command
B. The Network Policy Server console
C. The Server Manager console
D. The netsh.exe command

Answer: D

Explanation:
NPS trace logging files
You can use log files on servers running Network Policy Server (NPS) and NAP client computers to help troubleshoot NAP problems. Log files can provide the detailed information required for troubleshooting complex problems.
You can capture detailed information in log files on servers running NPS by enabling remote access tracing. The Remote Access service does not need to be installed or running to use remote access tracing. When you enable tracing on a server running NPS, several log files are created in %windir%\tracing.
The following log files contain helpful information about NAP:
IASNAP. LOG: Contains detailed information about NAP processes, NPS authentication, and NPS authorization.
IASSAM. LOG: Contains detailed information about user authentication and authorization.
Membership in the local Administrators group, or equivalent, is the minimum required to enable tracing. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups (http: //go. microsoft. com/fwlink/?LinkId=83477).
To create tracing log files on a server running NPS
? Open a command line as an administrator.

? Type netshras set tr * en.
? Reproduce the scenario that you are troubleshooting.
? Type netshras set tr * dis.
? Close the command prompt window.
Reference: http: //technet. microsoft. com/en-us/library/dd348461%28v=ws. 10%29. aspx

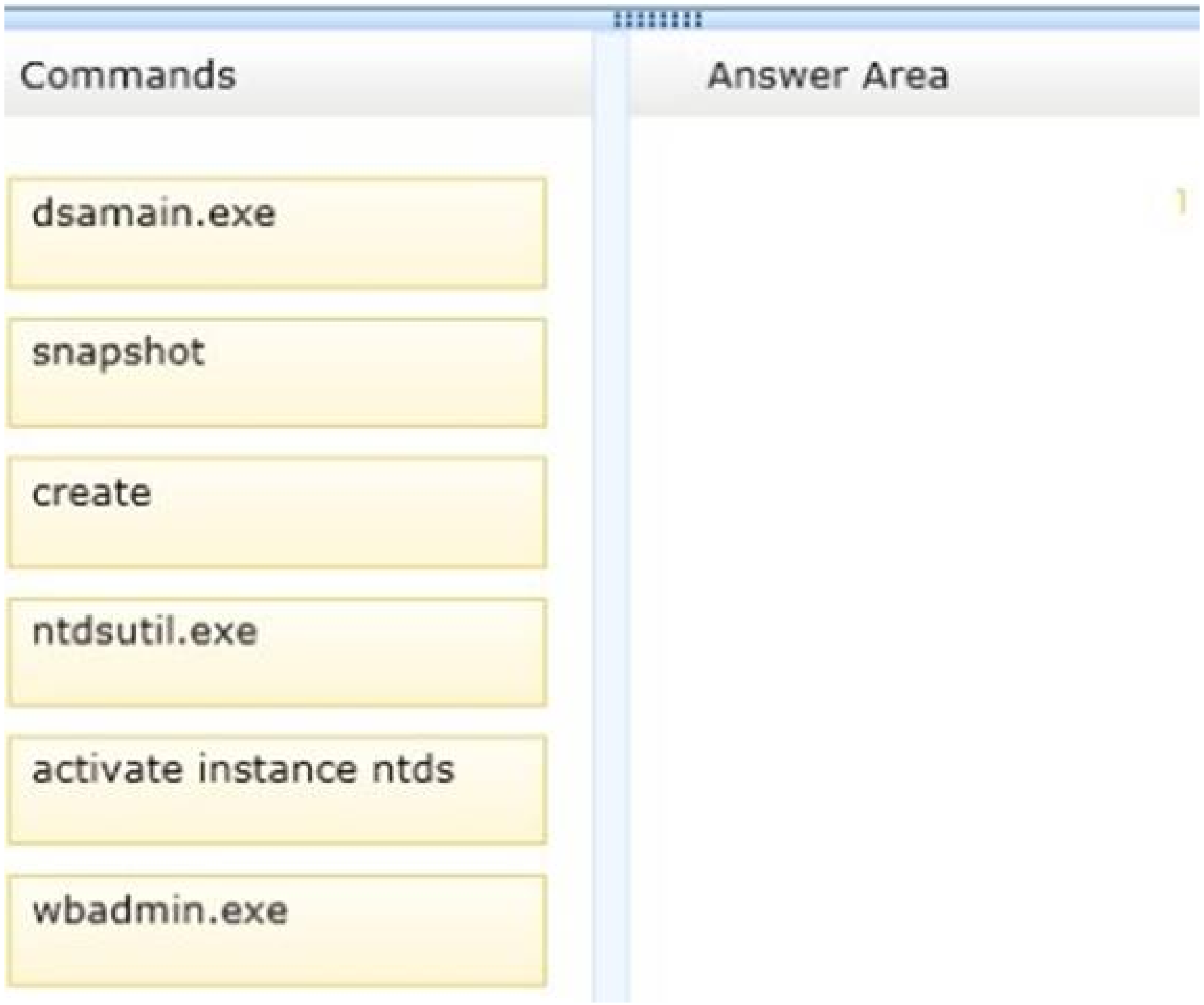
NEW QUESTION 86
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2.
You have a Password Settings object (PSOs) named PSO1.
You need to view the settings of PSO1. Which tool should you use?

A. Get-ADDefaultDomainPasswordPolicy
B. Active Directory Administrative Center
C. Local Security Policy
D. Get-ADAccountResultantPasswordReplicationPolicy

Answer: B

Explanation:
In Windows Server 2012, fine-grained password policy management is made much easier than Windows Server 2008/2008 R2. Windows Administrators not have to use ADSI Edit and configure complicated settings to create the Password Settings Object (PSO) in the Password Settings Container. Instead we can configure fine-grained password policy directly in Active Directory Administrative Center (ADAC).

NEW QUESTION 89
DRAG DROP - (Topic 2)
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1.
You need to create an Active Directory snapshot on DC1. Which four commands should you run?
To answer, move the four appropriate commands from the list of commands to the answer area and arrange them in the correct order.



Commands

Answer Area

dsamain.exe

snapshot

create

ntdsutil.exe

activate instance ntds

wbadmin.exe

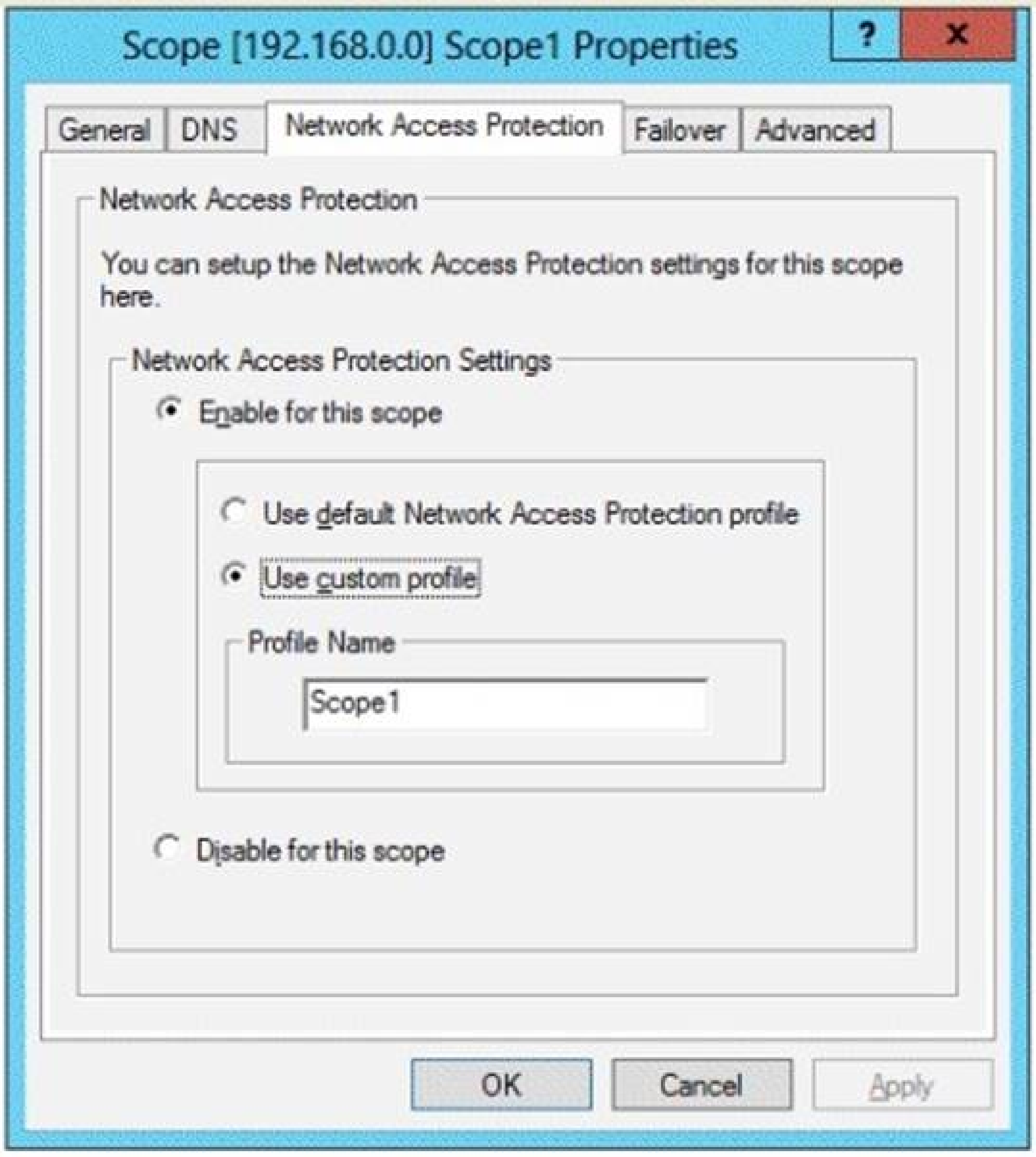
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: ntdsutil
Box 2: snapshot
Box 3: activate instance ntds Box 4: create
Note:
Create a snapshot of AD DS in Windows Server 2012 R2 by using NTDSUTIL
1 – On the domain server, open command prompt and type ntdsutil and press Enter. 2- Next, type snapshot and press Enter.
3 – Next, type activate instance ntds and press Enter.
4 – Next, type create (this create command is to generate a snapshot of my AD) and press Enter.

NEW QUESTION 92
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 has the DHCP Server server role

and the Network Policy Server role service installed.
Server1 contains three non-overlapping scopes named Scope1, Scope2, and Scope3. Server1 currently provides the same Network Access Protection (NAP) settings to the three scopes.
You modify the settings of Scope1 as shown in the exhibit. (Click the Exhibit button.)



Scope [192.168.0.0] Scope1 Properties

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

Scope1

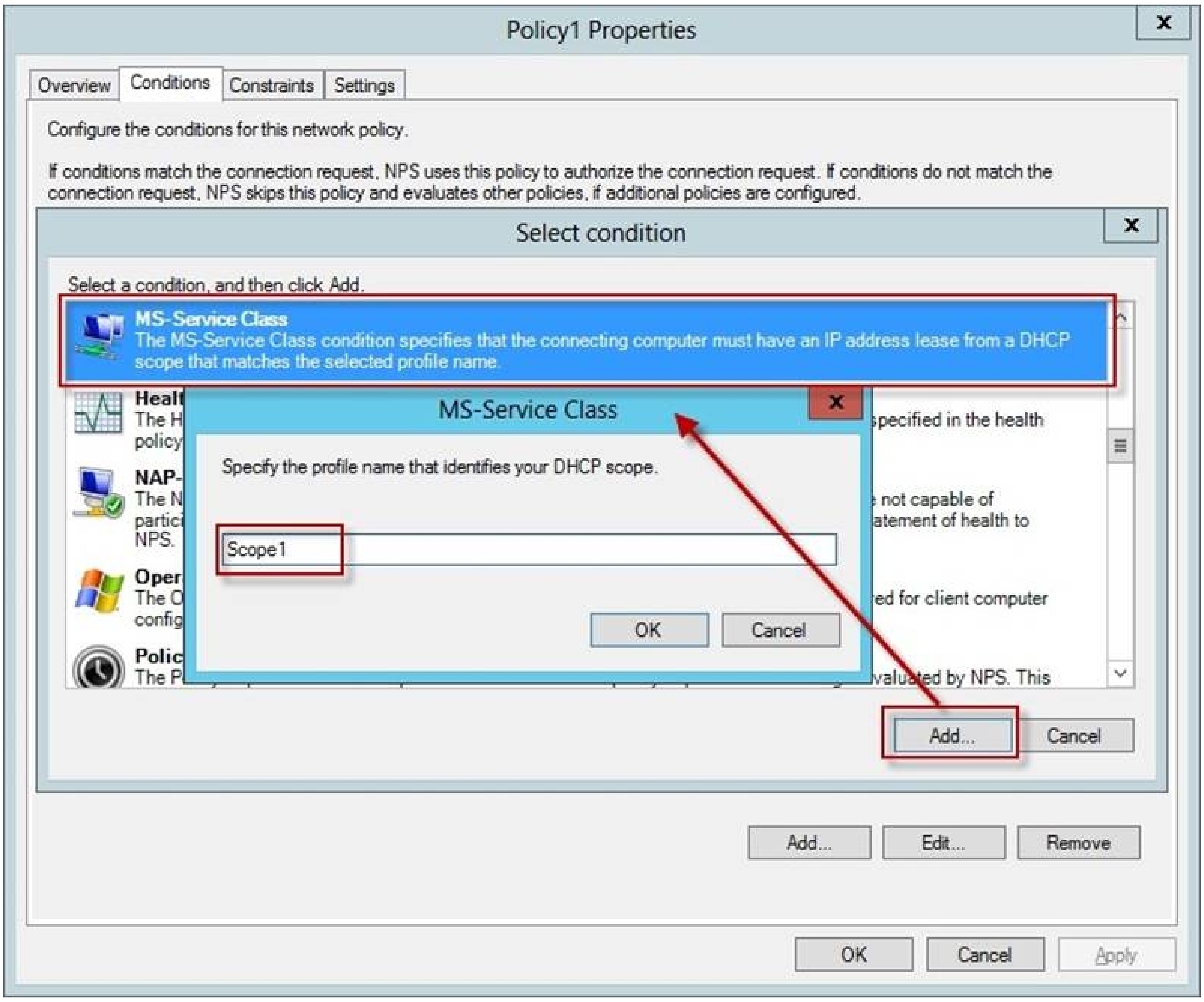
○ Disable for this scope

You need to configure Server1 to provide unique NAP enforcement settings to the NAP non-compliant DHCP clients from Scope1.
What should you create?

A. A connection request policy that has the Service Type condition
B. A connection request policy that has the Identity Type condition
C. A network policy that has the Identity Type condition
D. A network policy that has the MS-Service Class condition

Answer: D

Explanation:
MS-Service Class
Restricts the policy to clients that have received an IP address from a DHCP scope that matches the specified DHCP profile name. This condition is used only when you are deploying NAP with the DHCP enforcement method. To use the MS-Service Class attribute, in Specify the profile name that identifies your DHCP scope, type the name of an existing DHCP profile.
Open the NPS console, double-click Policies, click Network Policies, and then double-click the policy you want to configure.
In policy Properties, click the Conditions tab, and then click Add. In Select condition, scroll to the Network Access Protection group of conditions.
If you want to configure the Identity Type condition, click Identity Type, and then click Add. In Specify the method in which clients are identified in this policy, select the items appropriate for your deployment, and then click OK.
The Identity Type condition is used for the DHCP and Internet Protocol security (IPsec) enforcement methods to allow client health checks when NPS does not receive an Access- Request message that contains a value for the User-Name attribute; in this case, client health checks are performed, but authentication and authorization are not performed.
If you want to configure the MS-Service Class condition, click MS-Service Class, and then click Add. In Specify the profile name that identifies your DHCP scope, type the name of an existing DHCP profile, and then click Add.



Policy1 Properties

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Select condition

Select a condition, and then click Add.

MS-Service Class
The MS-Service Class condition specifies that the connecting computer must have an IP address lease from a DHCP scope that matches the selected profile name.

MS-Service Class

Specify the profile name that identifies your DHCP scope.

Scope1

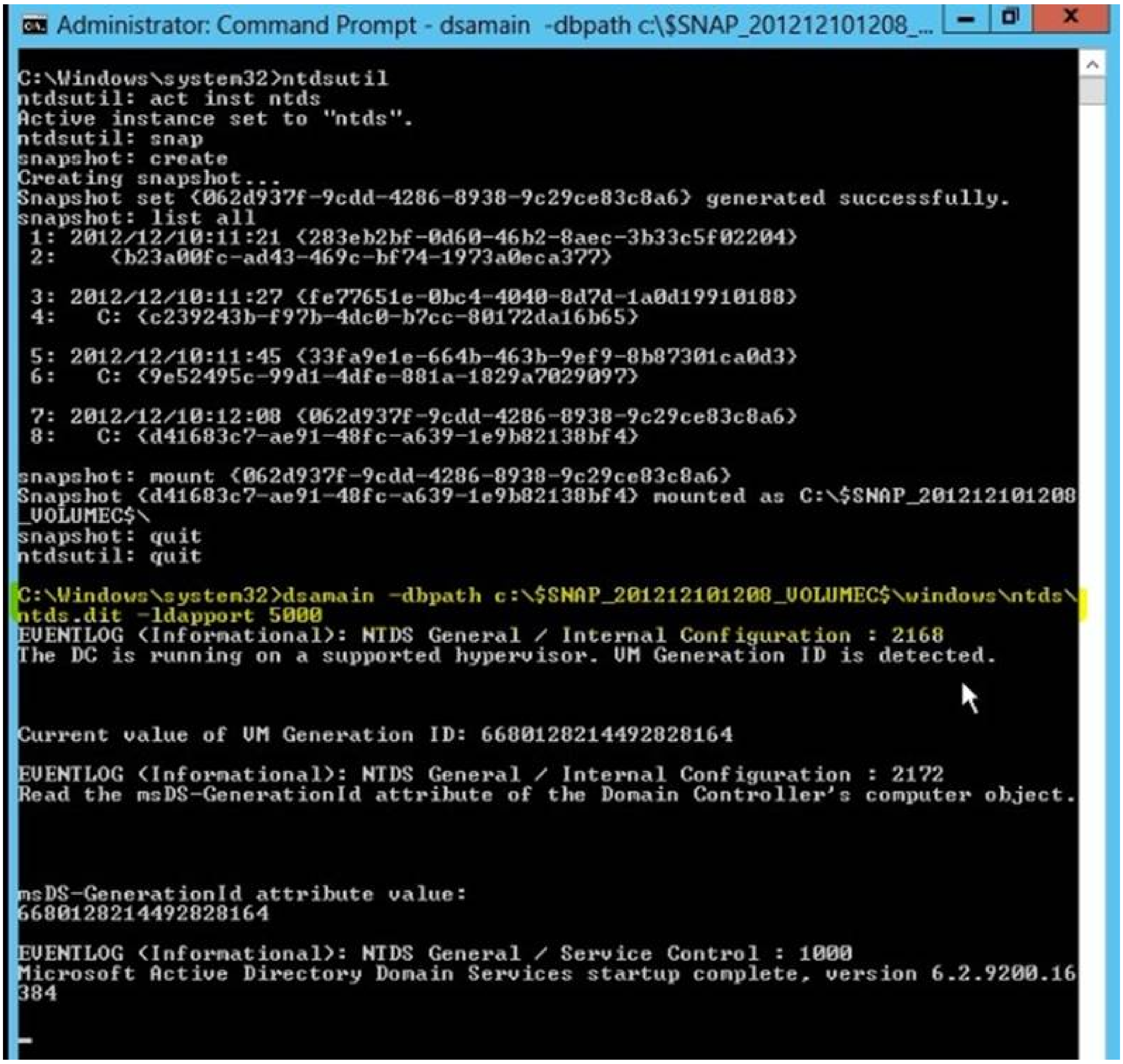
The MS-Service Class condition restricts the policy to clients that have received an IP address from a DHCP scope that matches the specified DHCP profile name. This condition is used only when you are deploying NAP with the DHCP enforcement method.
References:
http: //technet. microsoft. com/en-us/library/cc731560(v=ws. 10). aspx
http: //technet. microsoft. com/en-us/library/cc731220(v=ws. 10). aspx

NEW QUESTION 95
- (Topic 2)
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



Administrator: Command Prompt - dsamain -dbpath c:\$SNAP_201212101208_...

```
C:\Windows\system32>ntdsutil
ntdsutil: act inst ntds
Active instance set to "ntds".
ntdsutil: snap
snapshot: create
Creating snapshot...
Snapshot set {062d937f-9cdd-4286-8938-9c29ce83c8a6} generated successfully.
snapshot: list all
 1: 2012/12/10:11:21 {283eb2bf-0d60-46b2-8aec-3b33c5f02204}
 2:     {b23a00fc-ad43-469c-bf74-1973a0eca377}

 3: 2012/12/10:11:27 {fe77651e-0bc4-4040-8d7d-1a0d19910188}
 4:    C: {c239243b-f97b-4dc0-b7cc-80172da16b65}

 5: 2012/12/10:11:45 {33fa9e1e-664b-463b-9ef9-8b87301ca0d3}
 6:    C: {9e52495c-99d1-4dfe-881a-1829a7029097}

 7: 2012/12/10:12:08 {062d937f-9cdd-4286-8938-9c29ce83c8a6}
 8:    C: {d41683c7-ae91-48fc-a639-1e9b82138bf4}

snapshot: mount {062d937f-9cdd-4286-8938-9c29ce83c8a6}
Snapshot {d41683c7-ae91-48fc-a639-1e9b82138bf4} mounted as C:\$SNAP_201212101208
_VOLUMEC$\
snapshot: quit
ntdsutil: quit

C:\Windows\system32>dsamain -dbpath c:\$SNAP_201212101208_VOLUMEC$\windows\ntds\
ntds.dit -ldapport 5000
EVENTLOG (Informational): NTDS General / Internal Configuration : 2168
The DC is running on a supported hypervisor. VM Generation ID is detected.


Current value of VM Generation ID: 6680128214492828164

EVENTLOG (Informational): NTDS General / Internal Configuration : 2172
Read the msDS-GenerationId attribute of the Domain Controller's computer object.



msDS-GenerationId attribute value:
6680128214492828164

EVENTLOG (Informational): NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete, version 6.2.9200.16
384

_
```

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

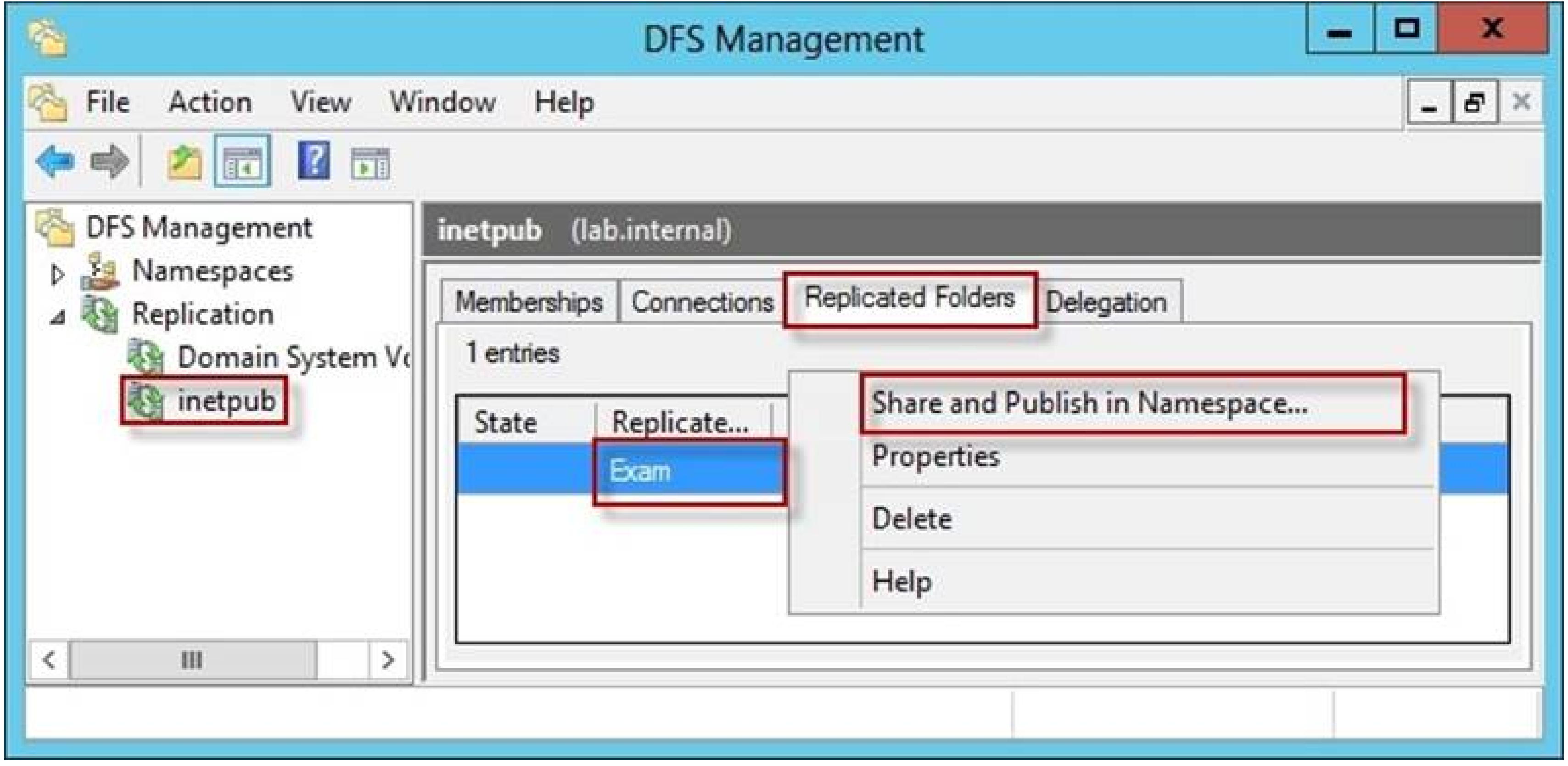
NEW QUESTION 97
- (Topic 2)
Your company has a main office and a branch office. The main office is located in Seattle. The branch office is located in Montreal. Each office is configured as an Active Directory site.
The network contains an Active Directory domain named adatum.com. The Seattle office 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.

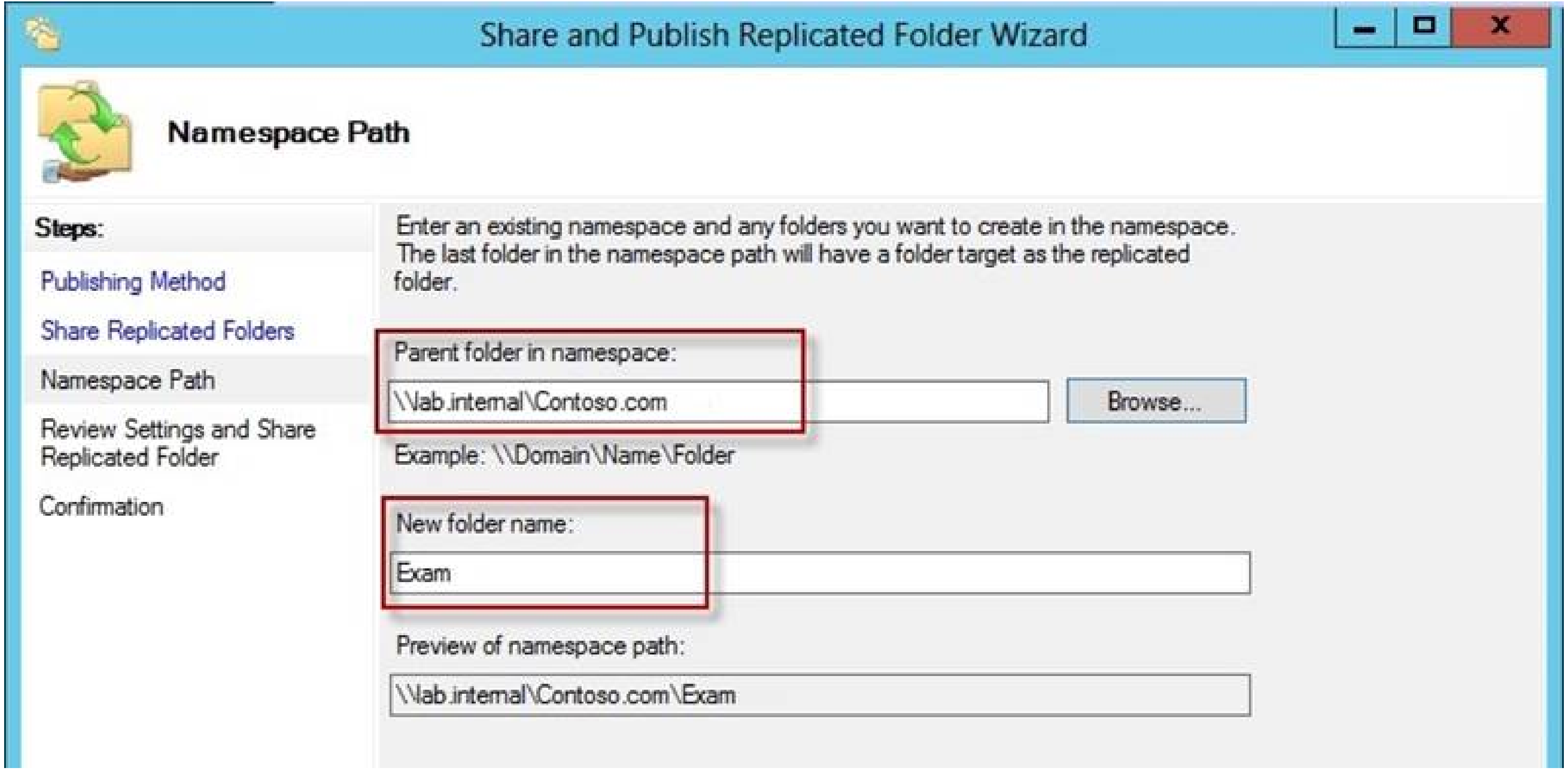
Answer: BCE

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."



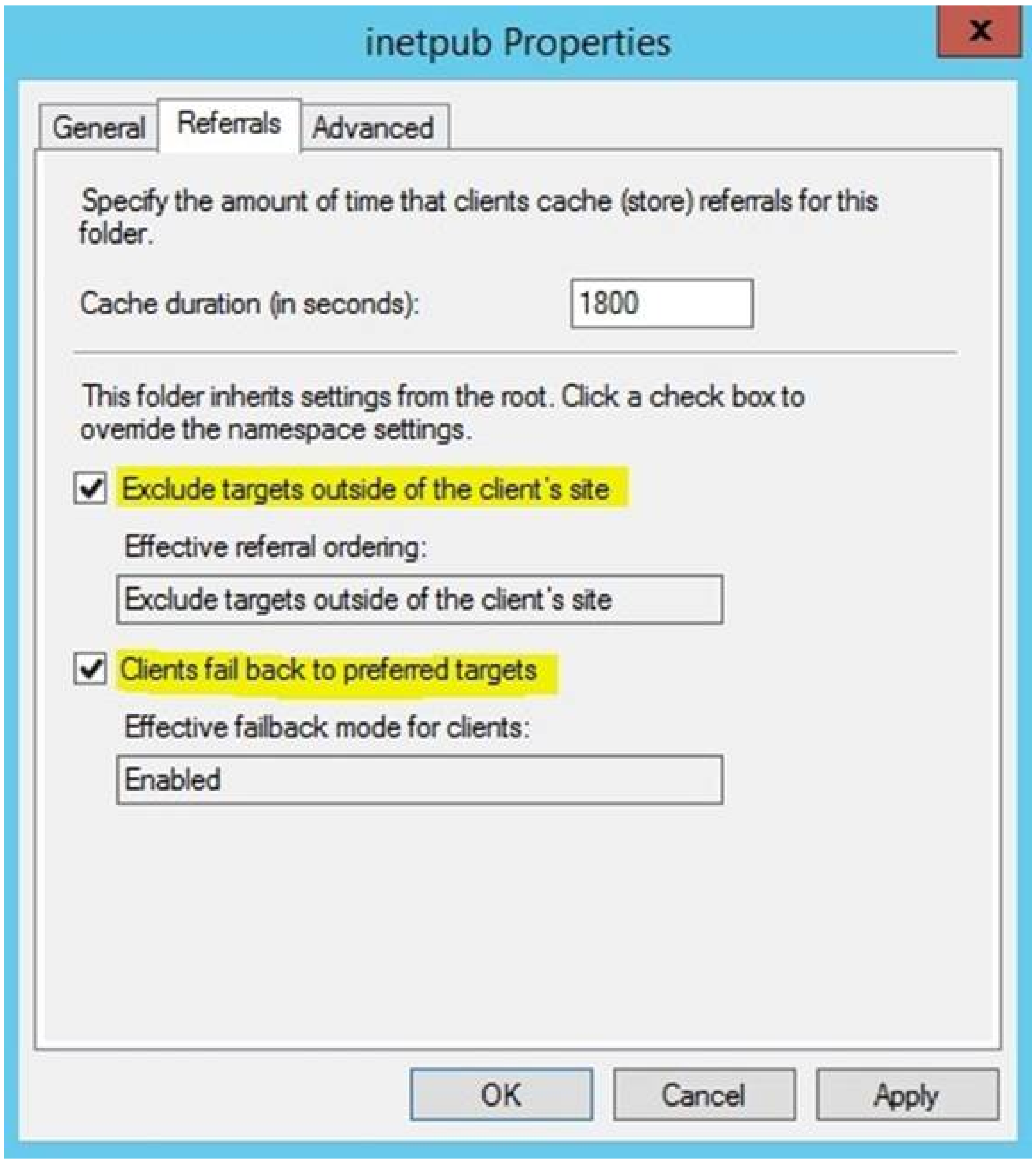
Enter an existing namespace and any folders you want to create in the namespace. The last folder in the namespace path will have a folder target as the replicated folder.

Parent folder in namespace:
\\lab.internal\Contoso.com

Example: \\Domain\Name\Folder

New folder name:
Exam

Preview of namespace path:
\\lab.internal\Contoso.com\Exam



Specify the amount of time that clients cache (store) referrals for this folder.

Cache duration (in seconds): 1800

This folder inherits settings from the root. Click a check box to override the namespace settings.

☑ Exclude targets outside of the client's site

Effective referral ordering:

Exclude targets outside of the client's site

☑ Clients fail back to preferred targets

Effective failback mode for clients:

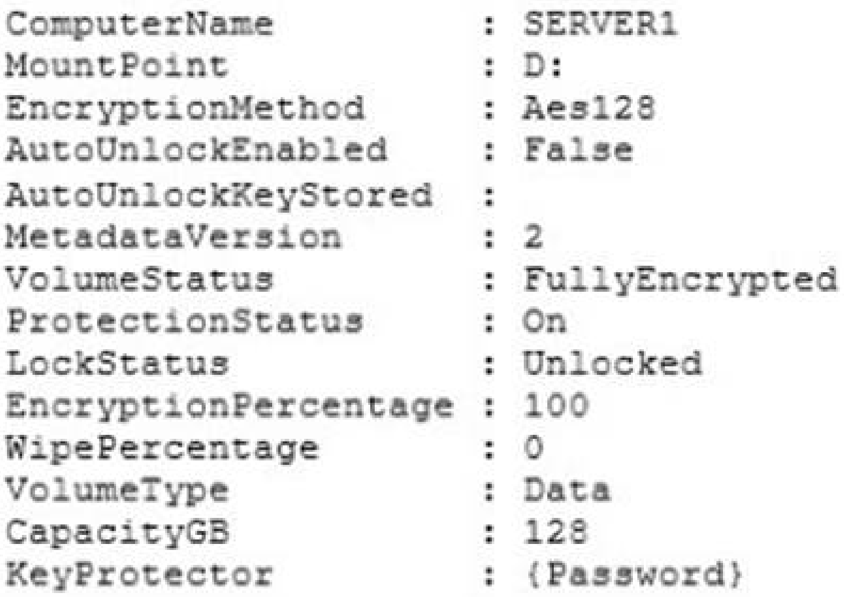
Enabled

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 101

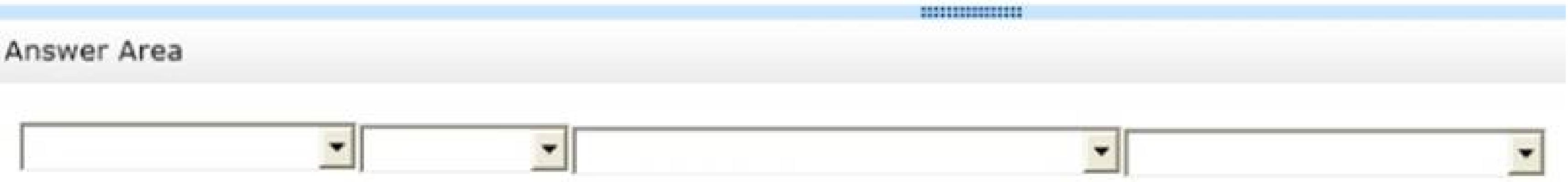
HOTSPOT - (Topic 2)

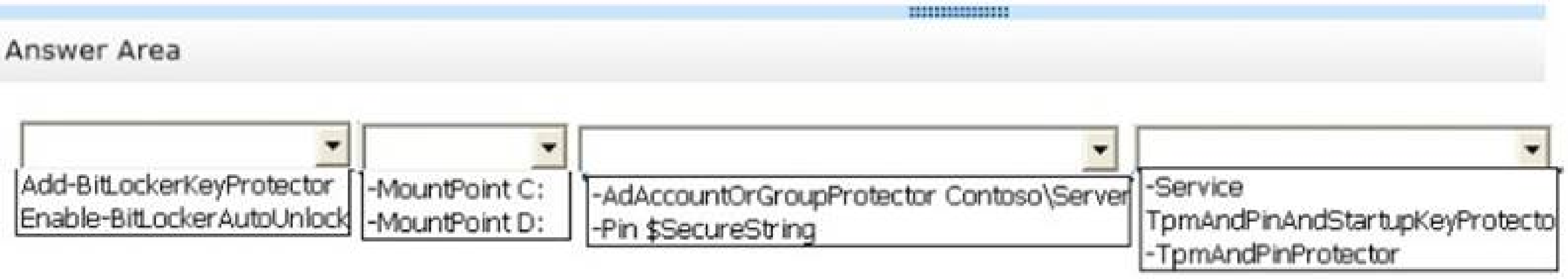
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the following BitLocker Drive Encryption (BitLocker) settings:



```
ComputerName         : SERVER1
MountPoint           : D:
EncryptionMethod     : Aes128
AutoUnlockEnabled    : False
AutoUnlockKeyStored  :
MetadataVersion      : 2
VolumeStatus         : FullyEncrypted
ProtectionStatus     : On
LockStatus           : Unlocked
EncryptionPercentage : 100
WipePercentage       : 0
VolumeType           : Data
CapacityGB           : 128
KeyProtector         : {Password}
```

You need to ensure that drive D will unlock automatically when Server1 restarts. What command should you run? To answer, select the appropriate options in the answer area.





Answer Area

Add-BitLockerKeyProtector
Enable-BitLockerAutoUnlock

-MountPoint C:
-MountPoint D:

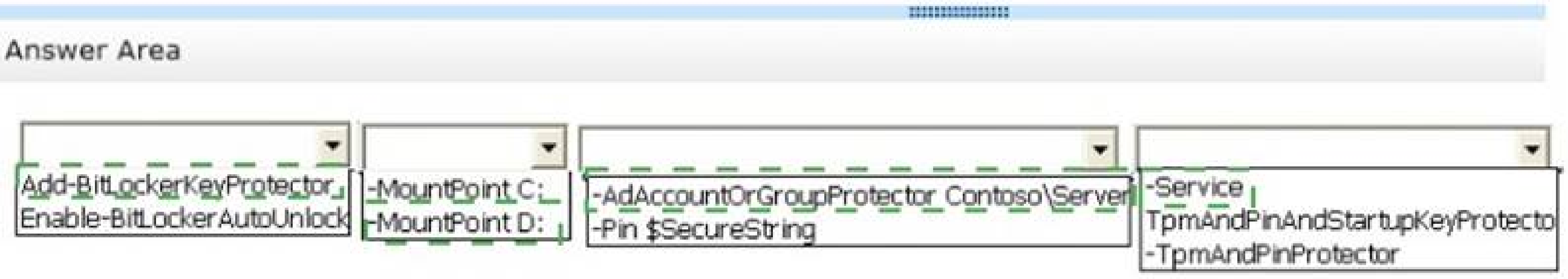
-AdAccountOrGroupProtector Contoso\Server
-Pin $SecureString

-Service
TpmAndPinAndStartupKeyProtecto
-TpmAndPinProtector

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Add-BitLockerKeyProtector
Enable-BitLockerAutoUnlock

-MountPoint C:
-MountPoint D:

-AdAccountOrGroupProtector Contoso\Server
-Pin $SecureString

-Service
TpmAndPinAndStartupKeyProtecto
-TpmAndPinProtector

NEW QUESTION 106

- (Topic 2)

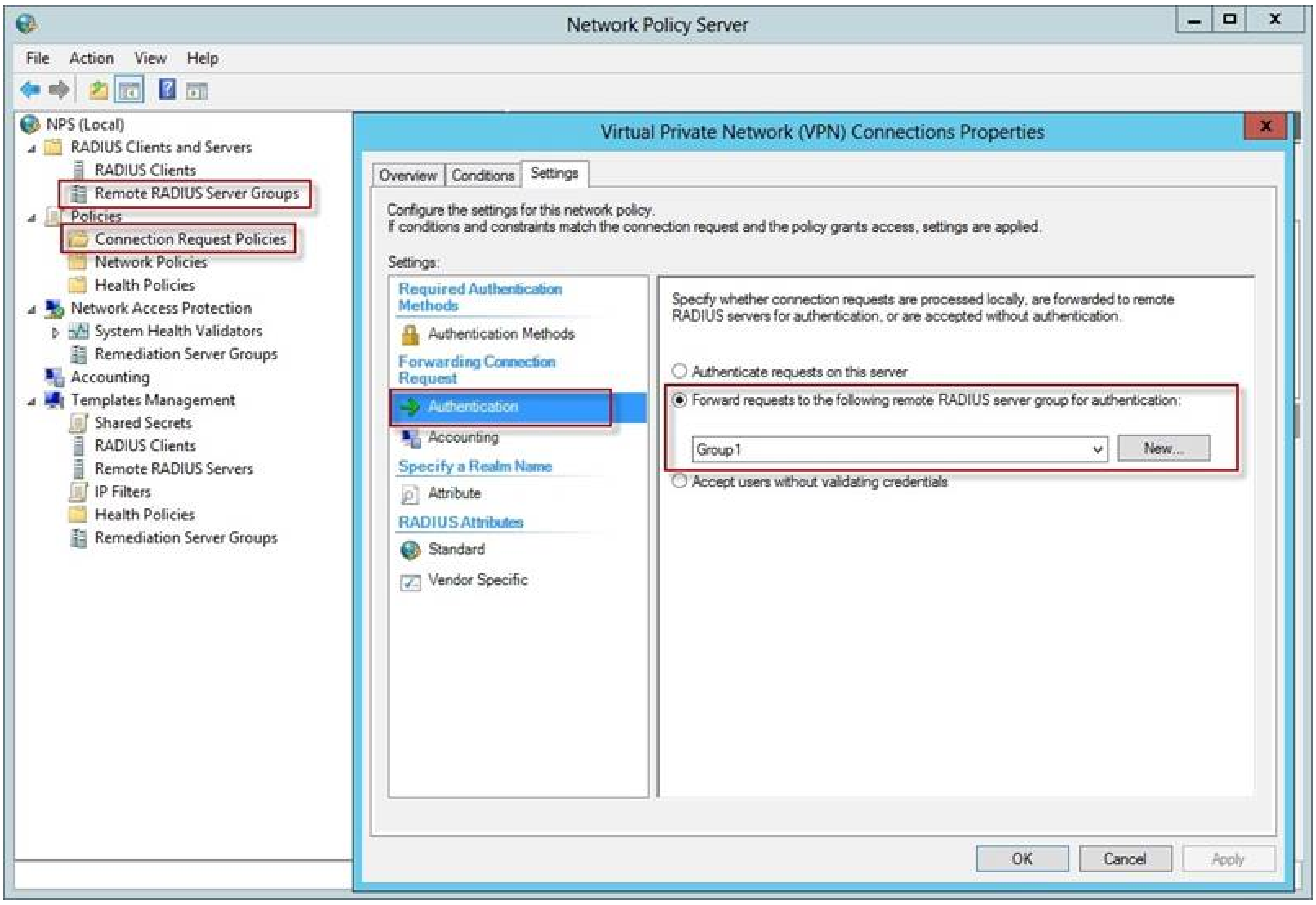
Your network contains two Active Directory forests named contoso.com and adatum.com. The contoso.com forest contains a server named Server1.contoso.com.
The adatum.com forest contains a server named server2. adatum.com. Both servers have the Network Policy Server role service installed.
The network contains a server named Server3. Server3 is located in the perimeter network and has the Network Policy Server role service installed.
You plan to configure Server3 as an authentication provider for several VPN servers. You need to ensure that RADIUS requests received by Server3 for a specific VPN server
are always forwarded to Server1.contoso.com.
Which two should you configure on Server3? (Each correct answer presents part of the solution. Choose two.)

A. Remediation server groups
B. Remote RADIUS server groups
C. Connection request policies
D. Network policies
E. Connection authorization policies

Answer: BC

Explanation:

To configure NPS as a RADIUS proxy, you must create a connection request policy that contains all of the information required for NPS to evaluate which messages to forward and where to send the messages.
When you configure Network Policy Server (NPS) as a Remote Authentication Dial-In User Service (RADIUS) proxy, you use NPS to forward connection requests to RADIUS servers that are capable of processing the connection requests because they can perform authentication and authorization in the domain where the user or computer account is located. For example, if you want to forward connection requests to one or more RADIUS servers in untrusted domains, you can configure NPS as a RADIUS proxy to forward the requests to the remote RADIUS servers in the untrusted domain. To configure NPS as a RADIUS proxy, you must create a connection request policy that contains all of the information required for NPS to evaluate which messages to forward and where to send the messages.
When you configure a remote RADIUS server group in NPS and you configure a connection request policy with the group, you are designating the location where NPS is to forward connection requests.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

○ Authenticate requests on this server

● Forward requests to the following remote RADIUS server group for authentication:

Group1

○ Accept users without validating credentials

References:
http: //technet. microsoft. com/en-us/library/cc754518. aspx
http: //technet. microsoft. com/en-us/library/cc754518. aspx
http: //technet. microsoft. com/en-us/library/cc754518. aspx

NEW QUESTION 110
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.
The network contains several group Managed Service Accounts that are used by four member servers.
You need to ensure that if a group Managed Service Account resets a password of a domain user account, an audit entry is created.
You create a Group Policy object (GPO) named GPO1. What should you do next?

A. In GPO1, configure the Advanced Audit Policy Configuration settings for Audit User Account Managemen
B. Link GPO1 to the Domain Controllers organizational unit (OU).
C. In GPO1, configure the Advanced Audit Policy Configuration settings for Audit User Account Managemen
D. Move the member servers to a new organizational unit (OU). Link GPO1 to the new OU.
E. In GPO1, configure the Advanced Audit Policy Configuration settings for Audit Sensitive Privilege Us
F. Link GPO1 to the Domain Controllers organizational unit (OU).
G. In GPO1, configure the Advanced Audit Policy Configuration settings for Audit Sensitive Privilege Us
H. Move the member servers to a new organizational unit (OU). Link GPO1 to the new OU.

Answer: A

Explanation:
Audit User Account Management
This security policy setting determines whether the operating system generates audit events when the following user account management tasks are performed:
? A user account is created, changed, deleted, renamed, disabled, enabled, locked out, or unlocked.
? A user account password is set or changed.
? Security identifier (SID) history is added to a user account.
? The Directory Services Restore Mode password is set.
? Permissions on accounts that are members of administrators groups are changed.
? Credential Manager credentials are backed up or restored.
This policy setting is essential for tracking events that involve provisioning and managing user accounts.

NEW QUESTION 115
- (Topic 2)
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 120
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2003, Windows Server 2008 R2, or Windows Server 2012 R2.
A support technician accidentally deletes a user account named User1. You need to use tombstone reanimation to restore the User1 account.
Which tool should you use?

A. Active Directory Administrative Center
B. Ntdsutil
C. Ldp
D. Esentutl

Answer: C

Explanation:
Use Ldp.exe to restore a single, deleted Active Directory object
This feature takes advantage of the fact that Active Directory keeps deleted objects in the database for a period of time before physically removing them.
use Ldp.exe to restore a single, deleted Active Directory object
The LPD.exe tool, included with Windows Server 2012, allows users to perform operations against any LDAP-compatible directory, including Active Directory. LDP is used to view objects stored in Active Directory along with their metadata, such as security descriptors and replication metadata.
References:
http: //www. petri. co. il/manually-undeleting-objects-windows-active-directory-ad. htm
http: //www. petri. co. il/manually-undeleting-objects-windows-active-directory-ad. htm
http: //technet. microsoft. com/en-us/magazine/2007. 09. tombstones. aspx
http: //technet. microsoft. com/nl-nl/library/dd379509(v=ws. 10). aspx#BKMK_2
http: //technet. microsoft. com/en-us/library/hh875546. aspx
http: //technet. microsoft. com/en-us/library/dd560651(v=ws. 10). aspx

NEW QUESTION 124
- (Topic 2)
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Access server role installed.
On Server1, you create a network policy named Policy1.
You need to configure Policy1 to ensure that users are added to a VLAN. Which attributes should you add to Policy1?

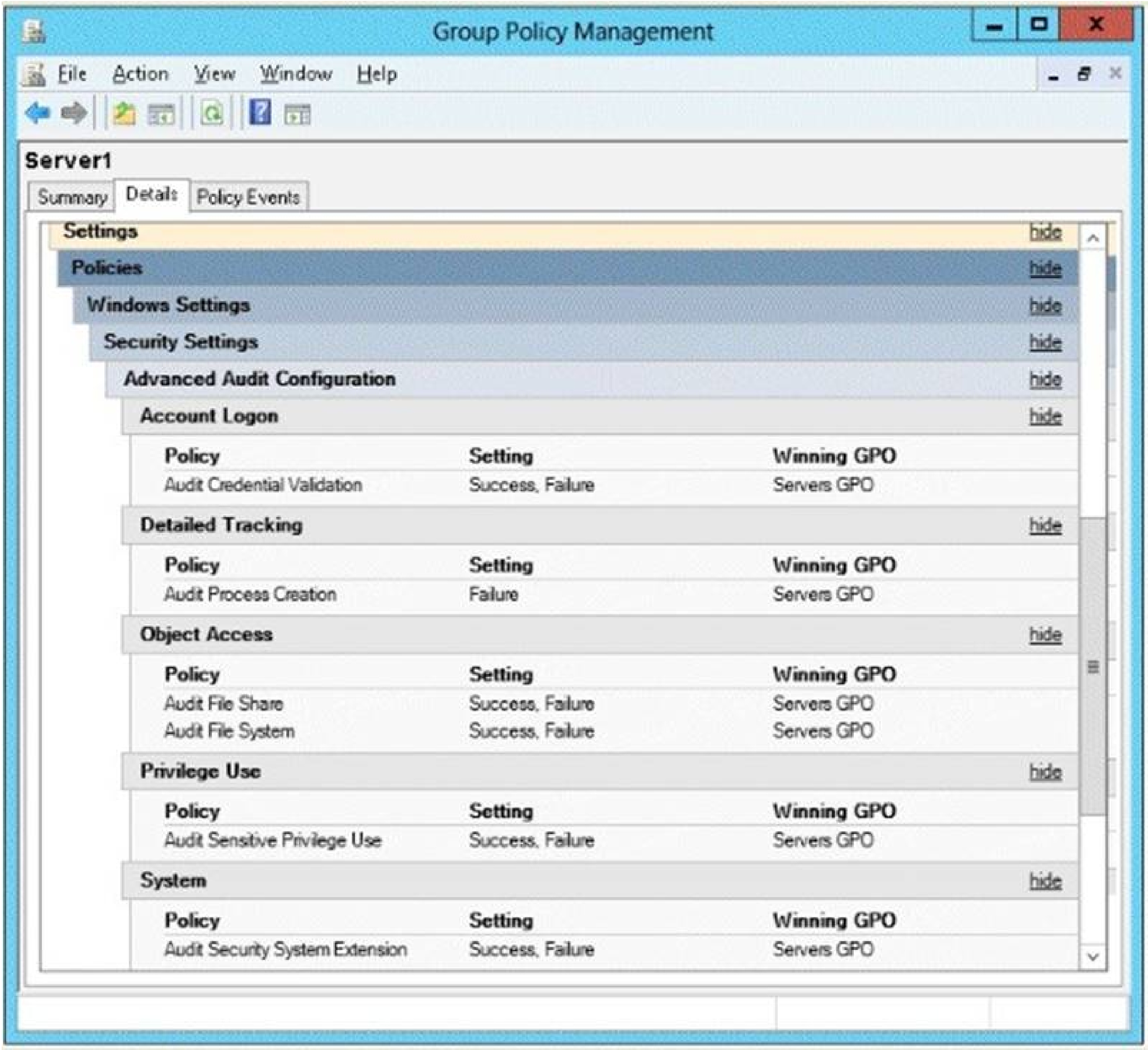
A. Tunnel-Tag, Tunnel-Password, Tunnel-Medium-Type, and Tunnel-Preference
B. Tunnel-Tag, Tunnel-Server-Auth-ID, Tunnel-Preference, and Tunnel-Pvt-Group-ID
C. Tunnel-Type, Tunnel-Tag, Tunnel-Medium-Type, and Tunnel-Pvt-Group-ID
D. Tunnel-Type, Tunnel-Password, Tunnel-Server-Auth-ID, and Tunnel-Pvt-Group-ID

Answer: C

Explanation:
VLAN attributes used in network policy
When you use network hardware, such as routers, switches, and access controllers that support virtual local area networks (VLANs), you can configure Network Policy Server (NPS) network policy to instruct the access servers to place members of Active Directory® groups on VLANs.
Before configuring network policy in NPS for VLANs, create groups of users in Active Directory Domain Services (AD DS) that you want to assign to specific VLANs. Then when you run the New Network Policy wizard, add the Active Directory group as a condition of the network policy.
You can create a separate network policy for each group that you want to assign to a VLAN. For more information, see Create a Group for a Network Policy. When you configure network policy for use with VLANs, you must configure the RADIUS standard attributes Tunnel-Medium-Type, Tunnel-Pvt-Group-ID, and Tunnel-Type. Some hardware vendors also require the use of the RADIUS standard attribute Tunnel-Tag.
To configure these attributes in a network policy, use the New Network Policy wizard to create a network policy. You can add the attributes to the network policy settings while running the wizard or after you have successfully created a policy with the wizard.
? Tunnel-Medium-Type. Select a value appropriate to the previous selections you
made while running the New Network Policy wizard. For example, if the network policy you are configuring is a wireless policy, in Attribute Value, select 802 (Includes all 802 media plus Ethernet canonical format).
? Tunnel-Pvt-Group-ID. Enter the integer that represents the VLAN number to which
group members will be assigned. For example, if you want to create a Sales VLAN for your sales team by assigning team members to VLAN 4, type the number 4.
? Tunnel-Type. Select the value Virtual LANs (VLAN).
? Tunnel-Tag. Some hardware devices do not require this attribute. If your hardware device requires this attribute, obtain this value from your hardware documentation.

NEW QUESTION 126
- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2.
You view the effective policy settings of Server1 as shown in the exhibit. (Click the Exhibit button.)



Account Logon

Policy	Setting	Winning GPO
Audit Credential Validation	Success, Failure	Servers GPO

Detailed Tracking

Policy	Setting	Winning GPO
Audit Process Creation	Failure	Servers GPO

Object Access

Policy	Setting	Winning GPO
Audit File Share	Success, Failure	Servers GPO
Audit File System	Success, Failure	Servers GPO

Privilege Use

Policy	Setting	Winning GPO
Audit Sensitive Privilege Use	Success, Failure	Servers GPO

System

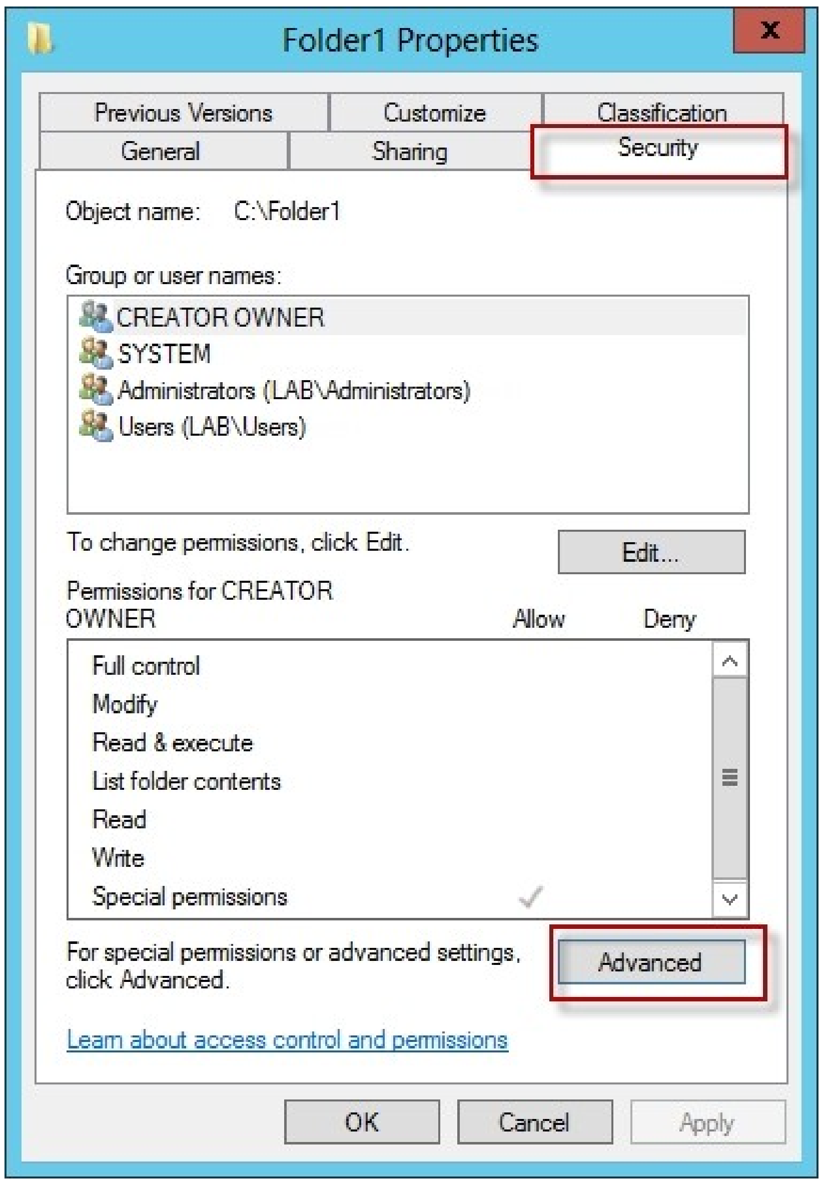
Policy	Setting	Winning GPO
Audit Security System Extension	Success, Failure	Servers GPO

On Server1, you have a folder named C:\Share1 that is shared as Share1. Share1 contains confidential data. A group named Group1 has full control of the content in Share1.
You need to ensure that an entry is added to the event log whenever a member of Group1 deletes a file in Share1.
What should you configure?

A. the Audit File Share setting of Servers GPO
B. the Sharing settings of C:\Share1
C. the Audit File System setting of Servers GPO
D. the Security settings of C:\Share1

Answer: D

Explanation:
You can use Computer Management to track all connections to shared resources on a Windows Server 2008 R2 system.
Whenever a user or computer connects to a shared resource, Windows Server 2008 R2 lists a connection in the Sessions node.
File access, modification and deletion can only be tracked, if the object access auditing is enabled you can see the entries in the event log.
To view connections to shared resources, type net session at a command prompt or follow these steps:
? In Computer Management, connect to the computer on which you created the
shared resource.
? In the console tree, expand System Tools, expand Shared Folders, and then select Sessions. You can now view connections to shares for users and computers.
To enable folder permission auditing, you can follow the below steps:
? Click start and run "secpol. msc" without quotes.
? Open the Local Policies\Audit Policy
? Enable the Audit object access for "Success" and "Failure".
? Go to target files and folders, right click the folder and select properties.
? Go to Security Page and click Advanced.



Object name: C:\Folder1

Group or user names:

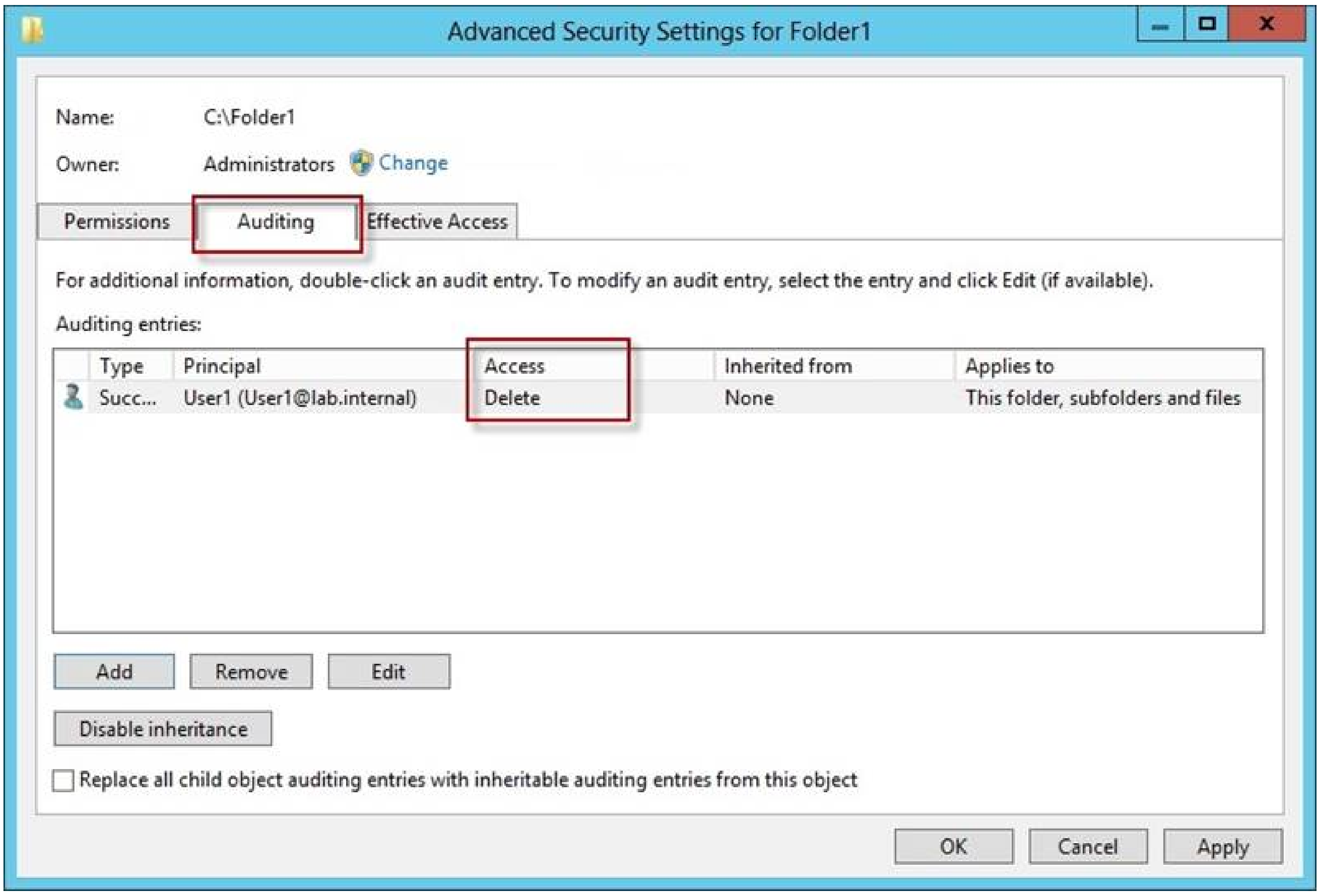
- CREATOR OWNER
- SYSTEM
- Administrators (LAB\Administrators)
- Users (LAB\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		
Special permissions	✓	

For special permissions or advanced settings, click Advanced.

? Click Auditing and Edit.
? Click add, type everyone in the Select User, Computer, or Group.
? Choose Apply onto: This folder, subfolders and files.
? Tick on the box “Change permissions”
? Click OK.



Name: C:\Folder1

Owner: Administrators

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	User1 (User1@lab.internal)	Delete	None	This folder, subfolders and files

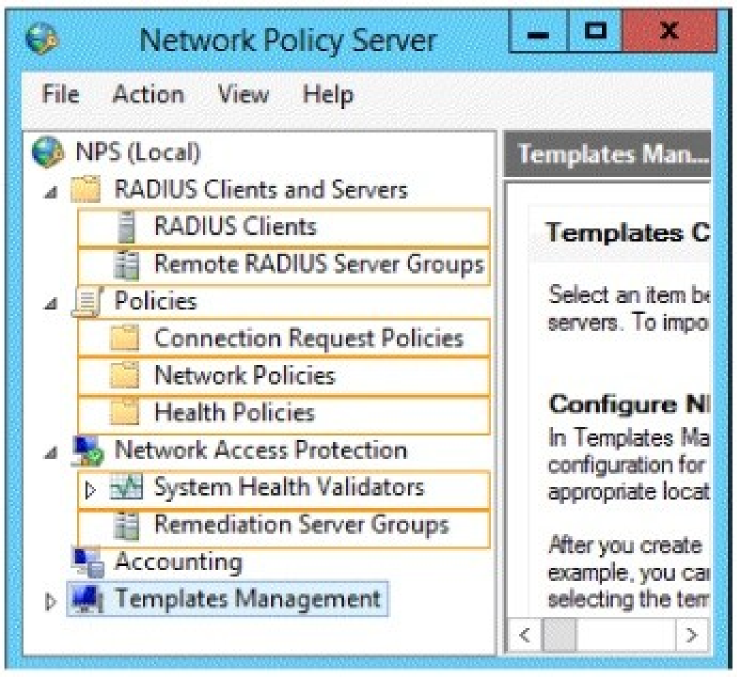
□ Replace all child object auditing entries with inheritable auditing entries from this object

After you enable security auditing on the folders, you should be able to see the folder permission changes in the server's Security event log. Task Category is File System.

References:

http: //social. technet. microsoft. com/Forums/en-US/winservergen/thread/13779c78-0c73- 4477-8014-f2eb10f3f10f/
http: //technet. microsoft. com/en-us/library/cc753927(v=ws. 10). aspx
http: //social. technet. microsoft. com/Forums/en-US/winservergen/thread/13779c78-0c73- 4477-8014-f2eb10f3f10f/
http: //support. microsoft. com/kb/300549
http: //www. windowsitpro. com/article/permissions/auditing-folder-permission-changes http: //www. windowsitpro. com/article/permissions/auditing-permission-changes-on-a- folder

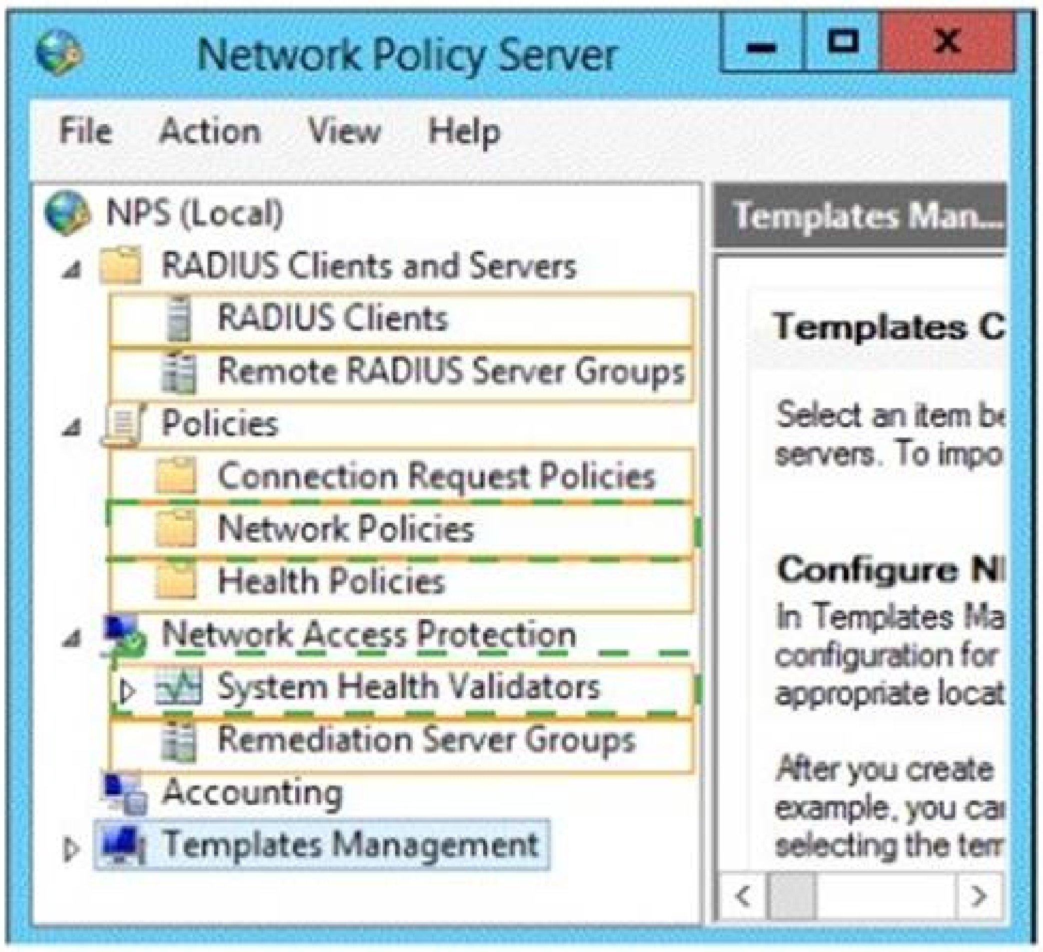
NEW QUESTION 128
HOTSPOT - (Topic 2)
You have a server named Server1 that runs Windows Server 2012 R2. You configure Network Access Protection (NAP) on Server1.
Your company implements a new security policy stating that all client computers must have the latest updates installed. The company informs all employees that they have two weeks
to update their computer accordingly.
You need to ensure that if the client computers have automatic updating disabled, they are provided with full access to the network until a specific date and time.
Which two nodes should you configure?
To answer, select the appropriate two nodes in the answer area.



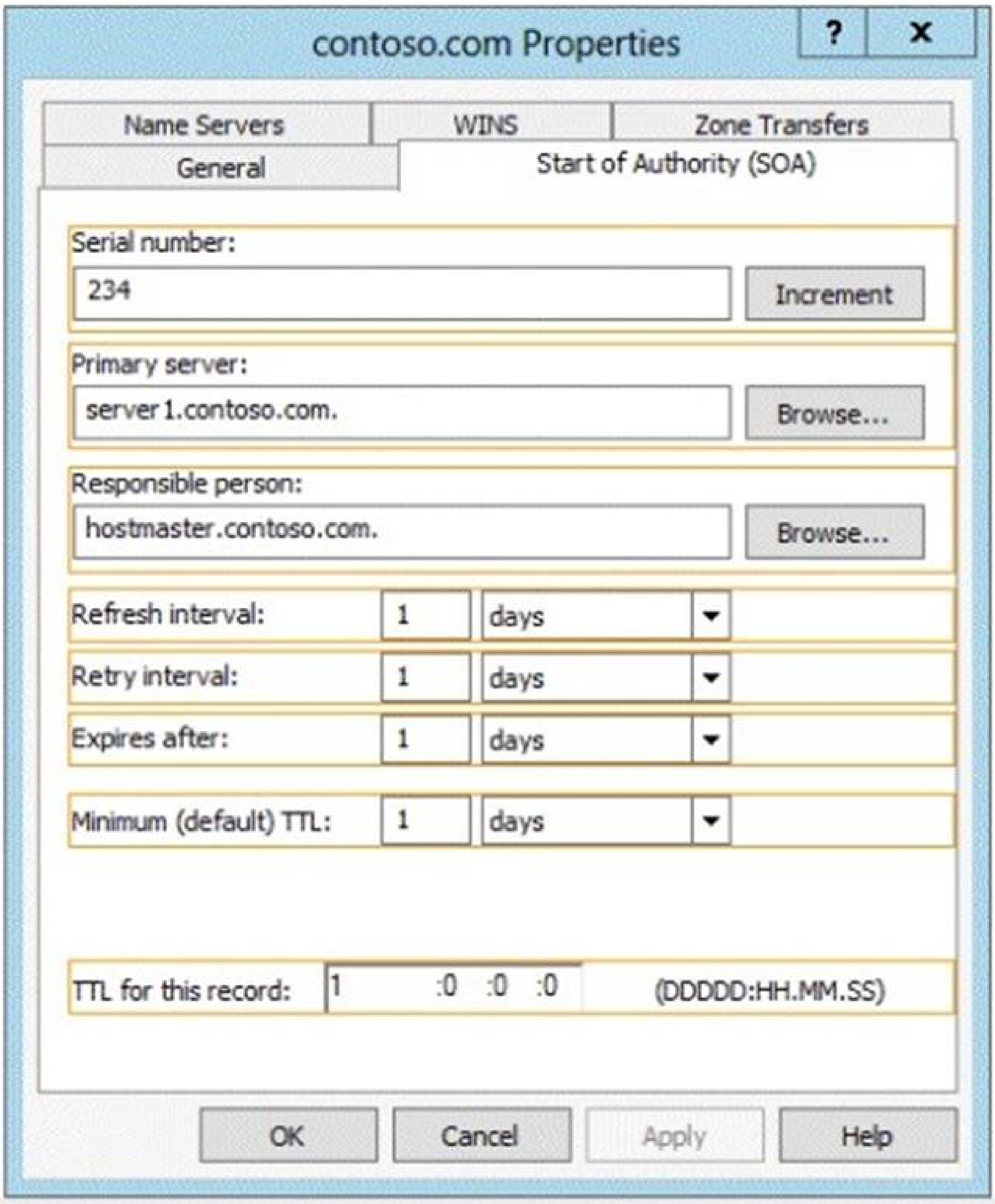
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 131
HOTSPOT - (Topic 2)
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.



contoso.com Properties

Serial number: 234

Primary server: server1.contoso.com.

Responsible person: hostmaster.contoso.com.

Refresh interval: 1 days

Retry interval: 1 days

Expires after: 1 days

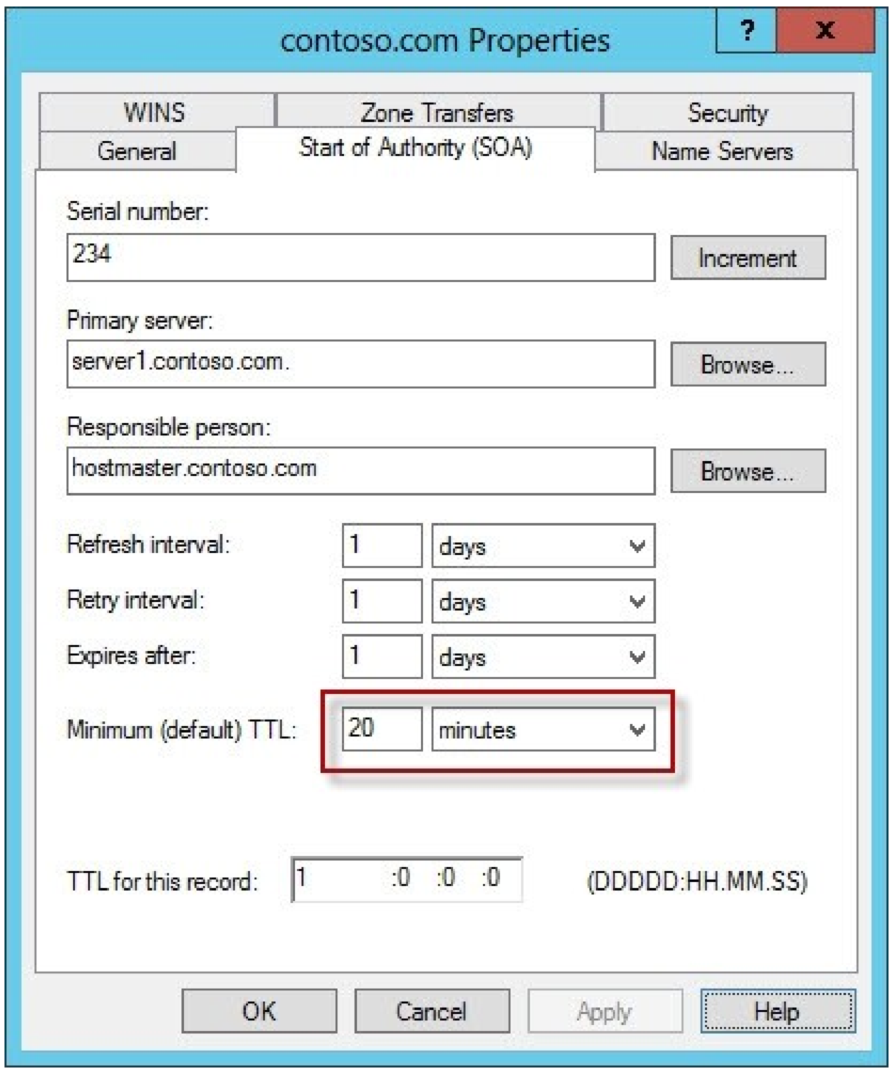
Minimum (default) TTL: 1 days

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

A. Mastered
B. Not Mastered

Answer: A

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.



Serial number: 234

Primary server: server1.contoso.com.

Responsible person: hostmaster.contoso.com

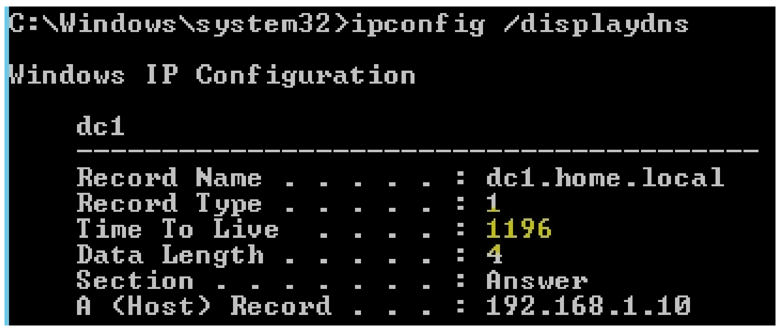
Refresh interval: 1 days

Retry interval: 1 days

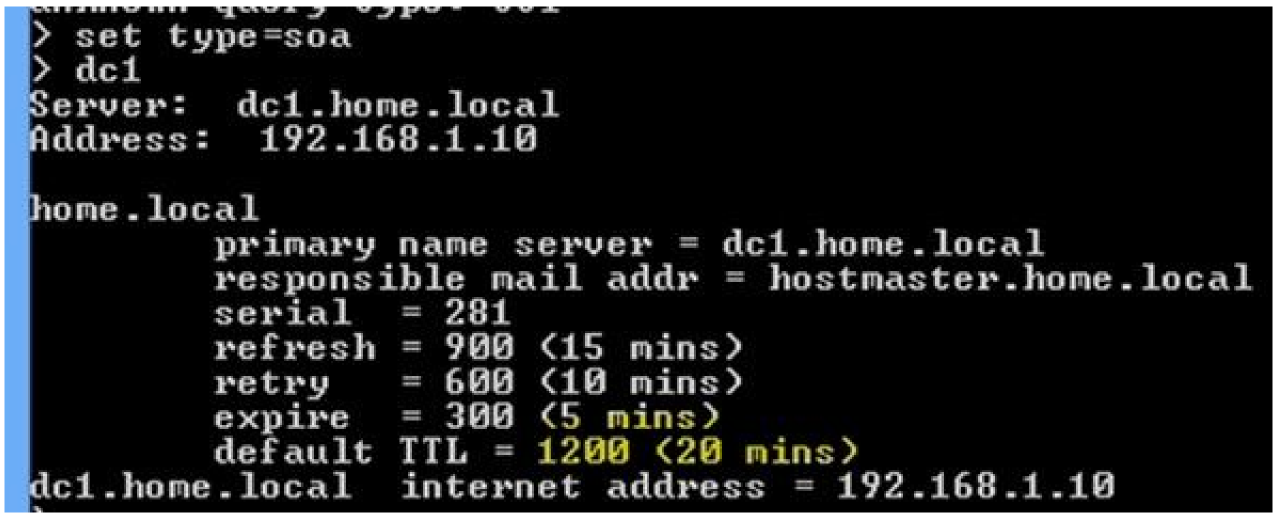
Expires after: 1 days

Minimum (default) TTL: 20 minutes

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



```
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 133

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2. Both servers have the File and Storage Services server role, the DFS Namespace role service, and the DFS Replication role service installed. Server1 and Server2 are part of a Distributed File System (DFS) Replication group named Group1. Server1 and Server2 are connected by using a high-speed LAN connection.

You need to minimize the amount of processor resources consumed by DFS Replication. What should you do?

A. Modify the replication schedule.
B. Modify the staging quota.
C. Disable Remote Differential Compression (RDC).
D. Reduce the bandwidth usage.

Answer: C

Explanation:

Because disabling RDC can help conserve disk input/output (I/O) and CPU resources, you might want to disable RDC on a connection if the sending and receiving members are in a local area network (LAN), and bandwidth use is not a concern. However, in a LAN environment where bandwidth is contended, RDC can be beneficial when transferring large files.

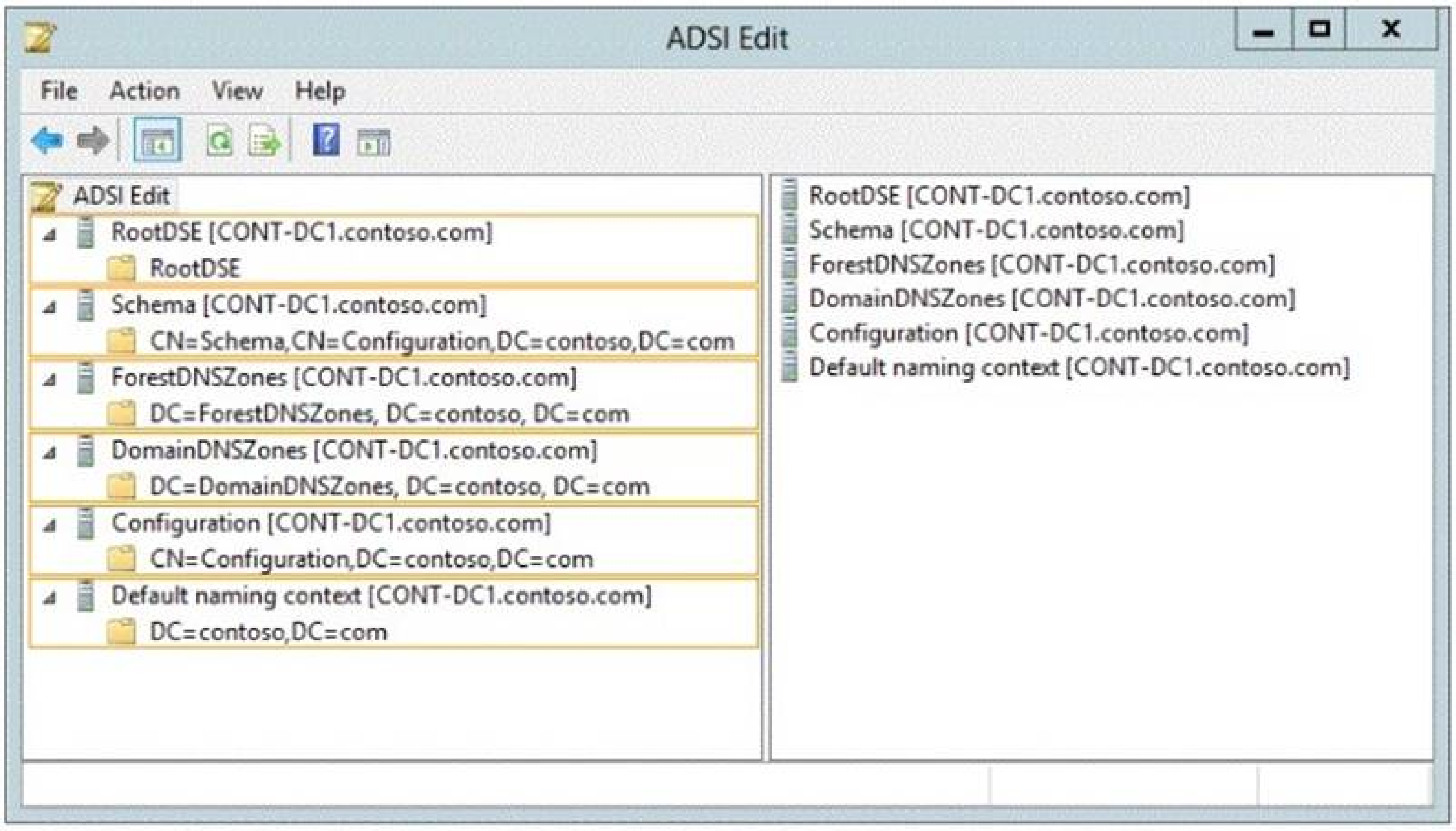
Question tells it uses a high-speed LAN connection.

References:

http: //technet. microsoft. com/en-us/library/cc758825%28v=ws. 10%29. aspx http: //technet. microsoft. com/en-us/library/cc754229. aspx

NEW QUESTION 134

HOTSPOT - (Topic 2)
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.


ADSI Edit
File
Action
View
Help
ADSI Edit
RootDSE [CONT-DC1.contoso.com]
RootDSE
Schema [CONT-DC1.contoso.com]
CN=Schema,CN=Configuration,DC=contoso,DC=com
ForestDNSZones [CONT-DC1.contoso.com]
DC=ForestDNSZones, DC=contoso, DC=com
DomainDNSZones [CONT-DC1.contoso.com]
DC=DomainDNSZones, DC=contoso, DC=com
Configuration [CONT-DC1.contoso.com]
CN=Configuration,DC=contoso,DC=com
Default naming context [CONT-DC1.contoso.com]
DC=contoso,DC=com
RootDSE [CONT-DC1.contoso.com]
Schema [CONT-DC1.contoso.com]
ForestDNSZones [CONT-DC1.contoso.com]
DomainDNSZones [CONT-DC1.contoso.com]
Configuration [CONT-DC1.contoso.com]
Default naming context [CONT-DC1.contoso.com]

A. Mastered
B. Not Mastered

Answer: A

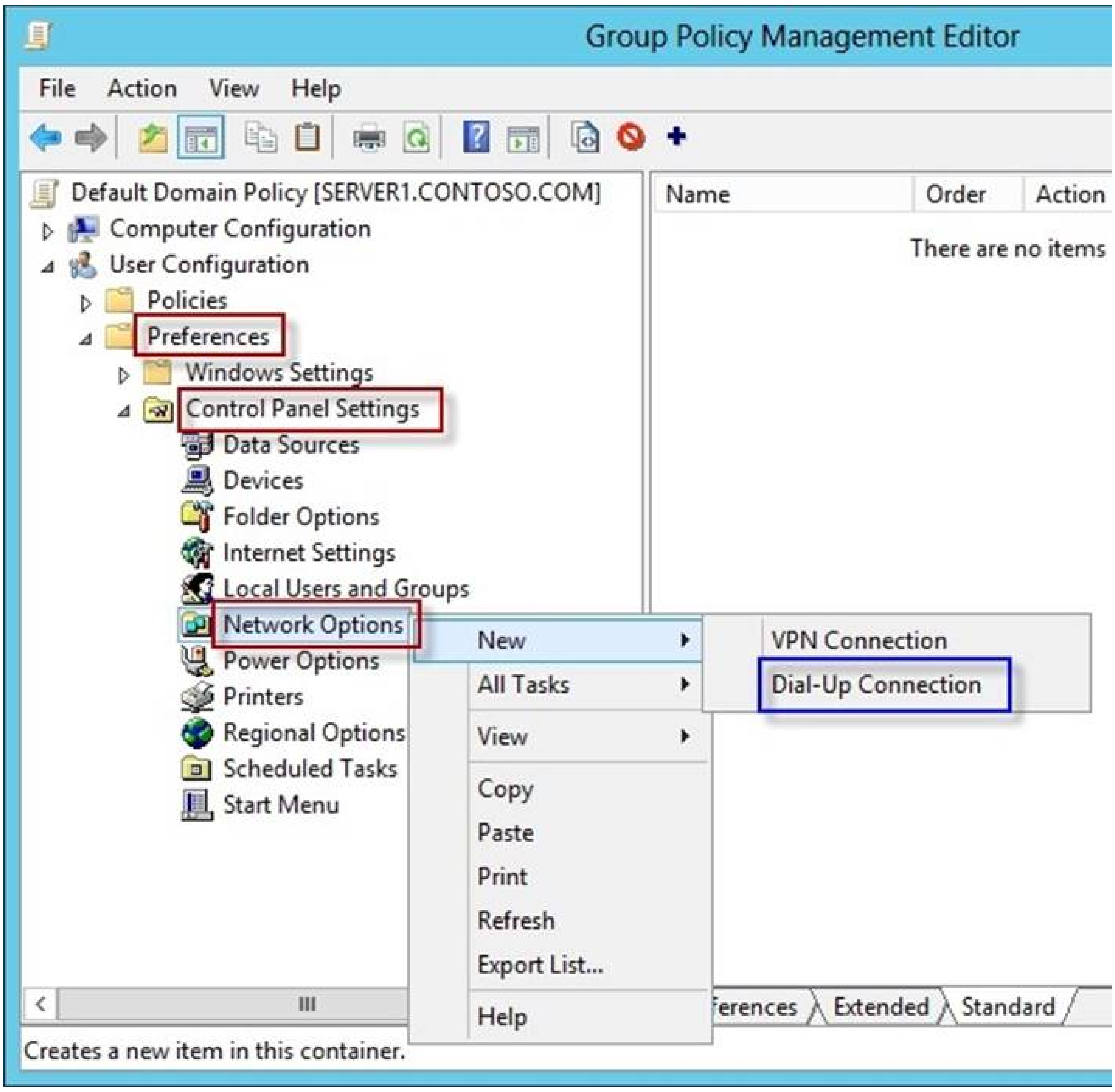
Explanation:
Starting in Windows Server 2008 R2, Active Directory now implements a true recycle bin. No longer will you need an authoritative restore to recover deleted users, groups, OU's, or other objects. Instead, it is now possible to use PowerShell commands to bring back objects with all their attributes, 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 139
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.
All sales users have laptop computers that run Windows 8. The sales computers are joined to the domain. All user accounts for the sales department are in an organizational unit (OU) named Sales_OU.
A Group Policy object (GPO) named GPO1 is linked to Sales_OU. You need to configure a dial-up connection for all of the sales users. What should you configure from User Configuration in GPO1?

A. Policies/Administrative Templates/Network/Windows Connect Now
B. Preferences/Control Panel Settings/Network Options
C. Policies/Administrative Templates/Windows Components/Windows Mobility Center
D. Policies/Administrative Templates/Network/Network Connections

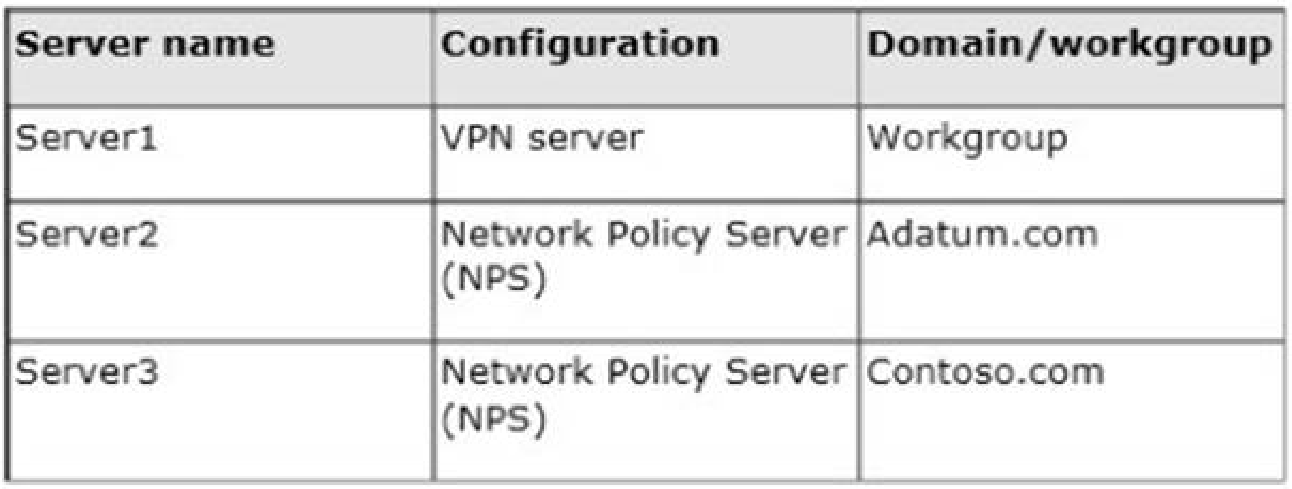
Answer: B

Explanation:
The Network Options extension allows you to centrally create, modify, and delete dial-up networking and virtual private network (VPN) connections. Before you create a network option preference item, you should review the behavior of each type of action possible with the extension.



To create a new Dial-Up Connection preference item
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 Control Panel Settings folder.
Right-click the Network Options node, point to New, and select Dial-Up Connection.
References:
http: //technet. microsoft. com/en-us/library/cc772107. aspx
http: //technet. microsoft. com/en-us/library/cc772107. aspx
http: //technet. microsoft. com/en-us/library/cc772449. aspx

NEW QUESTION 142
- (Topic 2)
Your network contains two Active Directory forests named adatum.com and contoso.com. The network contains three servers. The servers are configured as shown in the following table.



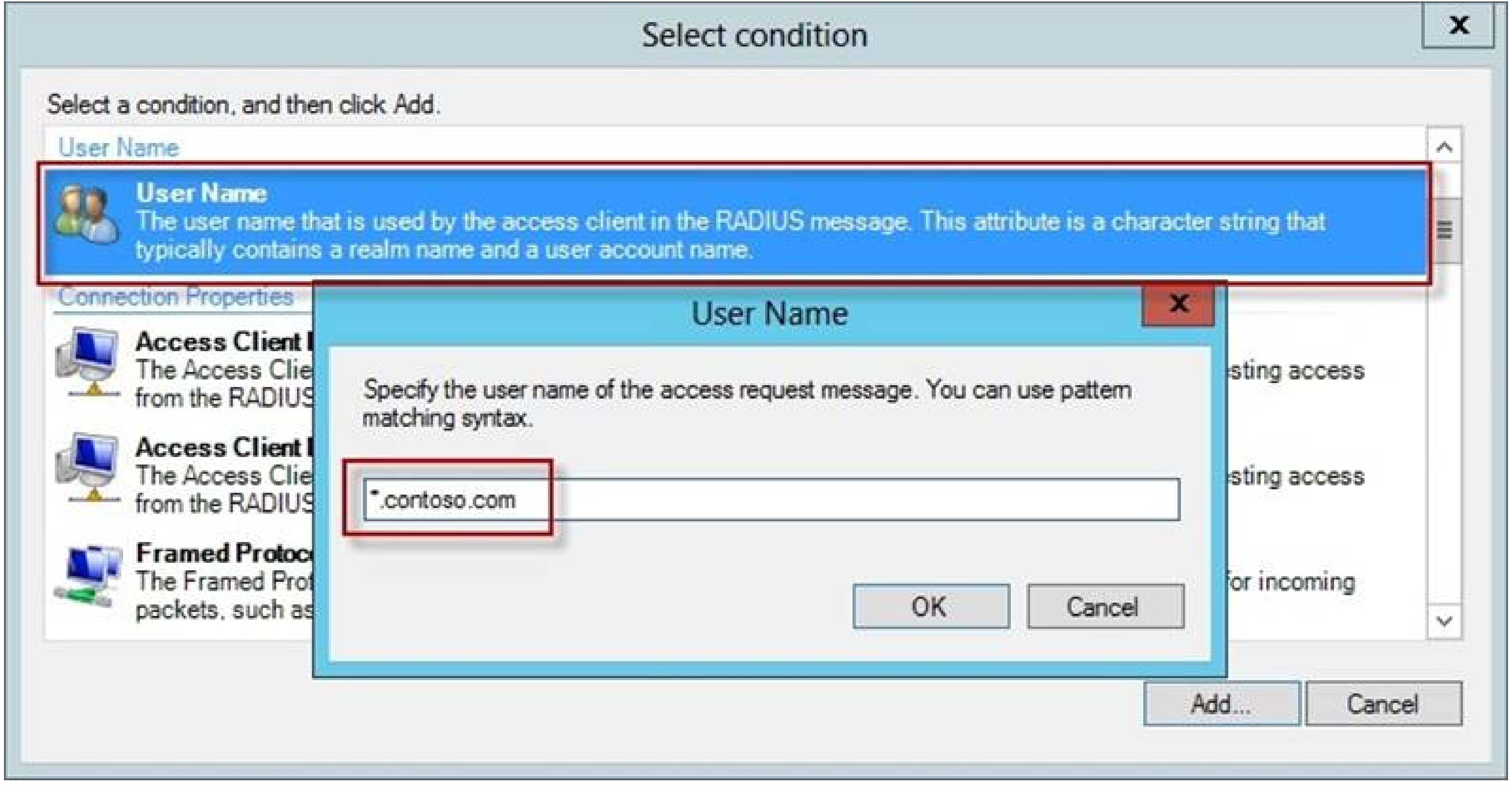
Server name	Configuration	Domain/workgroup
Server1	VPN server	Workgroup
Server2	Network Policy Server (NPS)	Adatum.com
Server3	Network Policy Server (NPS)	Contoso.com

You need to ensure that connection requests from adatum.com users are forwarded to Server2 and connection requests from contoso.com users are forwarded to Server3.
Which two should you configure in the connection request policies on Server1? (Each correct answer presents part of the solution. Choose two.)

A. The Authentication settings
B. The Standard RADIUS Attributes settings
C. The Location Groups condition
D. The Identity Type condition
E. The User Name condition

Answer: AE

Explanation:
The User Name attribute group contains the User Name attribute. By using this attribute, you can designate the user name, or a portion of the user name, that must match the user name supplied by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name. You can use pattern- matching syntax to specify user names.


Select condition

Select a condition, and then click Add.

User Name

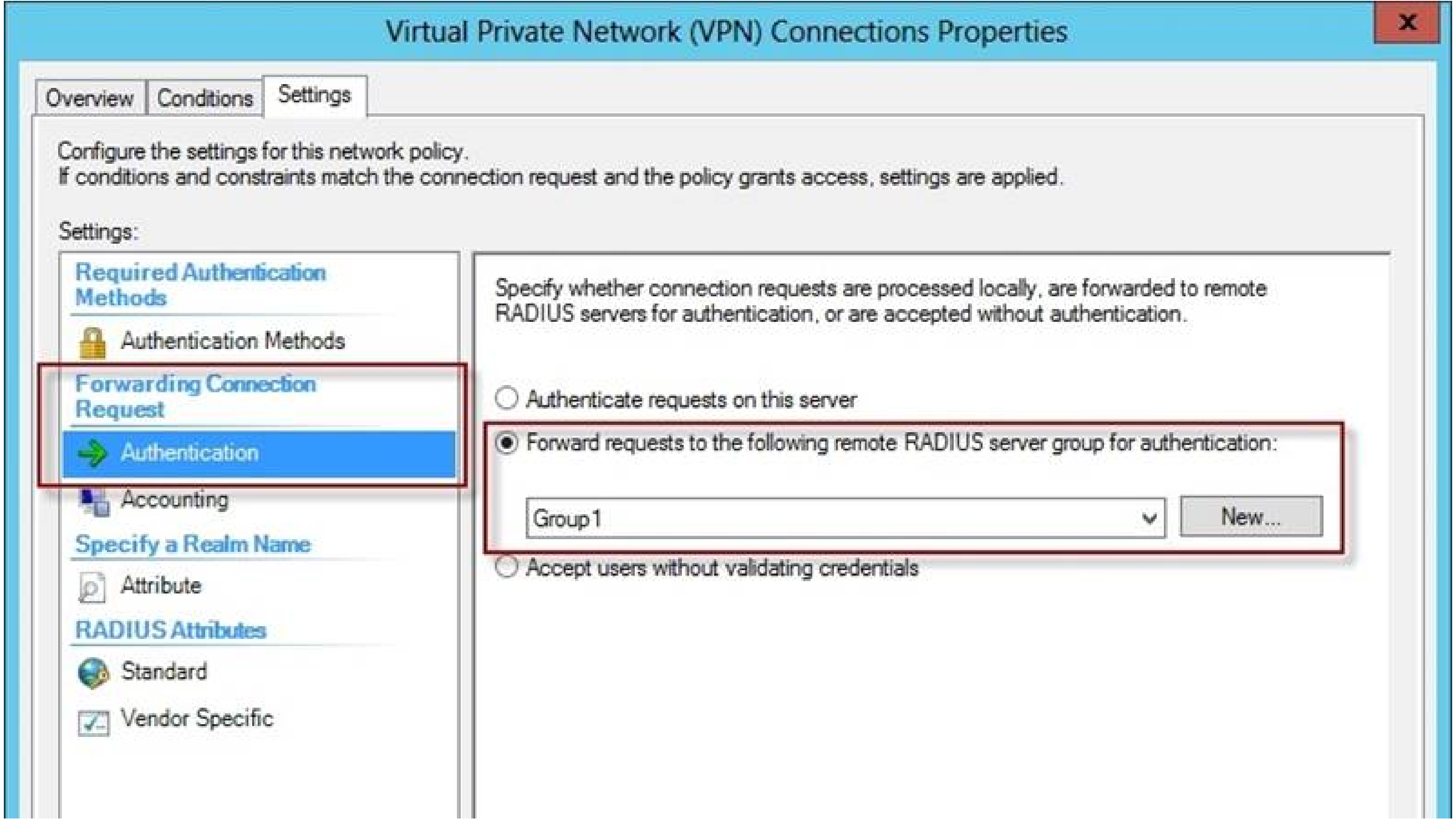
User Name
The user name that is used by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name.

User Name

Specify the user name of the access request message. You can use pattern matching syntax.

*.contoso.com

By using this setting, you can override the authentication settings that are configured in all network policies and you can designate the authentication methods and types that are required to connect to your network.
Forward requests to the following remote RADIUS server group . By using this setting, NPS forwards connection requests to the remote RADIUS server group that you specify. If the NPS server receives a valid Access-Accept message that corresponds to the Access- Request message, the connection attempt is considered authenticated and authorized. In this case, the NPS server acts as a RADIUS proxy


Virtual Private Network (VPN) Connections Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

○ Authenticate requests on this server
● Forward requests to the following remote RADIUS server group for authentication:
Group1
○ Accept users without validating credentials

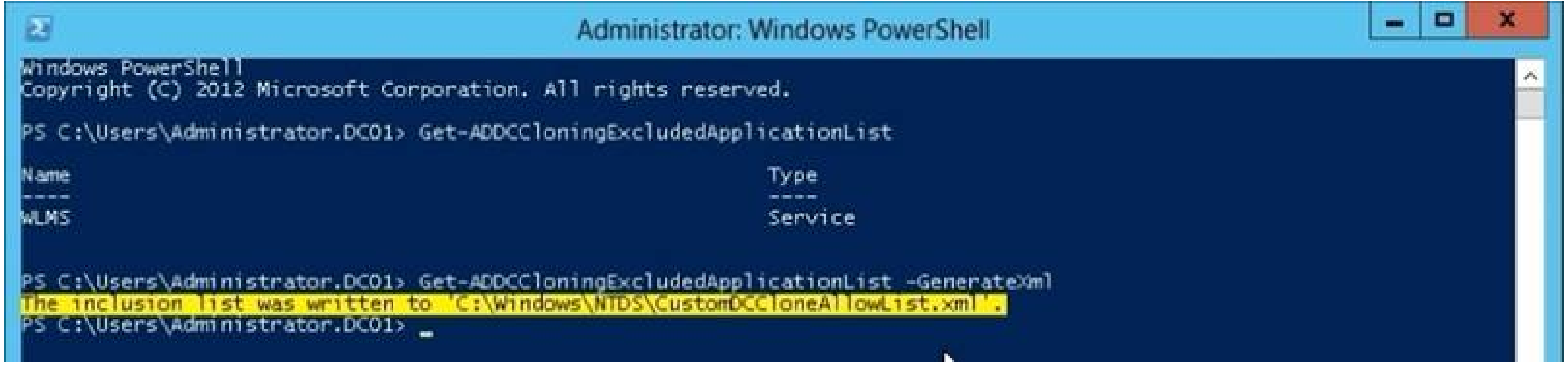
Connection request policies are sets of conditions and profile settings that give network administrators flexibility in configuring how incoming authentication and accounting request messages are handled by the IAS server. With connection request policies, you can create a series of policies so that some RADIUS request messages sent from RADIUS clients are processed locally (IAS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (IAS is being used as a RADIUS proxy). This capability allows IAS to be deployed in many new RADIUS scenarios.
With connection request policies, you can use IAS as a RADIUS server or as a RADIUS proxy, based on the time of day and day of the week, by the realm name in the request, by the type of connection being requested, by the IP address of the RADIUS client, and so on.
References:
http: //technet. microsoft. com/en-us/library/cc757328. aspx
http: //technet. microsoft. com/en-us/library/cc753603. aspx

NEW QUESTION 145
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
On all of the domain controllers, Windows is installed in C:\Windows and the Active
Directory database is located in D:\Windows\NTDS\.
All of the domain controllers have a third-party application installed.
The operating system fails to recognize that the application is compatible with domain controller cloning.
You verify with the application vendor that the application supports domain controller cloning.
You need to prepare a domain controller for cloning. What should you do?

A. In D:\Windows\NTDS\, create an XML file named DCCloneConfig.xml and add the application information to the file.
B. In the root of a USB flash drive, add the application information to an XML file named DefaultDCCloneAllowList.xml.
C. In D:\Windows\NTDS\, create an XML file named CustomDCCloneAllowList.xml and add the application information to the file.
D. In C:\Windows\System32\Sysprep\Actionfiles\, add the application information to an XML file named Respecialize.xml.

Answer: C

Explanation:
Place the CustomDCCloneAllowList.xml file in the same folder as the Active Directory database (ntds. dit) on the source Domain Controller.



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.DC01> Get-ADDCCloningExcludedApplicationList

Name                                                        Type
----                                                        ----
WLMS                                                        Service


PS C:\Users\Administrator.DC01> Get-ADDCCloningExcludedApplicationList -GenerateXml
The inclusion list was written to 'C:\Windows\NTDS\CustomDCCloneAllowList.xml'.
PS C:\Users\Administrator.DC01> _
```

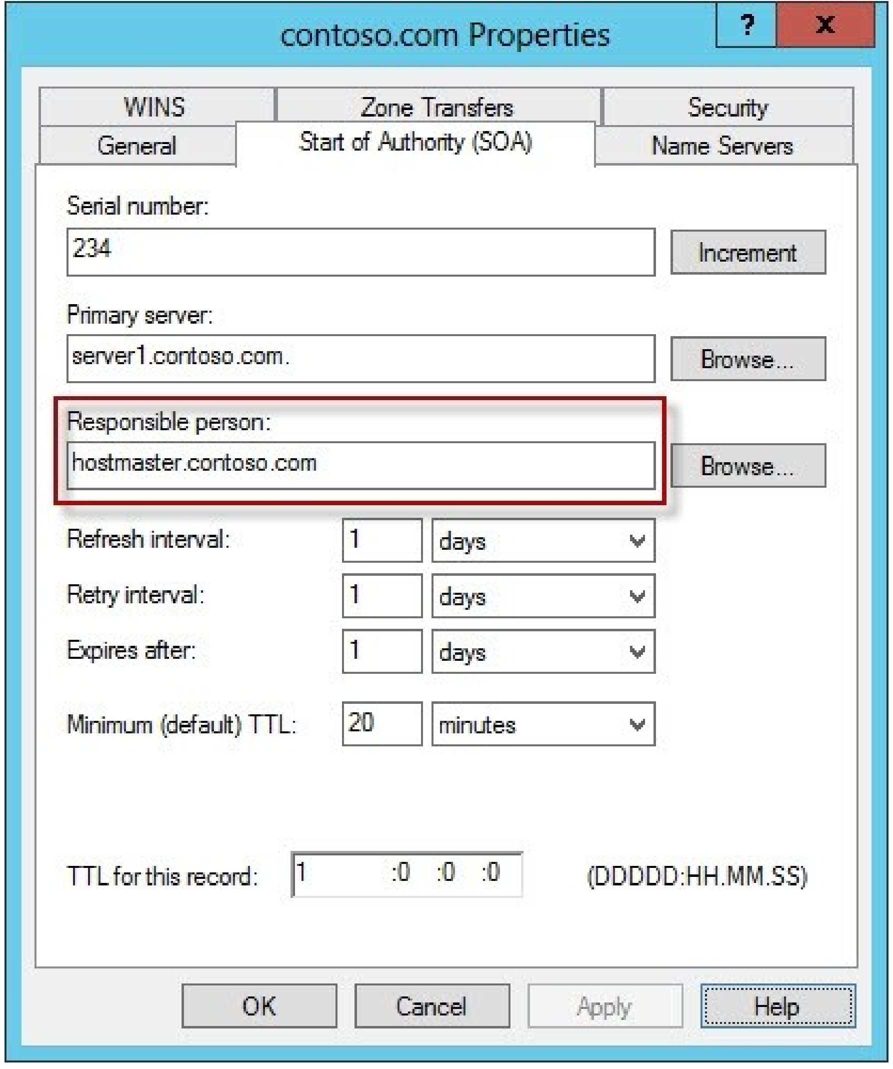
References:
http://blogs.dirteam.com/blogs/sanderberkouwer/archive/2012/09/10/new-features-in-active-directory-domain-services-in-windows-server-2012-part-13-domain-controller- cloning. aspx
http://www.thomasmaurer.ch/2012/08/windows-server-2012-hyper-v-how-to-clone-a-virtual-domain-controller
http: //technet. microsoft. com/en-us/library/hh831734. aspx

NEW QUESTION 149
- (Topic 2)
You have a DNS server named Server1 that runs Windows Server 2012 R2. On Server1, you create a DNS zone named contoso.com.
You need to specify the email address of the person responsible for the zone. Which type of DNS record should you configure?

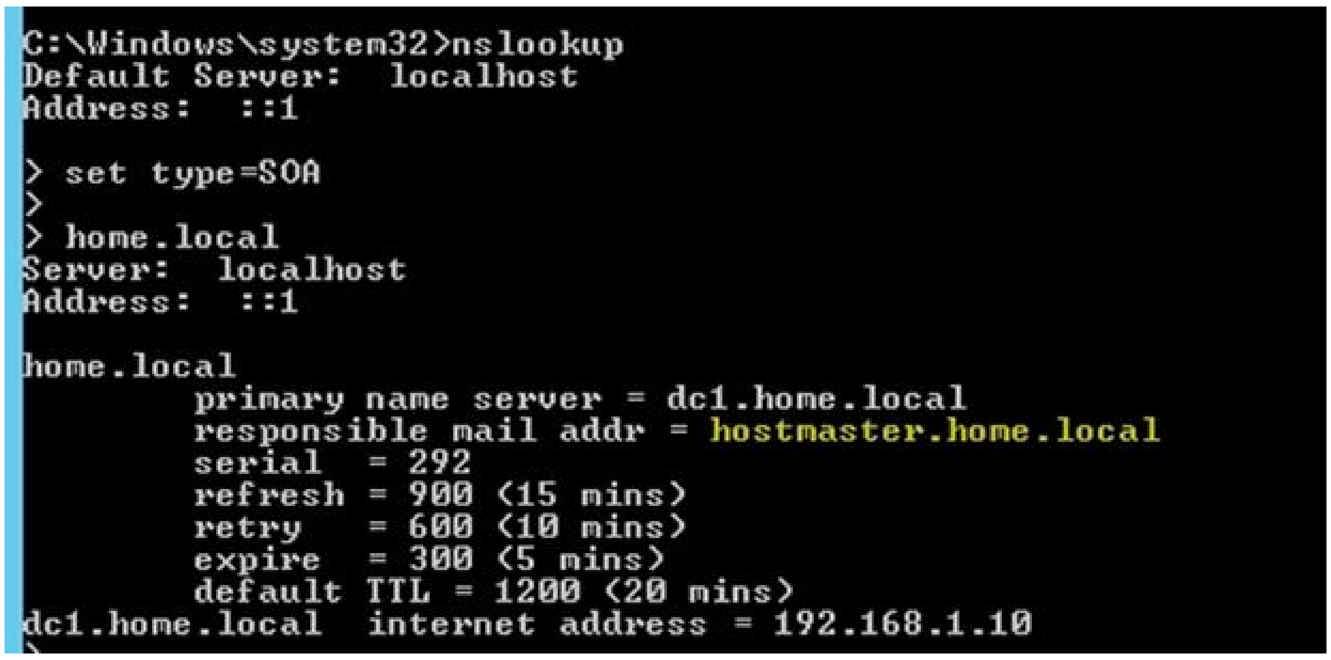
A. Start of authority (SOA)
B. Host information (HINFO)
C. Mailbox (MB)
D. Mail exchanger (MX)

Answer: A

Explanation:
A SOA-record defines the responsible person for an entire zone, but a zone may contain many individual hosts / domain names for which different people are responsible. The RP- record type makes it possible to identify the responsible person for individual host names contained within the zone.



Serial number: 234
Primary server: server1.contoso.com.
Responsible person: hostmaster.contoso.com
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)



```
C:\Windows\system32>nslookup
Default Server:  localhost
Address:  ::1

> set type=SOA
>
> home.local
Server:  localhost
Address:  ::1

home.local
        primary name server = dc1.home.local
        responsible mail addr = hostmaster.home.local
        serial  = 292
        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
>
```

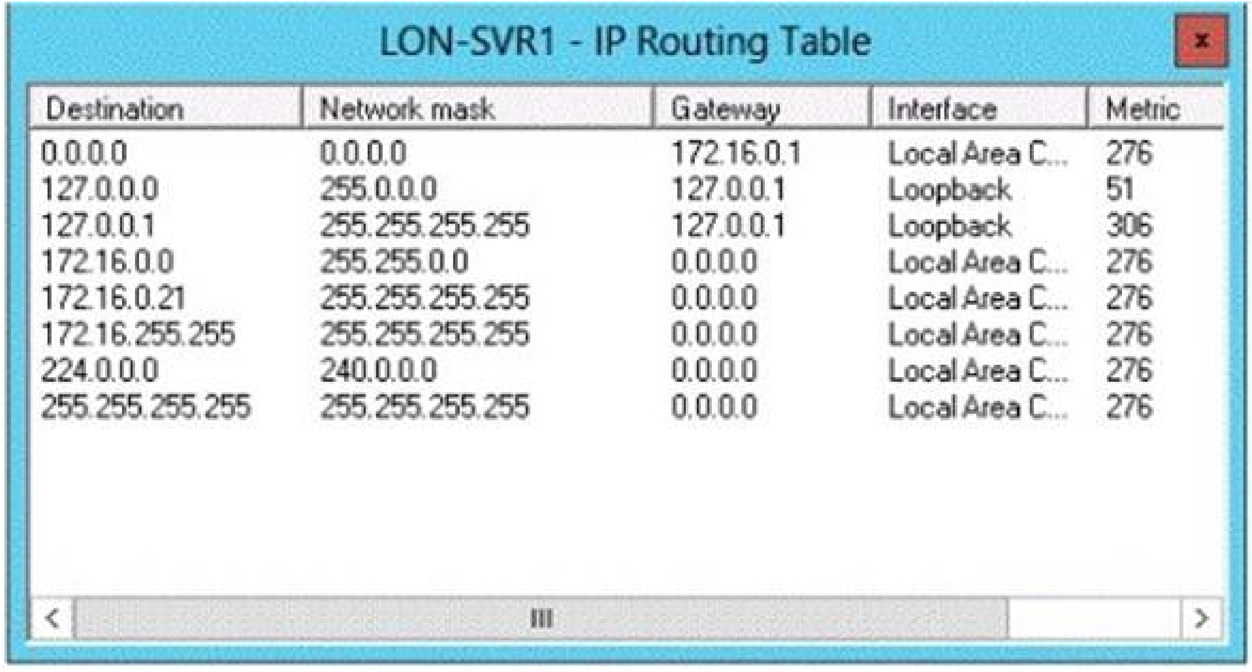
NEW QUESTION 153
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
Administrators use client computers that run Windows 8 to perform all management tasks. A central store is configured on a domain controller named DC1.
You have a custom administrative template file named App1.admx. App1.admx contains application settings for an application named Appl.
From a client computer named Computer1, you create a new Group Policy object (GPO) named GPO1.
You discover that the application settings for App1 fail to appear in GPO1.
You need to ensure that the App1 settings appear in all of the new GPOs that you create. What should you do?

A. From the Default Domain Controllers Policy, add App1.admx to the Administrative Templates.
B. Copy App1.admx to \\Contoso.com\SYSVOL\Contoso.com\Policies\PolicyDefinitions\.
C. From the Default Domain Policy, add App1.admx to the Administrative Templates.
D. Copy App1.admx to \\Contoso.com\SYSVOL\Contoso.com\StarterGPOs.

Answer: B

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.

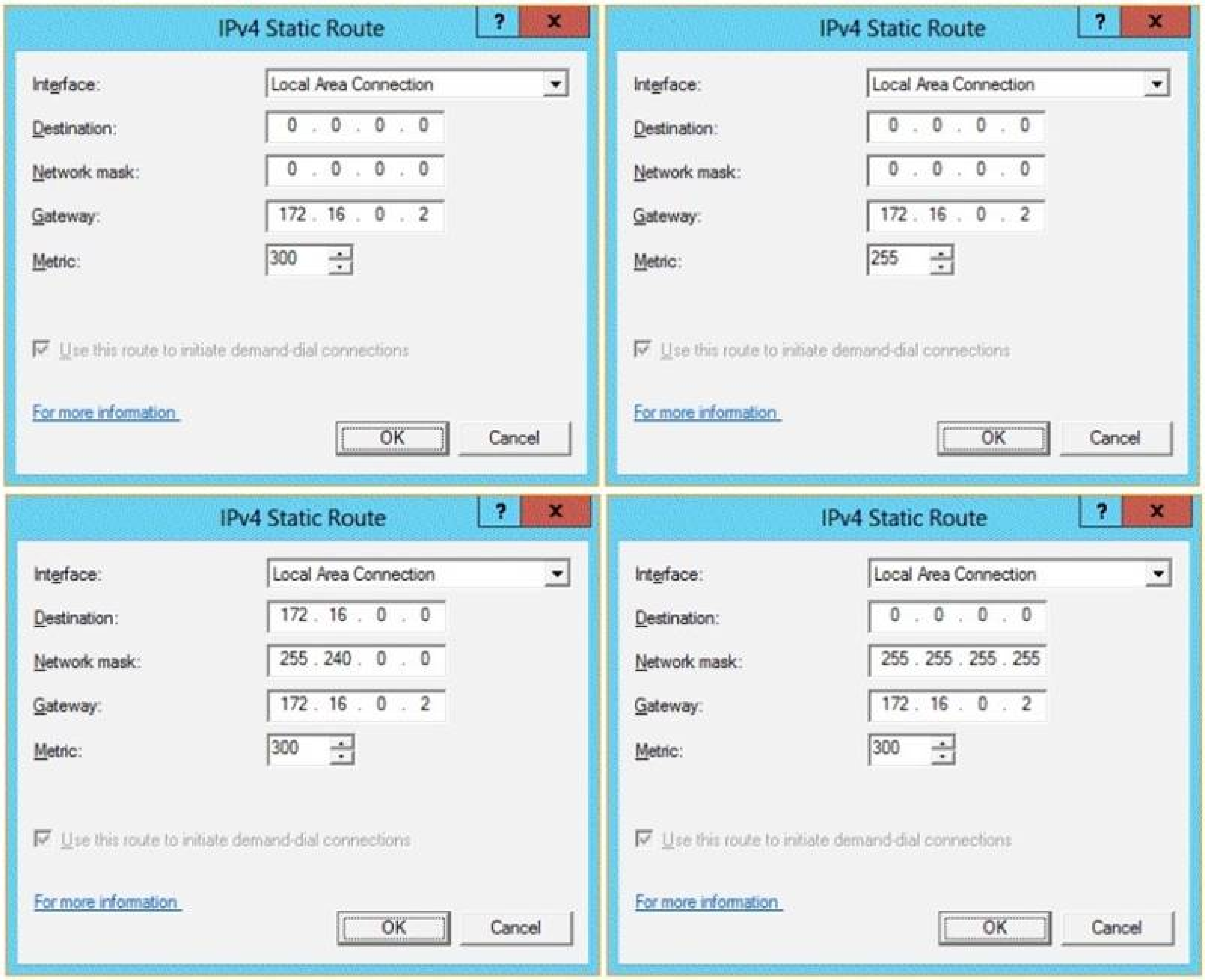
NEW QUESTION 154
HOTSPOT - (Topic 2)
You have a server named LON-SVR1 that runs Windows Server 2012 R2. LON-SVR1 has the Remote Access server role installed. LON-SVRl is located in the perimeter network.
The IPv4 routing table on LON-SVR1 is configured as shown in the following exhibit. (Click the Exhibit button.)



LON-SVR1 - IP Routing Table

Destination	Network mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.16.0.1	Local Area C...	276
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	51
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	306
172.16.0.0	255.255.0.0	0.0.0.0	Local Area C...	276
172.16.0.21	255.255.255.255	0.0.0.0	Local Area C...	276
172.16.255.255	255.255.255.255	0.0.0.0	Local Area C...	276
224.0.0.0	240.0.0.0	0.0.0.0	Local Area C...	276
255.255.255.255	255.255.255.255	0.0.0.0	Local Area C...	276

Your company purchases an additional router named Router1. Router1 has an interface that connects to the perimeter network and an interface that connects to the Internet. The IP address of the interface that connects to the perimeter network is 172.16.0.2.
You need to ensure that LON-SVR1 will route traffic to the Internet by using Router1 if the current default gateway is unavailable.
How should you configure the static route on LON-SVR1? To answer, select the appropriate static route in the answer area.



IPv4 Static Route

Interface: Local Area Connection
Destination: 0 . 0 . 0 . 0
Network mask: 0 . 0 . 0 . 0
Gateway: 172 . 16 . 0 . 2
Metric: 300

☑ Use this route to initiate demand-dial connections

For more information

IPv4 Static Route

Interface: Local Area Connection
Destination: 0 . 0 . 0 . 0
Network mask: 0 . 0 . 0 . 0
Gateway: 172 . 16 . 0 . 2
Metric: 255

☑ Use this route to initiate demand-dial connections

For more information

IPv4 Static Route

Interface: Local Area Connection
Destination: 172 . 16 . 0 . 0
Network mask: 255 . 240 . 0 . 0
Gateway: 172 . 16 . 0 . 2
Metric: 300

☑ Use this route to initiate demand-dial connections

For more information

IPv4 Static Route

Interface: Local Area Connection
Destination: 0 . 0 . 0 . 0
Network mask: 255 . 255 . 255 . 255
Gateway: 172 . 16 . 0 . 2
Metric: 300

☑ Use this route to initiate demand-dial connections

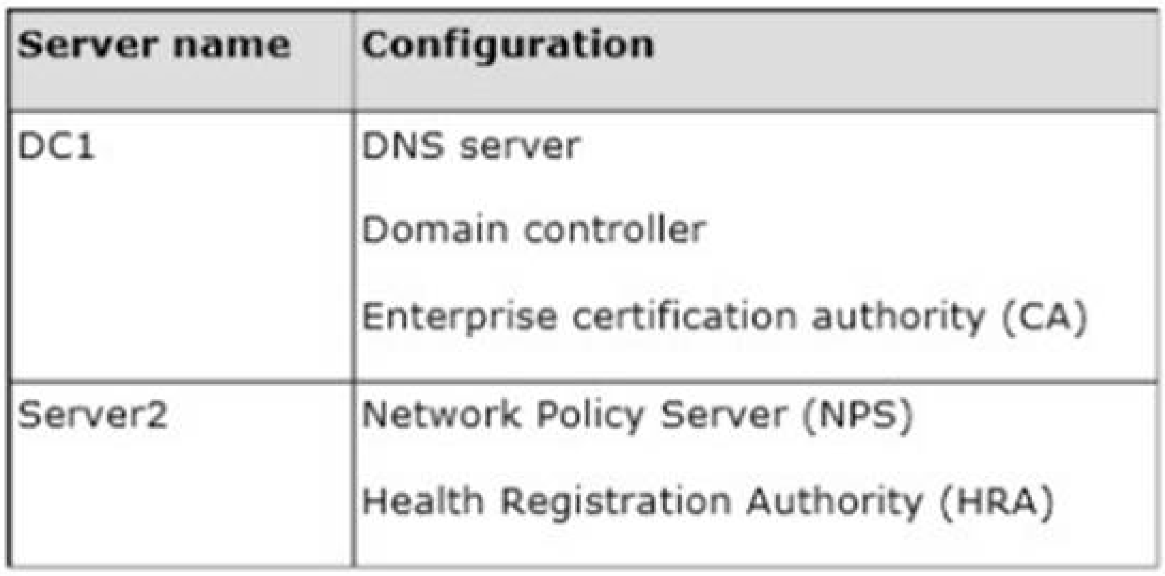
For more information

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Metric: Specifies an integer cost metric (ranging from 1 to 9999) for the route, which is used when choosing among multiple routes in the routing table that most closely match the destination address of a packet being forwarded. The route with the lowest metric is chosen. The metric can reflect the number of hops, the speed of the path, path reliability, path throughput, or administrative properties.
A metric is a value that is assigned to an IP route for a particular network interface that identifies the cost that is associated with using that route.
The metric that is assigned to specific default gateways can be configured independently for each gateway. This setup enables a further level of control over the metric that is used for the local routes.

NEW QUESTION 157
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The domain contains two servers. The servers are configured as shown in the following table.



Server name	Configuration
DC1	DNS server Domain controller Enterprise certification authority (CA)
Server2	Network Policy Server (NPS) Health Registration Authority (HRA)

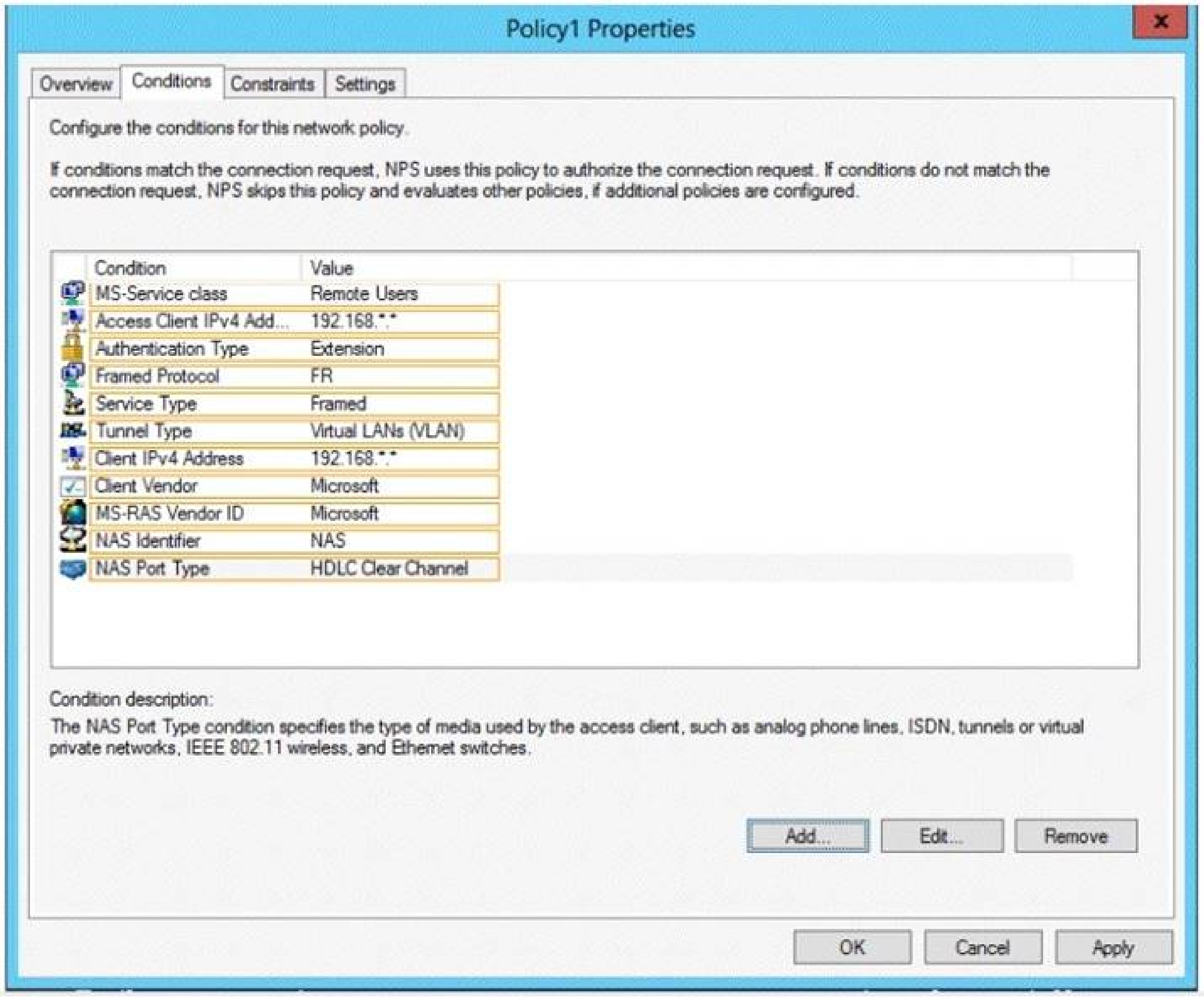
All client computers run Windows 8 Enterprise.
You plan to deploy Network Access Protection (NAP) by using IPSec enforcement.
A Group Policy object (GPO) named GPO1 is configured to deploy a trusted server group to all of the client computers.
You need to ensure that the client computers can discover HRA servers automatically. Which three actions should you perform? (Each correct answer presents part of the
solution. Choose three.)

A. On all of the client computers, configure the EnableDiscovery registry key.
B. In a GPO, modify the Request Policy setting for the NAP Client Configuration.
C. On Server2, configure the EnableDiscovery registry key.
D. On DC1, create an alias (CNAME) record.
E. On DC1, create a service location (SRV) record.

Answer: ABE

Explanation:
Requirements for HRA automatic discovery
The following requirements must be met in order to configure trusted server groups on NAP client computers using HRA automatic discovery:
Client computers must be running Windows Vista® with Service Pack 1 (SP1) or Windows XP with Service Pack 3 (SP3).
The HRA server must be configured with a Secure Sockets Layer (SSL) certificate. The EnableDiscovery registry key must be configured on NAP client computers. DNS SRV records must be configured.
The trusted server group configuration in either local policy or Group Policy must be cleared.
http: //technet. microsoft. com/en-us/library/dd296901. aspx

NEW QUESTION 162
HOTSPOT - (Topic 2)
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the Network Policy Server role service installed.
An administrator creates a Network Policy Server (NPS) network policy named Policy1. You need to ensure that Policy1 applies to L2TP connections only.
Which condition should you modify?
To answer, select the appropriate object in the answer area.



Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

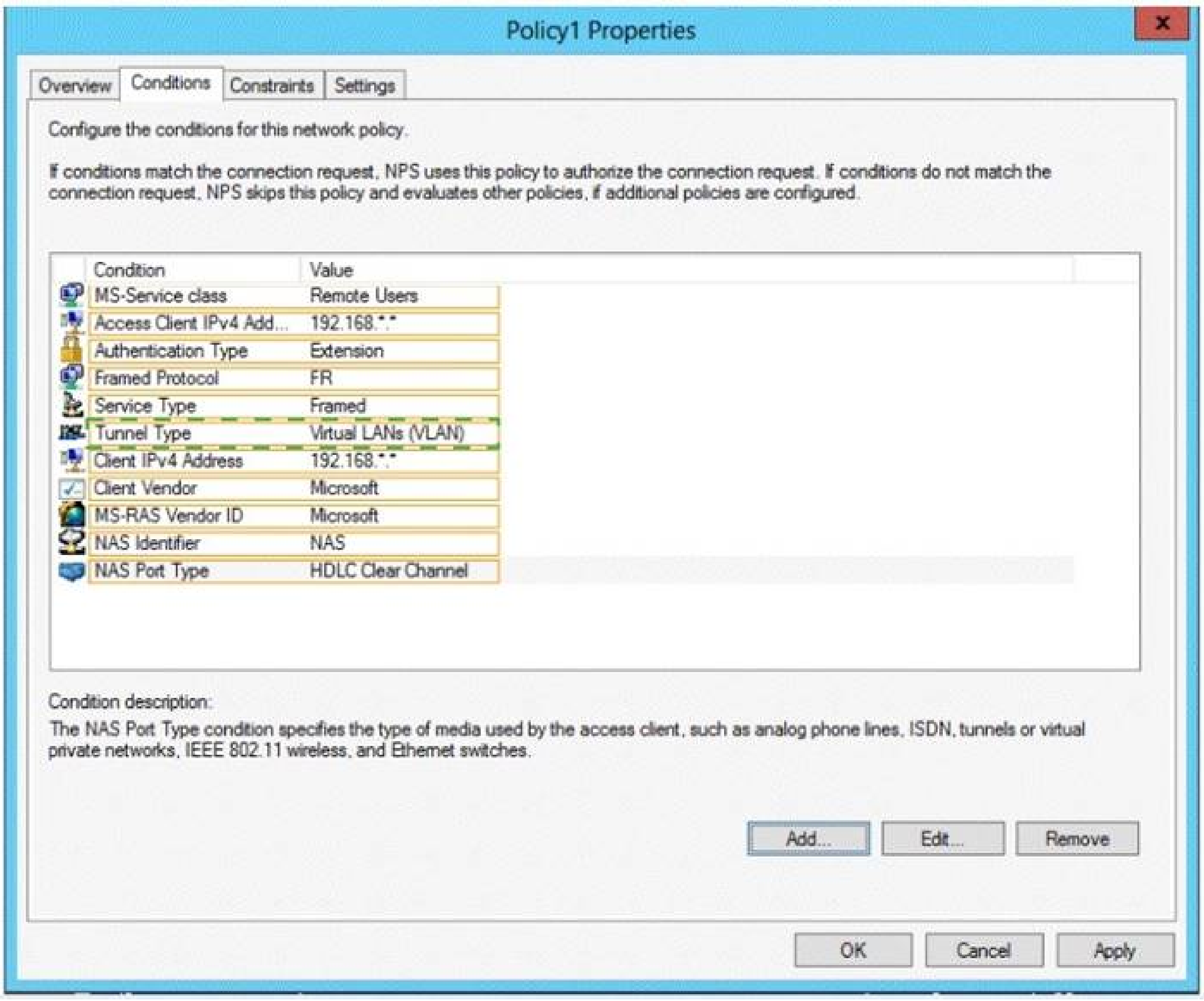
Condition	Value
MS-Service class	Remote Users
Access Client IPv4 Add...	192.168.*.*
Authentication Type	Extension
Framed Protocol	FR
Service Type	Framed
Tunnel Type	Virtual LANs (VLAN)
Client IPv4 Address	192.168.*.*
Client Vendor	Microsoft
MS-RAS Vendor ID	Microsoft
NAS Identifier	NAS
NAS Port Type	HDLC Clear Channel

Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Policy1 Properties

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
MS-Service class	Remote Users
Access Client IPv4 Add...	192.168.*.*
Authentication Type	Extension
Framed Protocol	FR
Service Type	Framed
Tunnel Type	Virtual LANs (VLAN)
Client IPv4 Address	192.168.*.*
Client Vendor	Microsoft
MS-RAS Vendor ID	Microsoft
NAS Identifier	NAS
NAS Port Type	HDLC Clear Channel

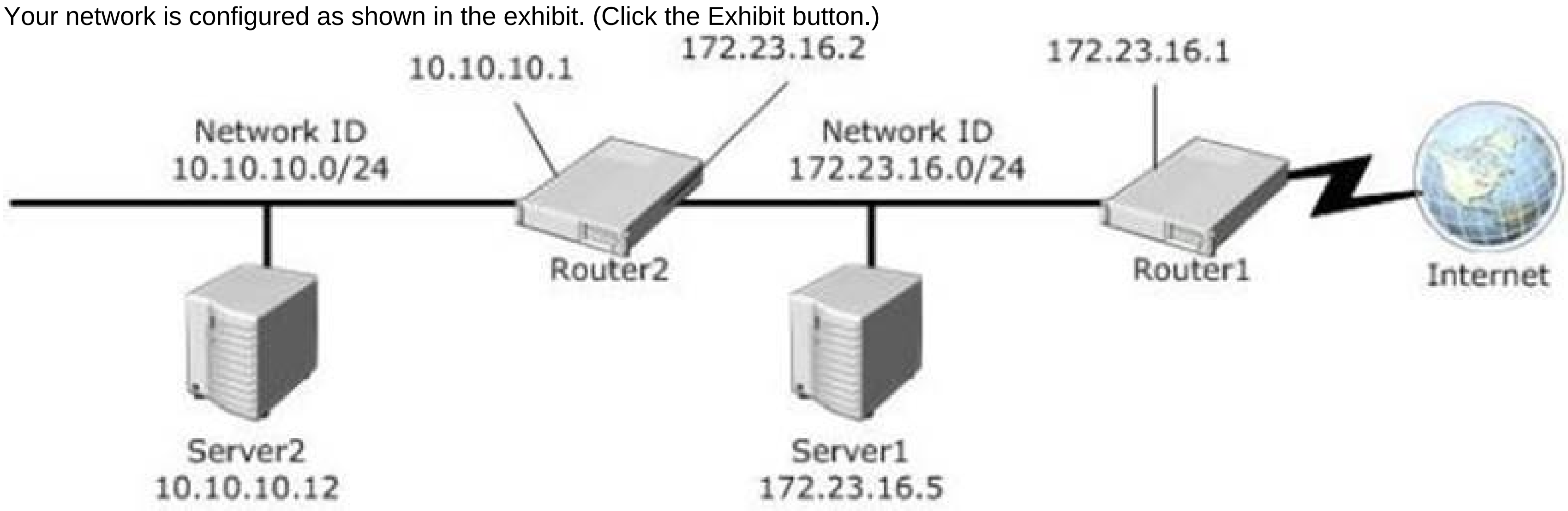
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

NEW QUESTION 165
- (Topic 3)
You deploy a Windows Server Update Services (WSUS) server named Server01.
You need to ensure that you can view update reports and computer reports on Server01.
Which two components should you install? Each correct answer presents part of the solution.

A. Microsoft XPS Viewer
B. Microsoft Report Viewer 2008 Redistributable Package
C. Microsoft SQL Server 2008 R2 Report Builder 3.0
D. Microsoft.NET Framework 2.0
E. Microsoft SQL server 2012 Reporting Services (SSRS)

Answer: BD

NEW QUESTION 168
- (Topic 3)
Your network is configured as shown in the exhibit. (Click the Exhibit button.)

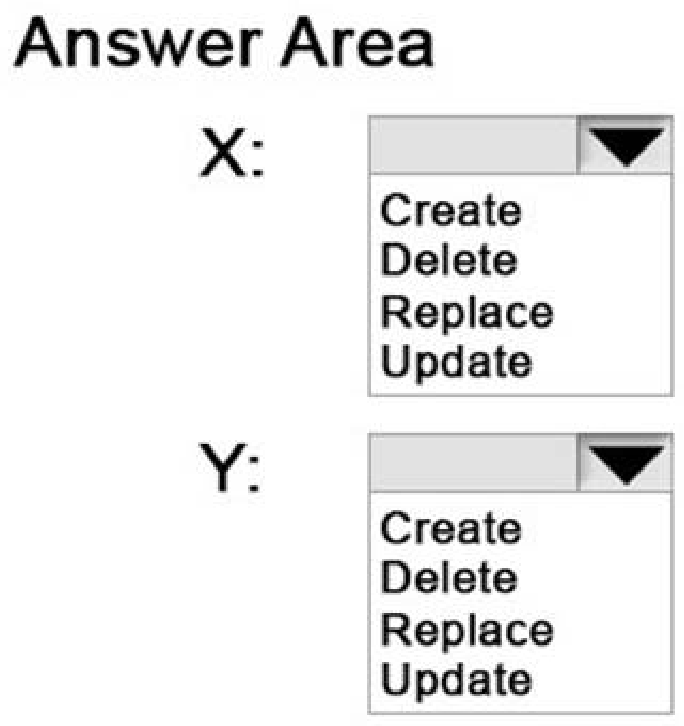


Server1 regularly accesses Server2.
You discover that all of the connections from Server1 to Server2 are routed through Routerl.
You need to optimize the connection path from Server1 to Server2. Which route command should you run on Server1?

A. Route add -p 192.168.2.0 MASK 255.255.255.0 192.168.2.1 METRIC 50
B. Route add -p 192.168.2.12 MASK 255.255.255.0 192.168.2.1 METRIC 100
C. Route add -p 192.168.2.12 MASK 255.255.255.0 192.168.2.0 METRIC 50
D. Route add -p 192.168.2.0 MASK 255.255.255.0 192.168.1.2 METRIC 100

Answer: D

NEW QUESTION 173
HOTSPOT - (Topic 3)
Your network contains one Active Directory forest named contoso.com.
All client computers for the sales department are in an organizational unit (OU) named Sales. All of the sales department computers run Windows 8.1.
You plan to use Group Policy preferences to map several drives on the sales department computers.
You need to perform the following actions:
• Create a drive mapping on all of the sales department computers for drive X. If drive X already exists, the current drive mapping should NOT be modified.
• Create a drive mapping on all of the sales department computers for drive Y. If drive Y already exists, the UNC path must be modified, but all other settings must be maintained.
Which action should you use for each drive mapping? To answer, select the appropriate options in the answer area.



Answer Area

X:
Create
Delete
Replace
Update

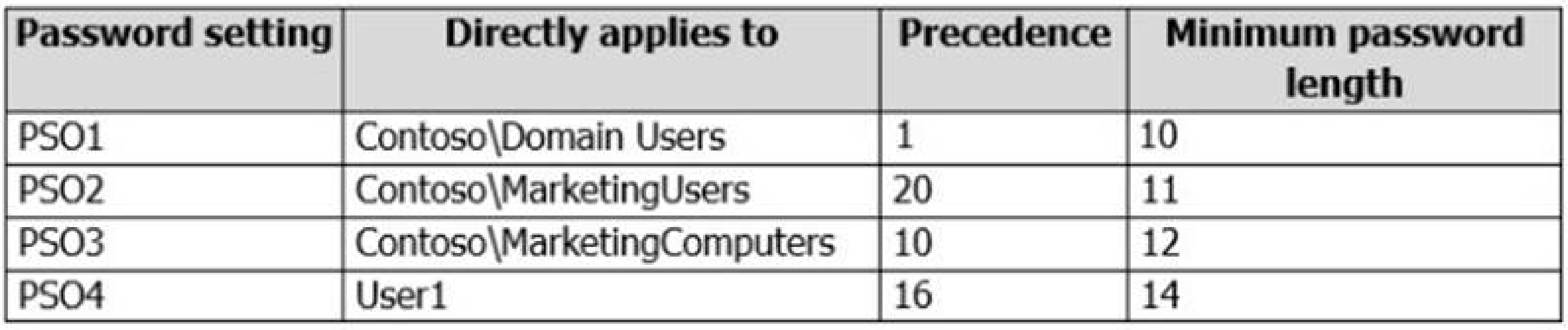
Y:
Create
Delete
Replace
Update

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Create – If a drive mapping doesn't exist for this user for the share "\shareuserDocuments", then create one. If there already is one, don't do anything! It's a kind, gentle sort of policy, it won't overwrite anything you already have, so it has a Green icon associated in the UI. Update – If that drive mapping exists, it will be updated with the settings specified here. If there are other settings associated with the drive mapping that aren't specified here, they will be maintained. If no drive mapping exists for this share, create it. https://blogs.technet.microsoft.com/grouppolicy/2009/10/26/group-policy-preferences-colorful-and-mysteriously-powerful-just-like-windows-7/

NEW QUESTION 178
- (Topic 3)
Your network contains an Active Directory forest named contoso.com. The functional level of the forest is Windows Server 2008 R2.
All of the user accounts in the marketing department are members of a group named Contoso\MarketingUsers. All of the computer accounts in the marketing department are members of a group named Contoso\MarketingComputers.
A domain user named User1 is a member of the Contoso\MarketingUsers group. A computer named Computer1 is a member of the Contoso\MarketingComputers group.
You have four Password Settings objects (PSOs). The PSOs are defined as shown in the following table.



Password setting	Directly applies to	Precedence	Minimum password length
PSO1	Contoso\Domain Users	1	10
PSO2	Contoso\MarketingUsers	20	11
PSO3	Contoso\MarketingComputers	10	12
PSO4	User1	16	14

When User1 logs on to Computer1 and attempts to change her password, she receives an error message indicating that her password is too short.
You need to tell User1 what her minimum password length is. What should you tell User1?

A. 10
B. 11
C. 12
D. 14

Answer: D

NEW QUESTION 180
- (Topic 3)
Your network contains one Active Directory domain named contoso.com. You pilot DirectAccess on the network.
During the pilot deployment, you enable DirectAccess only for a group named Contoso\Test Computers.
Once the pilot is complete, you need to enable DirectAccess for all of the client computers in the domain.

What should you do?

A. From Windows PowerShell, run the Set-DAClient cmdlet.
B. From Group Policy Management, modify the security filtering of an object named Direct Access Client Settings Group Policy.
C. From Active Directory Users and Computers, modify the membership of the Windows Authorization Access Group.
D. From Windows PowerShell, run the Set-DirectAccess cmdlet.
E. From Group Policy Management, modify the security filtering of an object named Direct Access Server Settings Group Policy.
F. From the Remote Access Management Console, run the Remote Access Server Setup wizard.
G. From Windows PowerShell, run the Set-DAServer cmdlet.

Answer: B

Explanation:
References:
https://technet.microsoft.com/en-GB/library/jj134239.aspx

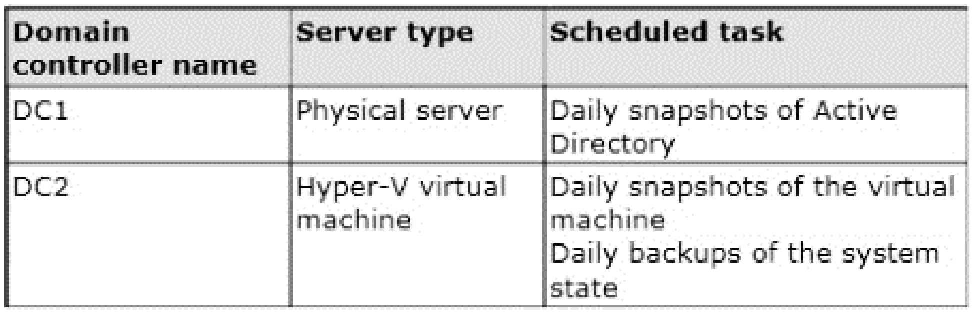
NEW QUESTION 181
- (Topic 3)
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Desktop Session Host role service installed. The computer account of Server1 resides in an organizational unit (OU) named OU1.
You create and link a Group Policy object (GPO) named GPO1 to OU1.
You need to prevent GPO1 from applying to your user account when you log on to Server1. GPO1 must apply to every other user who logs on to Server1.
What should you configure?

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

Answer: D

Explanation:
You can use item-level targeting to change the scope of individual preference items, so they apply only to selected users or computers. Within a single Group Policy object (GPO), you can include multiple preference items, each customized for selected users or computers and each targeted to apply settings only to the relevant users or computers.
Reference: https://technet.microsoft.com/en-us/library/cc733022.aspx

NEW QUESTION 185
- (Topic 3)
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012 R2.
The domain contains two domain controllers. The domain controllers are configured as shown in the following table.



Domain controller name	Server type	Scheduled task
DC1	Physical server	Daily snapshots of Active Directory
DC2	Hyper-V virtual machine	Daily snapshots of the virtual machine Daily backups of the system state

Active Directory Recycle Bin is enabled.
You discover that a support technician accidentally removed 100 users from an Active Directory group named Group1 an hour ago.
You need to restore the membership of Group1. What should you do?

A. Modify the isRecycledattribute of Group1.
B. Perform tombstone reanimation.
C. Perform a non-authoritative restore.
D. Perform an authoritative restore.

Answer: D

NEW QUESTION 186
- (Topic 3)
Your network contains one Active Directory domain named contoso.com. You pilot DirectAccess on the network.
During the pilot deployment, you enable DirectAccess only (or a group named
Contoso\Test Computers.
Once the pilot is complete, you need to enable DirectAccess for all of the client computers in the domain.
What should you do?

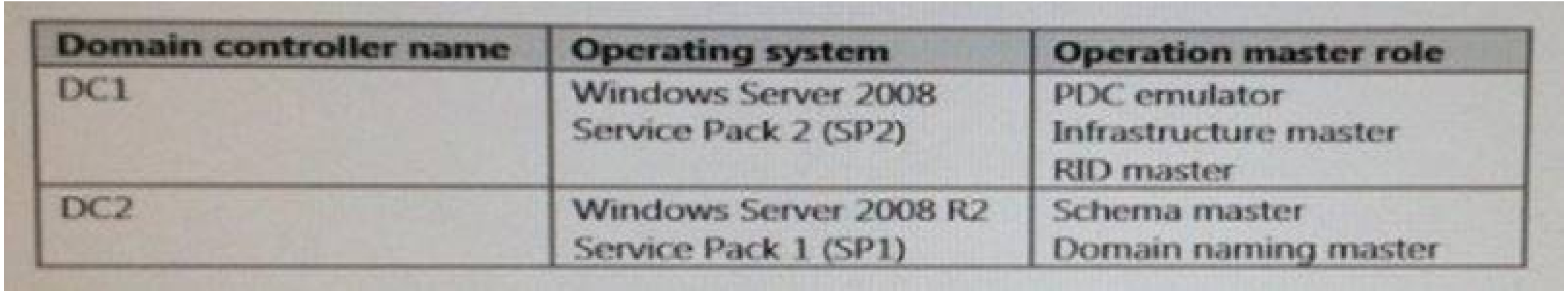
A. From Windows PowerShell, run the Set-DAServer cmdlet.
B. From Remote Access Management Console, run the remote access Server Setup wizard.
C. From Group Policy Management, modify the security filtering of an object named Direct Access Server Setting Group Policy
D. From Group Policy Management, modify the security filtering of an object named Direct Access Client Setting Group Policy.

Answer: D

Explanation:
The simplified Direct Access wizard creates two GPOs and liks them to the domain: “DirectAccess Server Settings” contains Connection Security Settings and Firewall inboud rules for Direct Access. “DirectAccess Clients Settings” sets name resolution policy for NLS validation. Both GPOs have security filtering applied,

with DirectAccess Clients Settings applied only to the DirectAccess enabled clients.
http://www.windowsecurity.com/articles-tutorials/Windows_Server_2012_Security/windows-server-2012-simplified-directaccess-wizard-overview-Part1.html

NEW QUESTION 187
- (Topic 3)
Your network contains an Active Directory domain named contoso.com. All domain controllers in the domain are configured as shown in the following table.



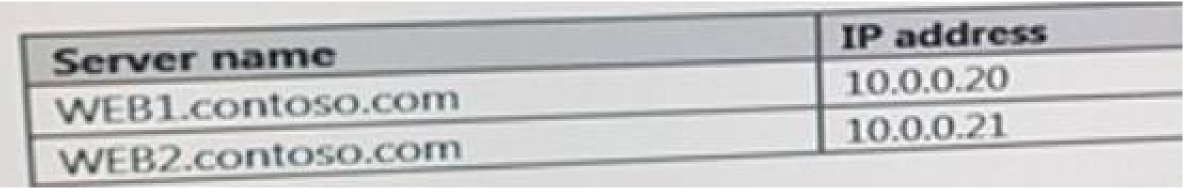
Domain controller name	Operating system	Operation master role
DC1	Windows Server 2008 Service Pack 2 (SP2)	PDC emulator Infrastructure master RID master
DC2	Windows Server 2008 R2 Service Pack 1 (SP1)	Schema master Domain naming master

You deploy a new domain controller named DC3 that runs Windows Server 2012 R2. You discover that you cannot create Password Settings objects (PSOs) by using Active Directory Administrative Center.
You need to ensure that you can create PSOs from Active Directory Administrative Center. What should you do?

A. Transfer the PDC emulator operations master role.
B. Upgrade DC1.
C. Raise the functional level of the domain.
D. Transfer the infrastructure master operations master role.

Answer: C

NEW QUESTION 188
- (Topic 3)
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 two 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

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. 2
C. 3
D. 4

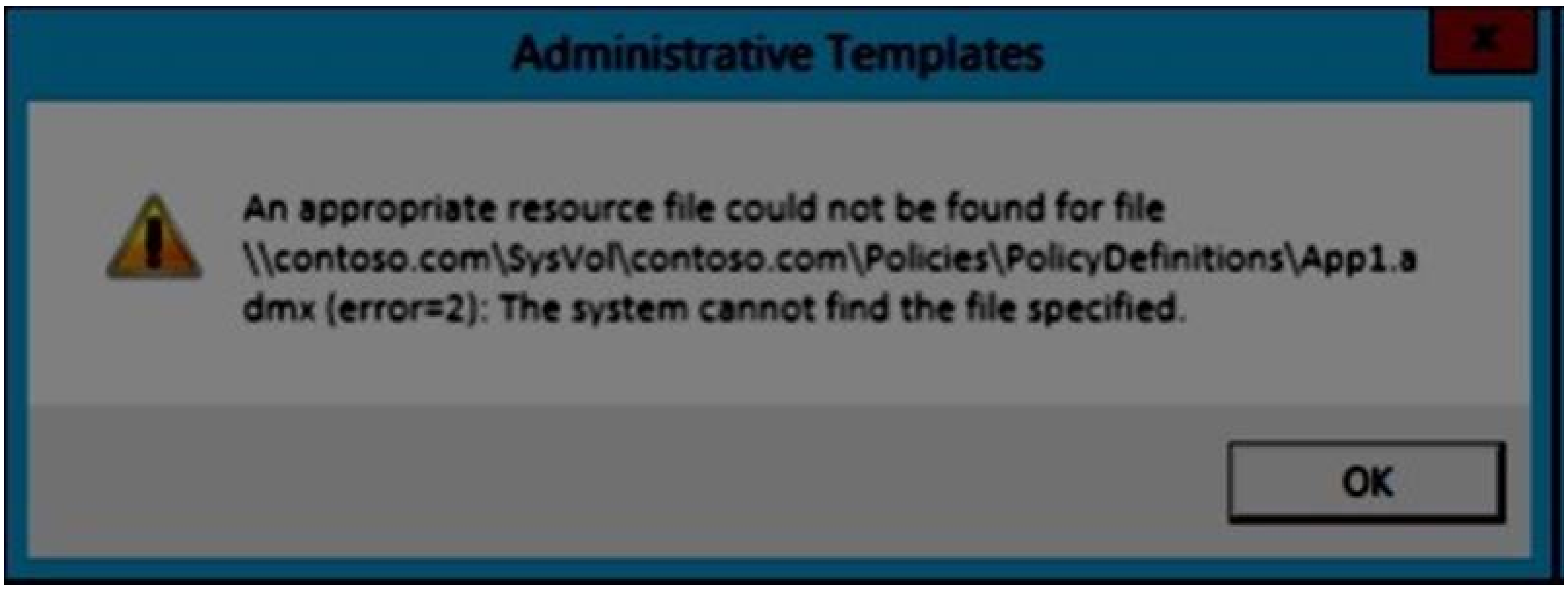
Answer: B

NEW QUESTION 192
- (Topic 3)
Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.
The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.
You need to identify which security principals are authorized to have their password cached on RODC1.
Which cmdlet should you use?

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

Answer: B

NEW QUESTION 197
- (Topic 3)
Your network contains one Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.
A central store is configured on a domain controller named DC1.
You have a custom administrative template file named App1.admx. App1.admx contains application settings for an application named App1.
You copy App1.admx to the central store. You create a new Group Policy object (GPO) named App1.Settings.
When you edit App1.Settings, you receive the warning message shown in the following exhibit.


Administrative Templates

An appropriate resource file could not be found for file \\contoso.com\SysVol\contoso.com\Policies\PolicyDefinitions\App1.admx (error=2): The system cannot find the file specified.

You need to ensure that you can edit the settings for App1 from the app1_settings GPO.

A. Modify the permissions of the ADMX file.
B. Copy an ADML file to the central store.
C. Add an administrative Template to the App1_settings GPO.
D. Move the ADMX file to the local Policy definitions folder.

Answer: B

Explanation:
This error indicates that the .adml file of Appc1.admx is not found in your central store.
Please check whether the App1.adml file exists in '\SYSVOL\domainname\Policies\PolicyDefinitions\en-us'. (en-us is for English version ADML files)
https://social.technet.microsoft.com/Forums/windowsserver/en-US/ef9d69db-3ae1-4ec3-9e21-b6398556ec15/error-in-gpmc?forum=winserverGP

NEW QUESTION 202
- (Topic 3)
You have two Windows Server Update Services (WSUS) servers named Server01 and Server02. Server01 synchronizes from Microsoft Update. Server02 synchronizes updates from Server01. Both servers are members of the same Active Directory domain.
You configure Server01 to require SSL for all WSUS metadata by using a certificate issued by an enterprise root certification authority (CA).
You need to ensure that Server02 synchronizes updates from Server01. What should you do on Server02?

A. From a command prompt, run wsusutil.exe configuresslproxy server02 443.
B. From a command prompt, run wsusutil.exe configuressl server01.
C. From a command prompt, run wsusutil.exe configuresslproxy server01 443.
D. From the Update Services console, modify the Update Source and Proxy Server options.

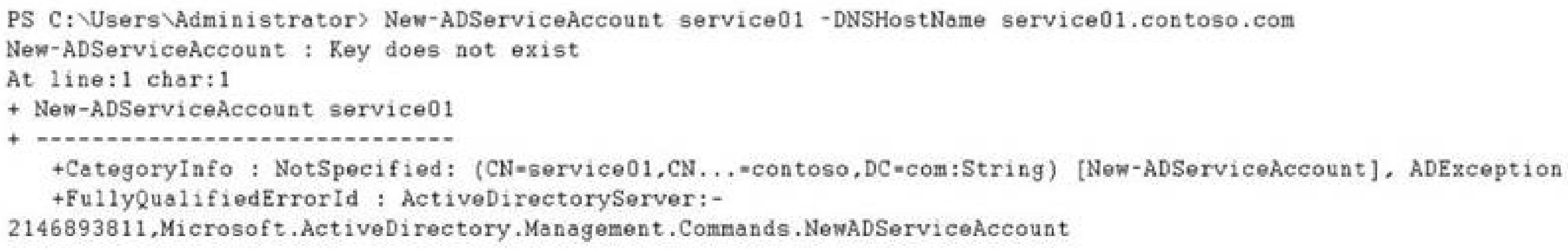
Answer: C

NEW QUESTION 207
- (Topic 3)
Your network contains one Active Directory domain named contoso.com. The domain contains a server named Server01 that runs Windows Server 2012 R2.
Server01 does not have a Trusted Platform Module (TPM).
You need to ensure that you can enable BitLocket Drive Encryption (BitLocker) on the operating system drive.
Which Group policy setting should you configure?

A. Allow network unlock at startup.
B. Enforce drive encryption type on operating system drives.
C. Allow enhanced PINs for startup.
D. Require additional authentication at startup.

Answer: A

NEW QUESTION 211
- (Topic 3)
You have the following Windows PowerShell Output.



```
PS C:\Users\Administrator> New-ADServiceAccount service01 -DNSHostName service01.contoso.com
New-ADServiceAccount : Key does not exist
At line:1 char:1
+ New-ADServiceAccount service01
+ ------------------------------
   +CategoryInfo : NotSpecified: (CN=service01,CN...=contoso,DC=com:String) [New-ADServiceAccount], ADException
   +FullyQualifiedErrorId : ActiveDirectoryServer:-
2146893811,Microsoft.ActiveDirectory.Management.Commands.NewADServiceAccount
```

You need to create a Managed Service Account. What should you do?

A. Run New-ADServiceAccount –Name “service01” –DNSHostName service01.contoso.com –SAMAccountName service01.
B. Run New-AuthenticationPolicySilo, and then run New-ADServiceAccount –Name “service01” –DNSHostName service01.contoso.com.
C. Run Add-KDSRootKey, and then run New-ADServiceAccount –Name “service01”–DNSHostName service01.contoso.com.
D. Run Set-KDSConfiguration, and then run New-ADServiceAccount –Name “service01” –DNSHostName service01.contoso.com.

Answer: C

Explanation:
From the exhibit we see that the required key does not exist. First we create this key, then we create the managed service account.
The Add-KdsRootKey cmdlet generates a new root key for the Microsoft Group Key Distribution Service (KdsSvc) within Active Directory (AD). The Microsoft Group KdsSvc generates new group keys from the new root key.
The New-ADServiceAccount cmdlet creates a new Active Directory managed service account.
Reference: New-ADServiceAccount
https://technet.microsoft.com/en-us/library/hh852236(v=wps.630).aspx
Reference: Add-KdsRootKey
ttps://technet.microsoft.com/en-us/library/jj852117(v=wps.630).aspx

NEW QUESTION 213
......