



Microsoft

Exam Questions 70-411

Administering Windows Server 2012

NEW QUESTION 1

- (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 2

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.

The domain contains a server named Server1 that has the Network Policy Server server role and the Remote Access server role installed. The domain contains a server named Server2 that is configured as a RADIUS server.

Server1 provides VPN access to external users.

You need to ensure that all of the VPN connections to Server1 are logged to the RADIUS server on Server2.

What should you run?

- A. Add-RemoteAccessRadius -ServerNameServer1 -AccountingOnOffMsg Enabled - SharedSecret "Secret" -Purpose Accounting
- B. Set-RemoteAccessAccounting -AccountingOnOffMsg Enabled -AccountingOnOffMsg Enabled
- C. Add-RemoteAccessRadius -ServerName Server2 -AccountingOnOffMsg Enabled - SharedSecret "Secret" -Purpose Accounting
- D. Set-RemoteAccessAccounting -EnableAccountingType Inbox -AccountingOnOffMsg Enabled

Answer: C

Explanation:

Add-RemoteAccessRadius

Adds a new external RADIUS server for VPN authentication, accounting for DirectAccess (DA) and VPN, or one-time password (OTP) authentication for DA.

AccountingOnOffMsg<String>

Indicates the enabled state for sending of accounting on or off messages. The acceptable values for this parameter are:

? Enabled.

? Disabled. This is the default value.

This parameter is applicable only when the RADIUS server is being added for Remote Access accounting.

NEW QUESTION 3

- (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.

A local account named Admin1 is a member of the Administrators group on Server1.

You need to generate an audit event whenever Admin1 is denied access to a file or folder. What should you run?

- A. auditpol.exe /set /userradmin1 /failure: enable
- B. auditpol.exe /set /user: admin1 /category: "detailed tracking" /failure: enable
- C. auditpol.exe /resourcesacl /set /type: file /user: admin1 /failure
- D. auditpol.exe /resourcesacl /set /type: key /user: admin1 /failure /access: ga

Answer: C

Explanation:

<http://technet.microsoft.com/en-us/library/ff625687.aspx>

To set a global resource SACL to audit successful and failed attempts by a user to perform generic read and write functions on files or folders:

auditpol /resourceSACL /set /type: File /user: MYDOMAINmyuser /success /failure /access: FRFW

<http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx> Syntax

auditpol /resourceSACL

[/set /type: <resource> [/success] [/failure] /user: <user> [/access: <access flags>]] [/remove /type: <resource> /user: <user> [/type: <resource>]]

[/clear [/type: <resource>]]

[/view [/user: <user>] [/type: <resource>]]

References:

<http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/ff625687.aspx>

<http://technet.microsoft.com/en-us/library/ff625687.aspx>

<http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx>

NEW QUESTION 4

- (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.

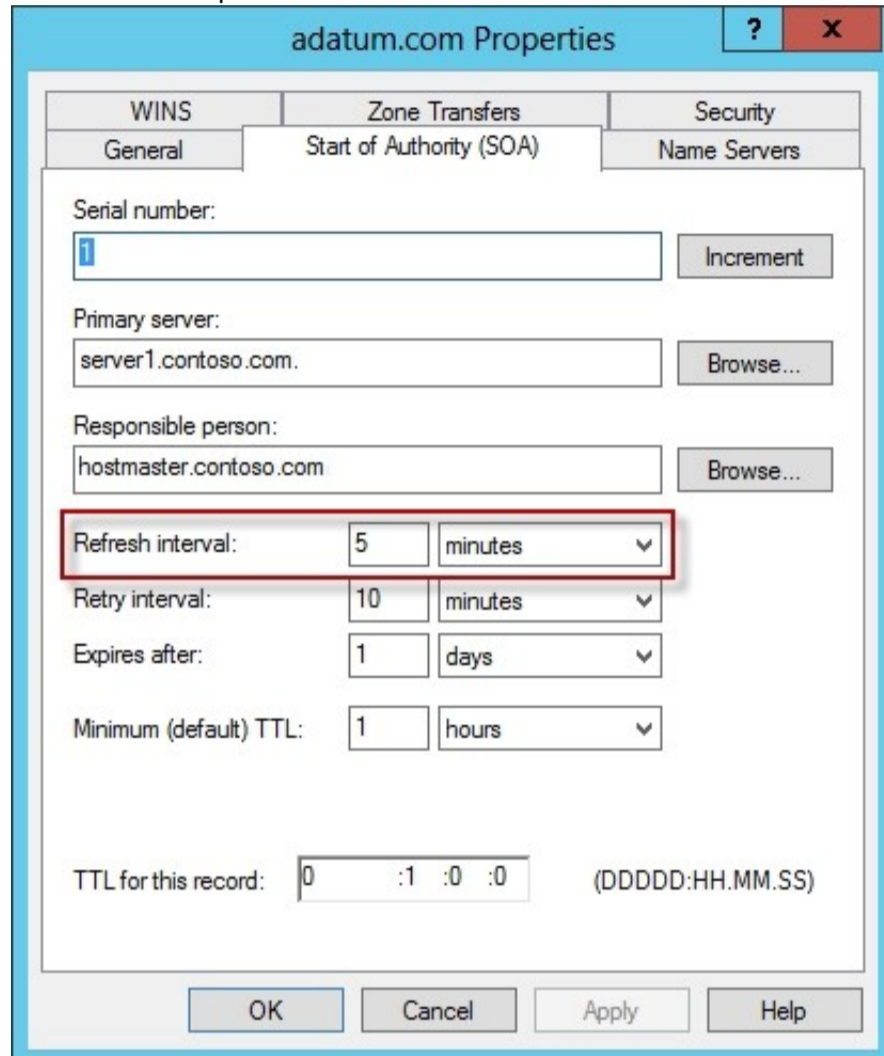
Which setting should you modify in the start of authority (SOA) record?

- 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.



NEW QUESTION 5

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 P.2. Server1 has the Network Policy and Access Services server role installed.

You plan to deploy 802.1x authentication to secure the wireless network.

You need to identify which Network Policy Server (NPS) authentication method supports certificate-based mutual authentication for the 802.1x deployment.

Which authentication method should you identify?

- A. MS-CHAP
- B. PEAP-MS-CHAPv2
- C. EAP-TLS
- D. MS-CHAP v2

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.

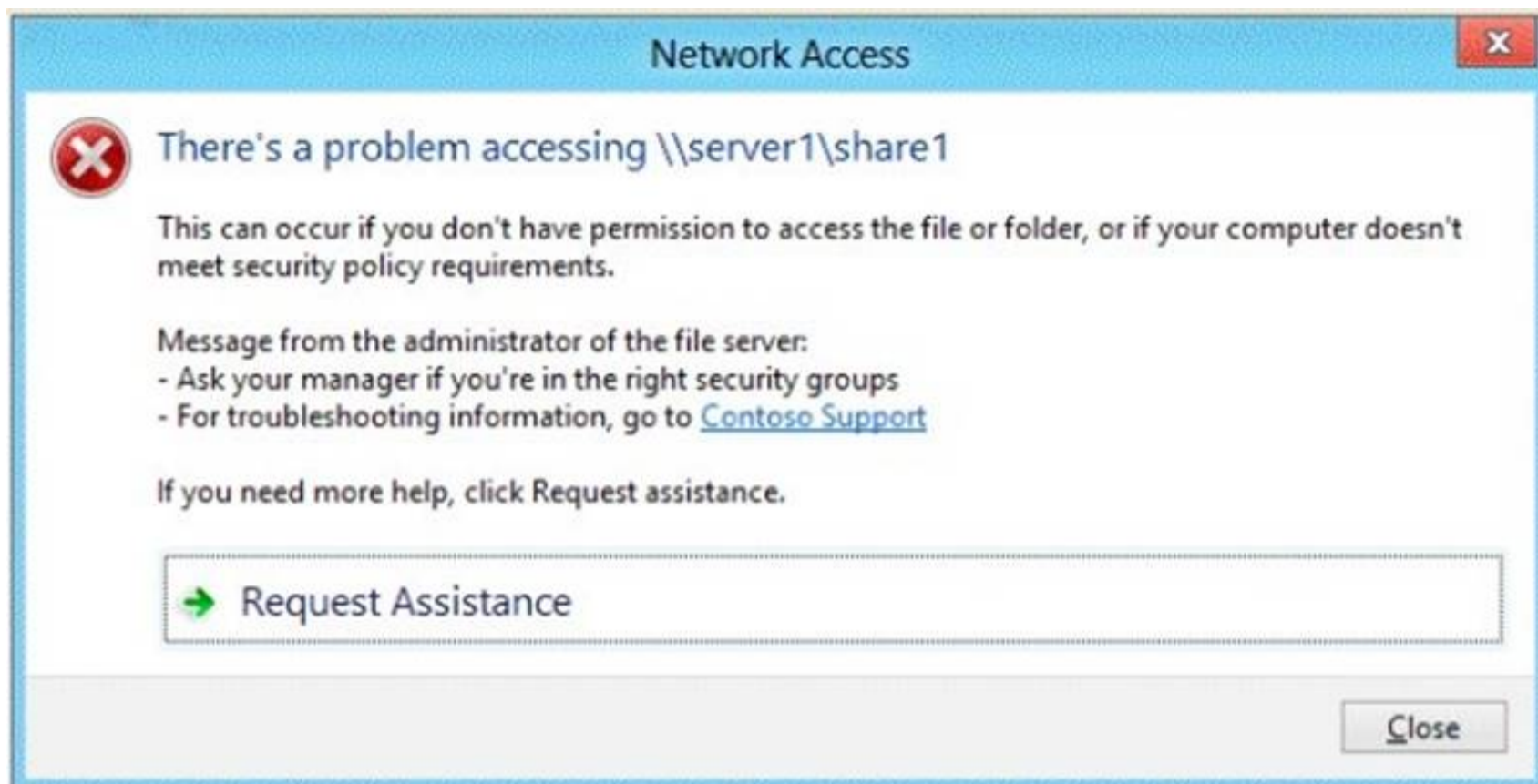
NEW QUESTION 6

- (Topic 1)

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

Server1 has a share named Share1.

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



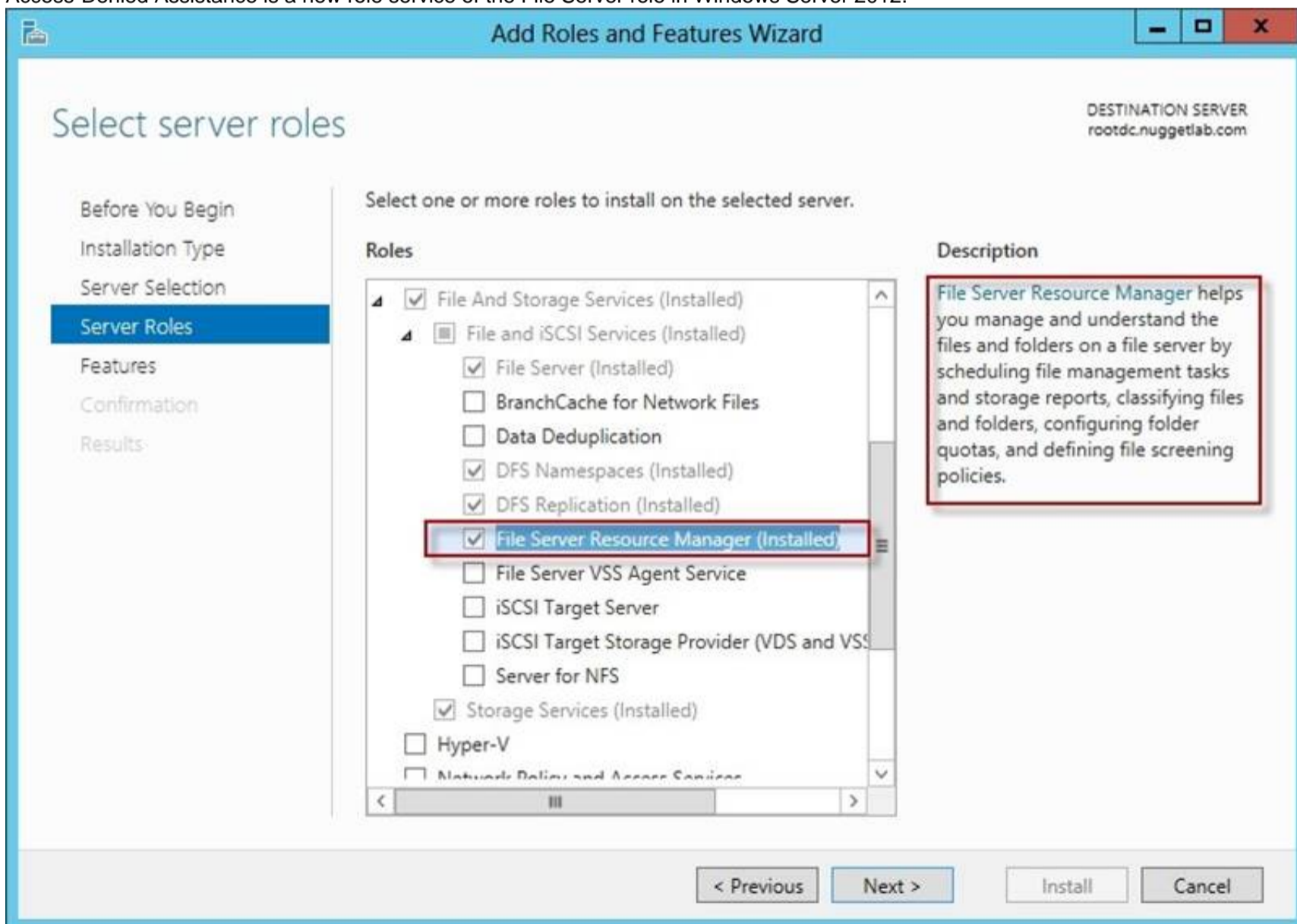
You deploy a new file server named Server2 that runs Windows Server 2012 R2.
 You need to configure Server2 to display the same custom Access Denied message as Server1.
 What should you install on Server2?

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

Answer: C

Explanation:

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



We need to install the prerequisites for Access-Denied Assistance.

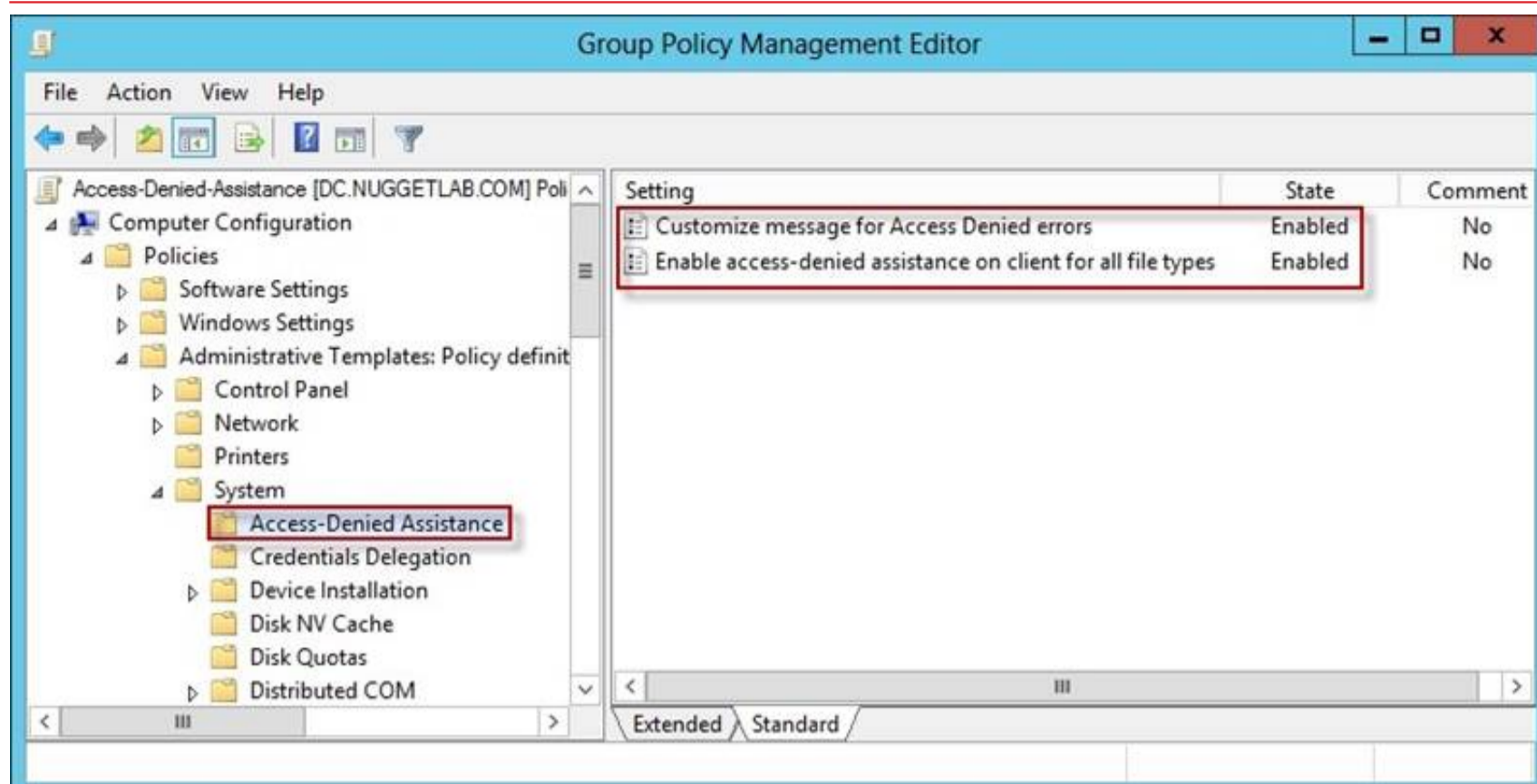
Because Access-Denied Assistance relies up on e-mail notifications, we also need to configure each relevant file server with a Simple Mail Transfer Protocol (SMTP) server address. Let's do that quickly with Windows PowerShell:

```
Set-FSRMSetting -SMTPServer mailserver.nuggetlab.com -AdminEmailAddress admingroup@nuggetlab.com -FromEmailAddress admingroup@nuggetlab.com
```

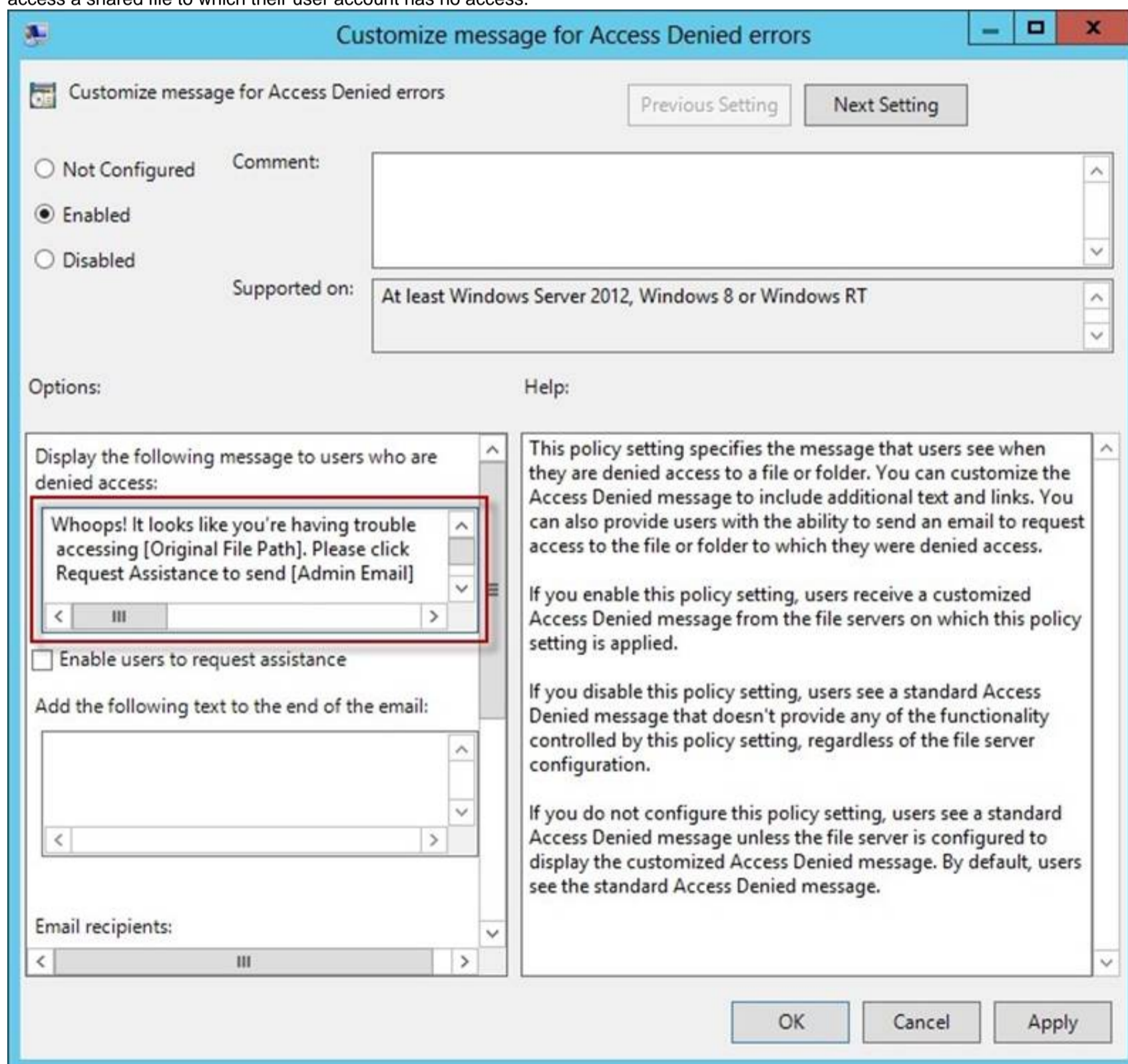
You can enable Access-Denied Assistance either on a per-server basis or centrally via Group Policy. To my mind, the latter approach is infinitely preferable from an administration standpoint.

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

\Computer Configuration\Policies\Administrative Templates\System\Access-Denied Assistance



The Customize message for Access Denied errors policy, shown in the screenshot below, enables us to create the actual message box shown to users when they access a shared file to which their user account has no access.



What's cool about this policy is that we can "personalize" the e-mail notifications to give us administrators (and, optionally, file owners) the details they need to resolve the permissions issue quickly and easily.

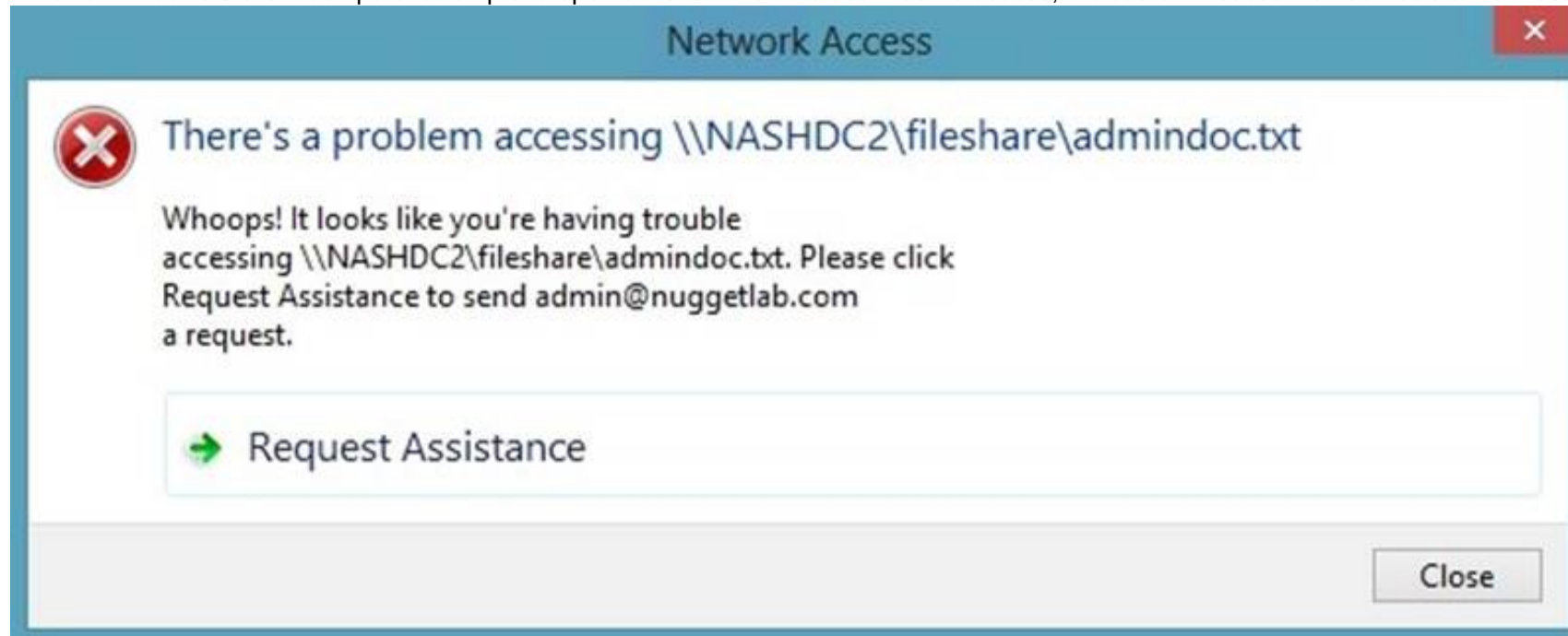
For instance, we can insert pre-defined macros to swap in the full path to the target file, the administrator e-mail address, and so forth. See this example: Whoops! It looks like you're having trouble accessing [Original File Path]. Please click Request Assistance to send [Admin Email] a help request e-mail message. Thanks!

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

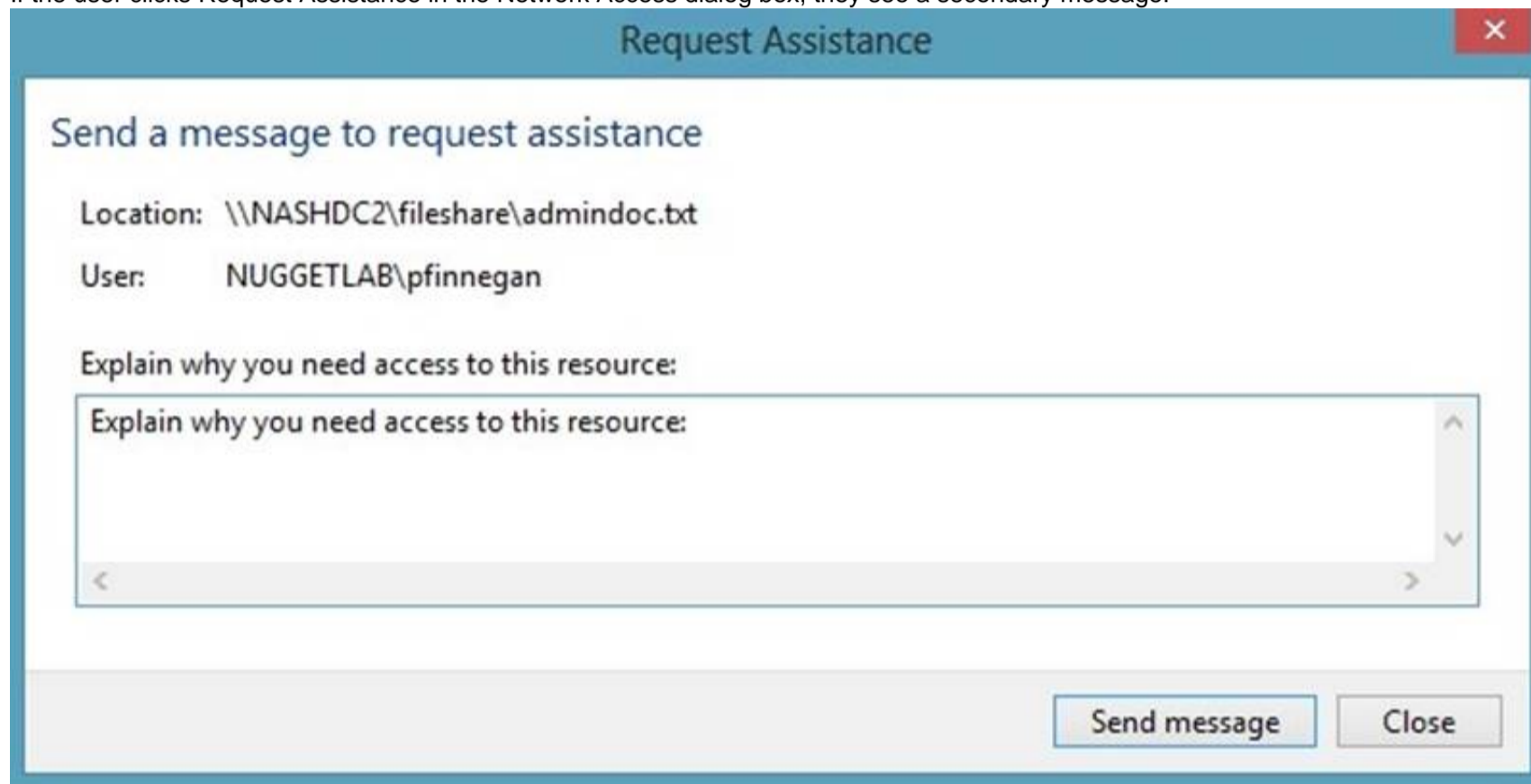
The Enable access-denied assistance on client for all file types policy should be enabled to force client computers to participate in Access-Denied Assistance. Again, you must make sure to target your GPO scope accordingly to "hit" your domain workstations as well as your Windows Server 2012 file servers.

Testing the configuration

This should come as no surprise to you, but Access-Denied Assistance works only with Windows Server 2012 and Windows 8 computers. More specifically, you must enable the Desktop Experience feature on your servers to see Access-Denied Assistance messages on server computers. When a Windows 8 client computer attempts to open a file to which the user has no access, the custom Access-Denied Assistance message should appear:



If the user clicks Request Assistance in the Network Access dialog box, they see a secondary message:



At the end of this process, the administrator(s) will receive an e-mail message that contains the key information they need in order to resolve the access problem:
 The user's Active Directory identity
 The full path to the problematic file
 A user-generated explanation of the problem
 So that's it, friends! Access-Denied Assistance presents Windows systems administrators with an easy-to-manage method for more efficiently resolving user access problems on shared file system resources. Of course, the key caveat is that your file servers must run Windows Server 2012 and your client devices must run Windows 8, but other than that, this is a great technology that should save admins extra work and end-users extra headaches.
 Reference: <http://4sysops.com/archives/access-denied-assistance-in-windows-server-2012/>

NEW QUESTION 7

- (Topic 1)

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

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

Answer: B

Explanation:

RADIUS client properties

Following are the RADIUS client conditions that you can configure in network policy.

? Calling Station ID: Specifies the network access server telephone number that was dialed by the dial-up access client.

? Client Friendly Name: Specifies the name of the RADIUS client that forwarded the connection request to the NPS server.

? Client IPv4 Address: Specifies the Internet Protocol (IP) version 4 address of the RADIUS client that forwarded the connection request to the NPS server.

? Client IPv6 Address: Specifies the Internet Protocol (IP) version 6 address of the RADIUS client that forwarded the connection request to the NPS server.

? Client Vendor: Specifies the name of the vendor or manufacturer of the RADIUS client that sends connection requests to the NPS server.

? MS RAS Vendor: Specifies the vendor identification number of the network access server that is requesting authentication.

NEW QUESTION 8

- (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 following role services installed:

? DirectAccess and VPN (RRAS)

? Network Policy Server

Remote users have client computers that run either Windows XP, Windows 7, or Windows 8.

You need to ensure that only the client computers that run Windows 7 or Windows 8 can establish VPN connections to Server1.

What should you configure on Server1?

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

Answer: A

Explanation:

If you want to configure the Operating System condition, click Operating System, and then click Add. In Operating System Properties, click Add, and then specify the operating system settings that are required to match the policy.

The Operating System condition specifies the operating system (operating system version or service pack number), role (client or server), and architecture (x86, x64, or ia64) required for the computer configuration to match the policy.

NEW QUESTION 9

- (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 /Domain:contoso.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/cc785343(v=WS.10).aspx) <http://technet.microsoft.com/en-us/library/cc733107.aspx>

NEW QUESTION 10

HOTSPOT - (Topic 1)

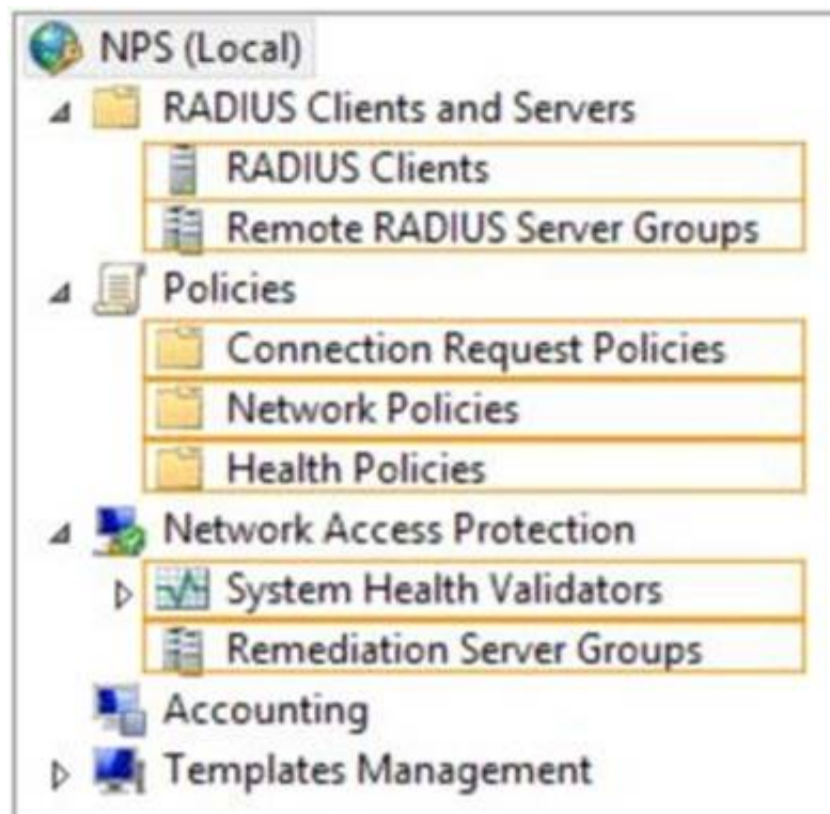
Your network contains a RADIUS server named Server1.

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.

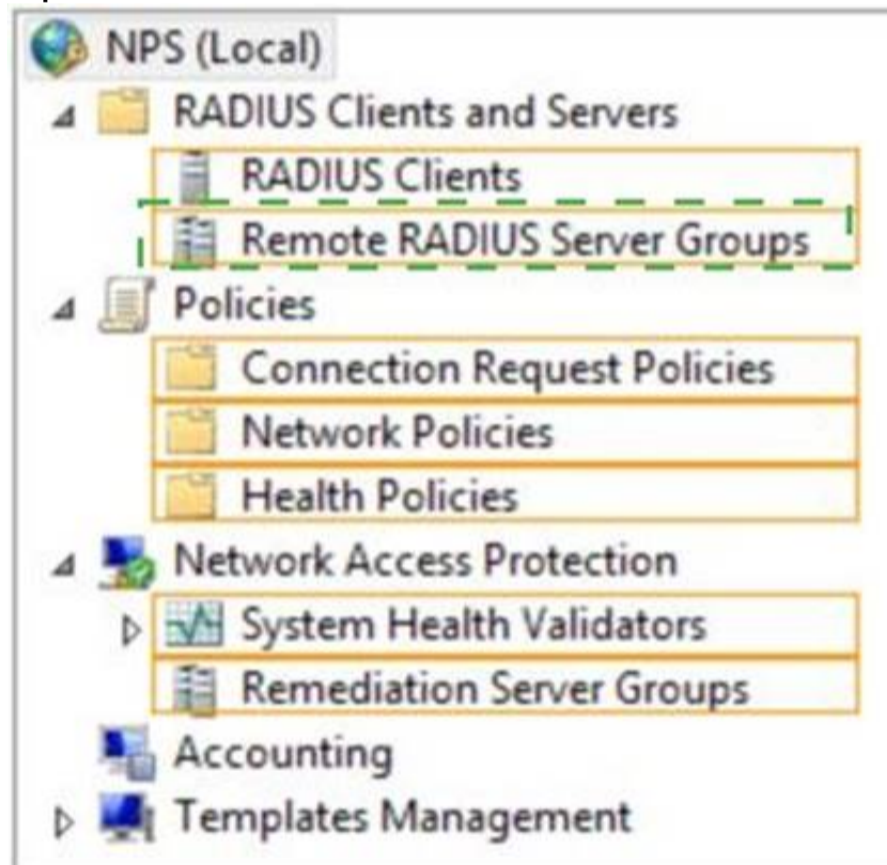
What else should you configure on Server2? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 10

- (Topic 1)

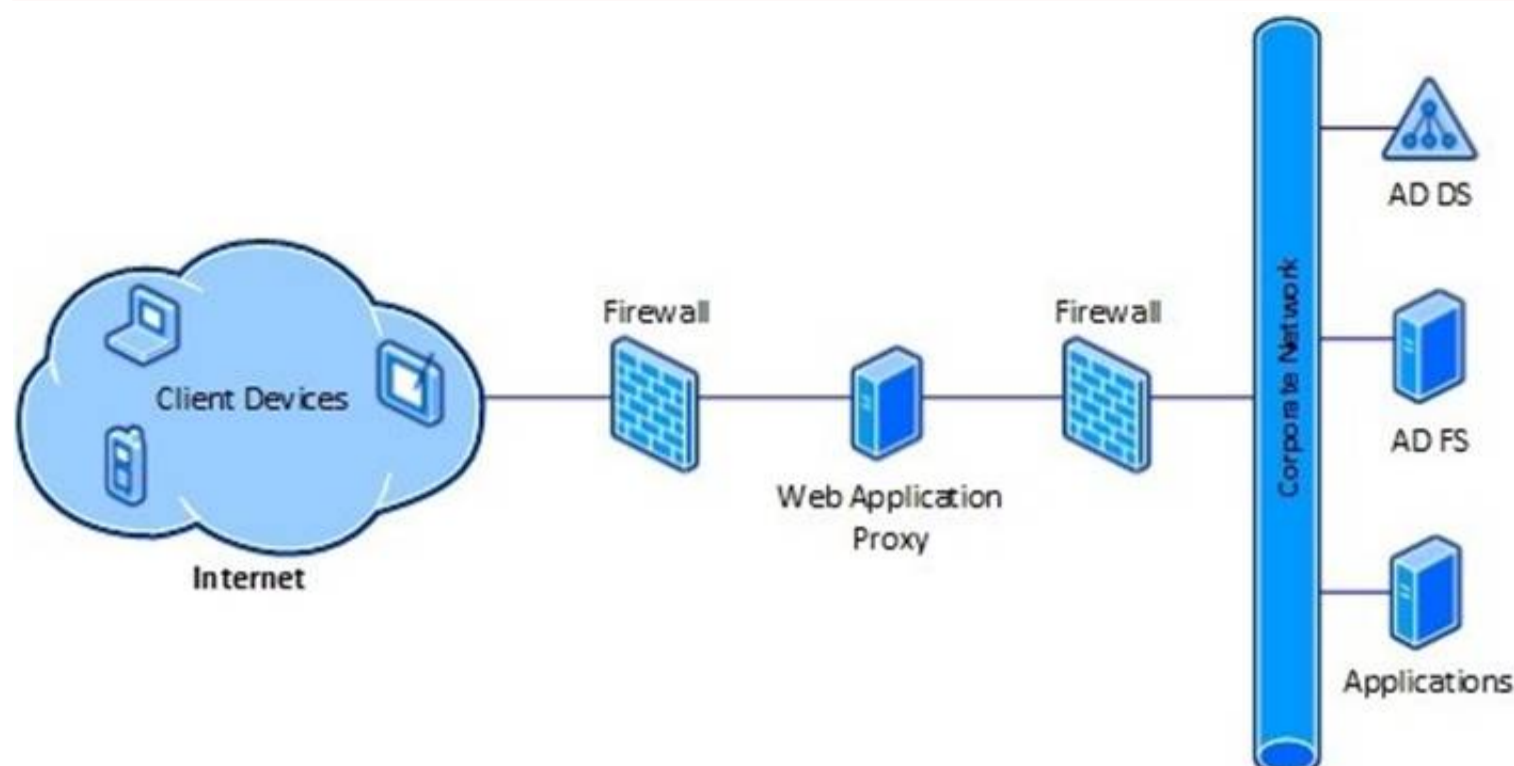
Your network contains an Active Directory domain named contoso.com. You need to install and configure the Web Application Proxy role service. What should you do?

- A. Install the Active Directory Federation Services server role and the Remote Access server role on different servers.
- B. Install the Active Directory Federation Services server role and the Remote Access server role on the same server.
- C. Install the Web Server (IIS) server role and the Application Server server role on the same server.
- D. Install the Web Server (IIS) server role and the Application Server server role on different servers.

Answer: A

Explanation:

Web Application Proxy is a new Remote Access role service in Windows Server® 2012 R2.



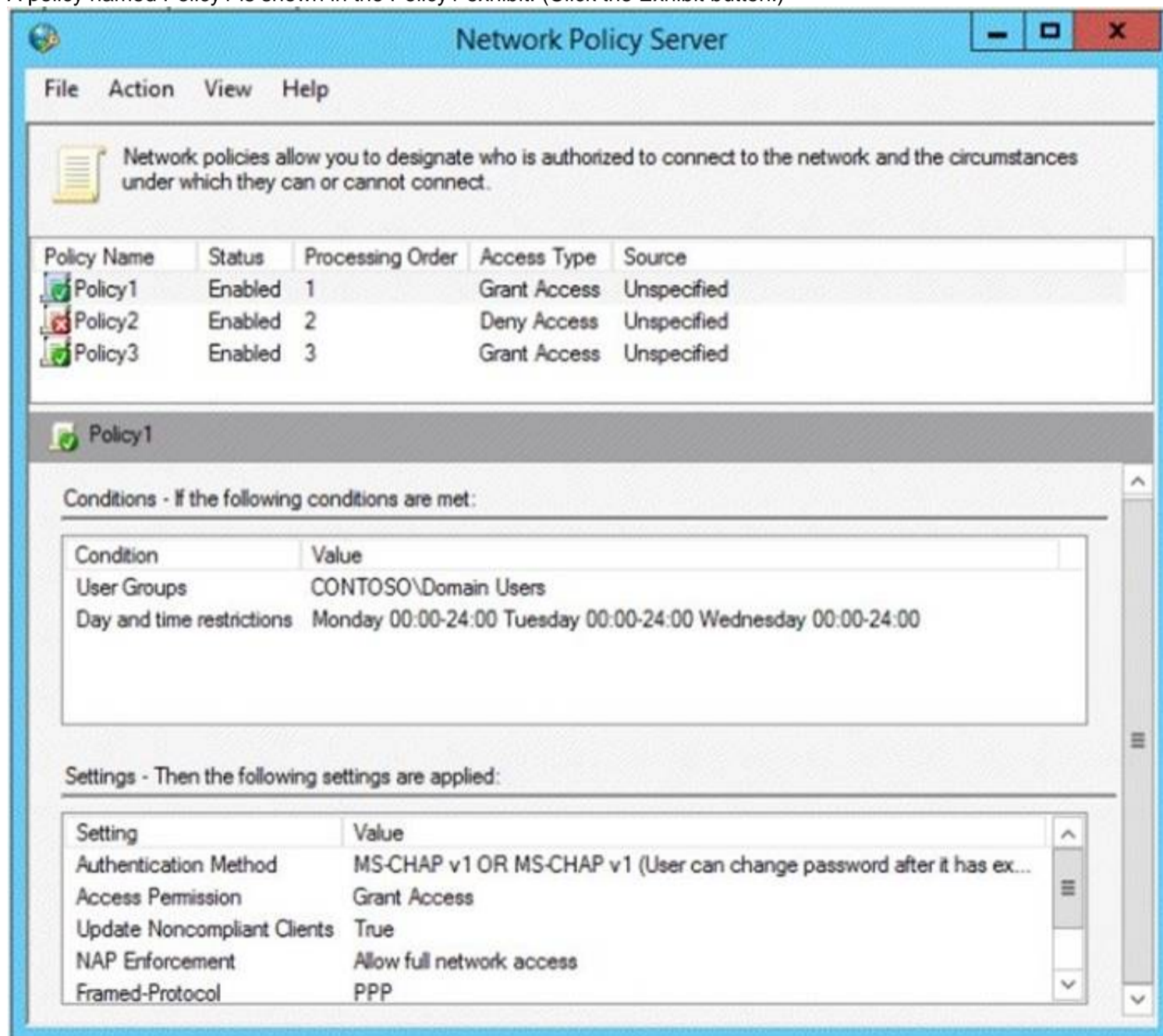
NEW QUESTION 11

HOTSPOT - (Topic 1)

Your network contains an Active Directory named contoso.com. You have users named User1 and user2.

The Network Access Permission for User1 is set to Control access through NPS Network Policy. The Network Access Permission for User2 is set to Allow access.

A policy named Policy1 is shown in the Policy1 exhibit. (Click the Exhibit button.)



Network Policy Server

File Action View Help

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

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

Policy1

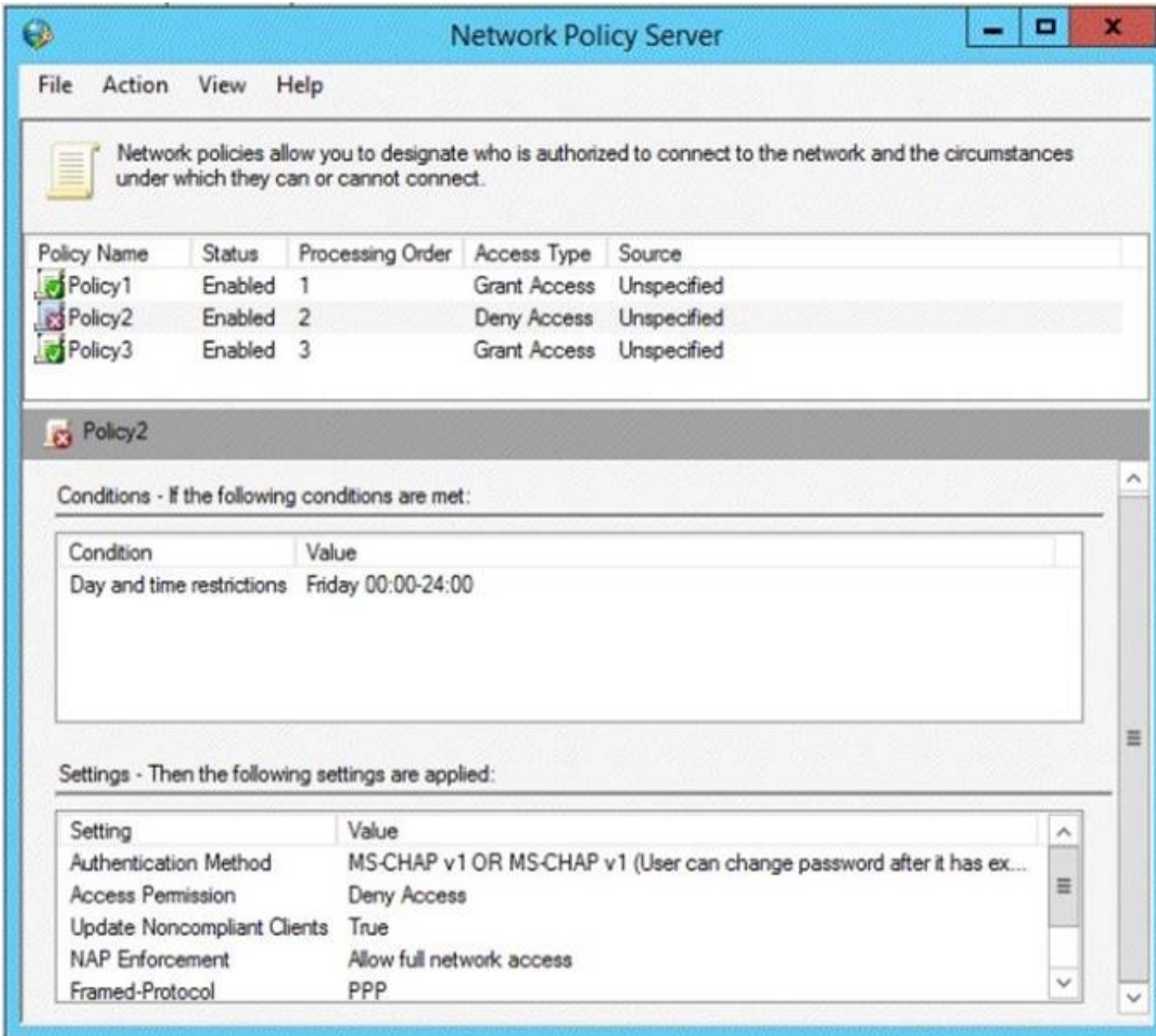
Conditions - If the following conditions are met:

Condition	Value
User Groups	CONTOSO\Domain Users
Day and time restrictions	Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00

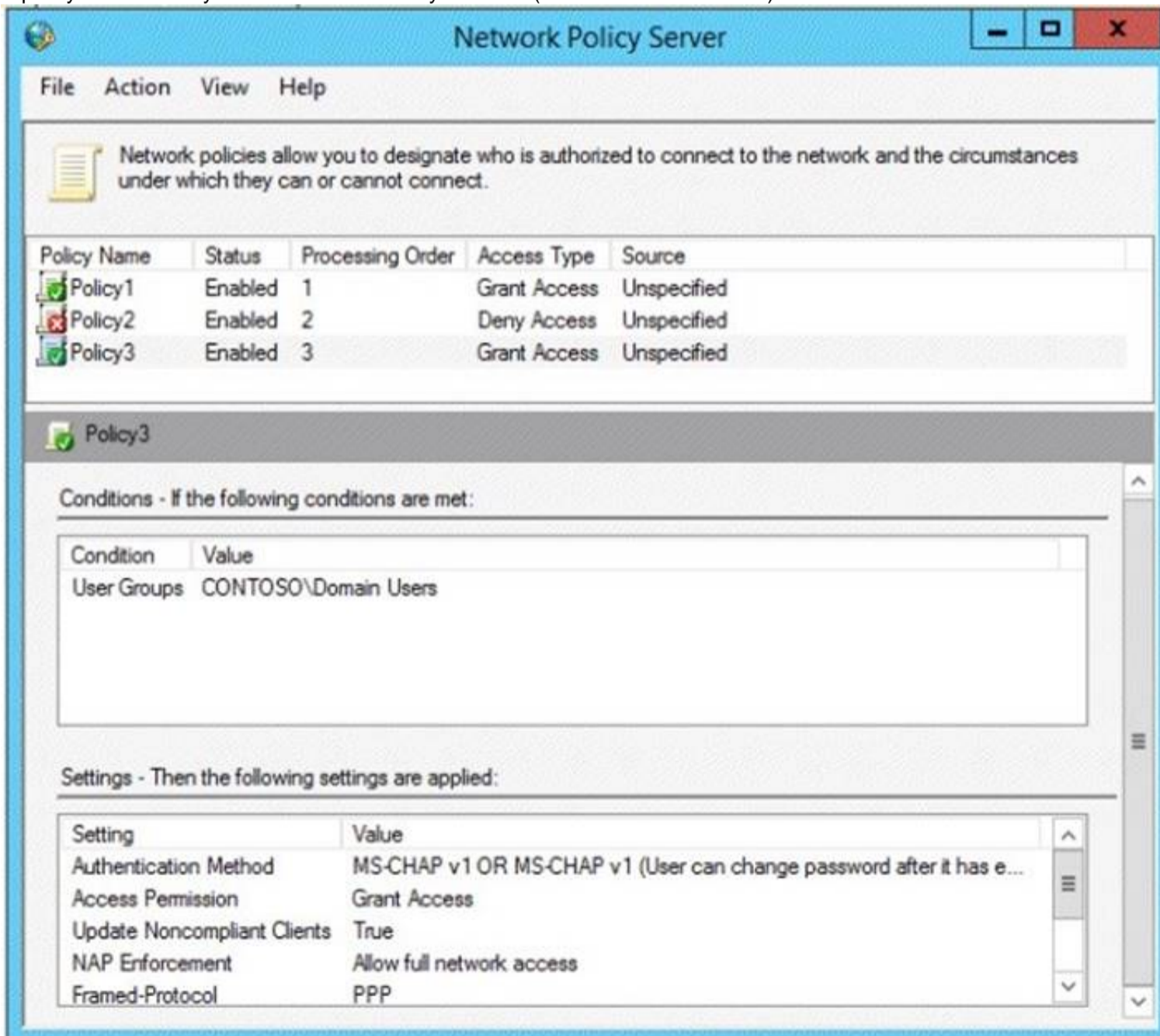
Settings - Then the following settings are applied:

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

A policy named Policy2 is shown in the Policy2 exhibit. (Click the Exhibit button.)



A policy named Policy3 is shown in the Policy3 exhibit. (Click the Exhibit button.)



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

	Yes	No
User1 will be able to establish a VPN connection on Thursday.	<input type="radio"/>	<input type="radio"/>
User1 will be able to establish a VPN connection on Friday.	<input type="radio"/>	<input type="radio"/>
User2 will be able to establish a VPN connection on Friday.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

	Yes	No
User1 will be able to establish a VPN connection on Thursday.	<input checked="" type="radio"/>	<input type="radio"/>
User1 will be able to establish a VPN connection on Friday.	<input type="radio"/>	<input checked="" type="radio"/>
User2 will be able to establish a VPN connection on Friday.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 16

HOTSPOT - (Topic 1)

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

User name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

To answer, select the appropriate policy for each user in the answer area.

Answer Area

User1:

User2:

User3:

Answer Area

User1:
Policy1
Policy2
Policy3

User2:
Policy1
Policy2
Policy3

User3:
Policy1
Policy2
Policy3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

When you configure multiple network policies in NPS, the policies are an ordered list of rules. NPS evaluates the policies in listed order from first to last. If there is a network policy that matches the connection request, NPS uses the policy to determine whether to grant or deny access to the user or computer connection. Network policies are evaluated according to the processing order. Once a match is found, no further network policy is processed.

Policies are processed in this order:

-Policy2 (applies only to members of Group1)

-Policy1 (applies to all users during specified time slot)

-Policy3 (applies only to members of Group2)

Since policy1 will always apply (sunday 0:00 to saturday 24:00 = always), policy3 will never be evaluated.

Correct answer is : User1: Policy2 User2: Policy1 User3: Policy1

[https://technet.microsoft.com/en-us/library/cc732724\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732724(v=ws.10).aspx)

NEW QUESTION 20

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All domain controllers run either Windows Server 2008 or Windows Server 2008 R2.

You deploy a new domain controller named DC1 that runs Windows Server 2012 R2. You log on to DC1 by using an account that is a member of the Domain Admins group. 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. Modify the membership of the Group Policy Creator Owners group.
- B. Transfer the PDC emulator operations master role to DC1.
- C. Upgrade all of the domain controllers that run Window Server 2008.
- D. Raise the functional level of the domain.

Answer: D

Explanation:

Fine-grained password policies allow you to specify multiple password policies within a single domain so that you can apply different restrictions for password and account lockout policies to different sets of users in a domain. To use a fine-grained password policy, your domain functional level must be at least Windows Server 2008. To enable fine-grained password policies, you first create a Password Settings Object (PSO). You then configure the same settings that you configure for the password and account lockout policies. You can create and apply PSOs in the Windows Server 2012 environment by using the Active Directory Administrative Center (ADAC) or Windows PowerShell.

Step 1: Create a PSO

Applies To: Windows Server 2008, Windows Server 2008 R2

ce:

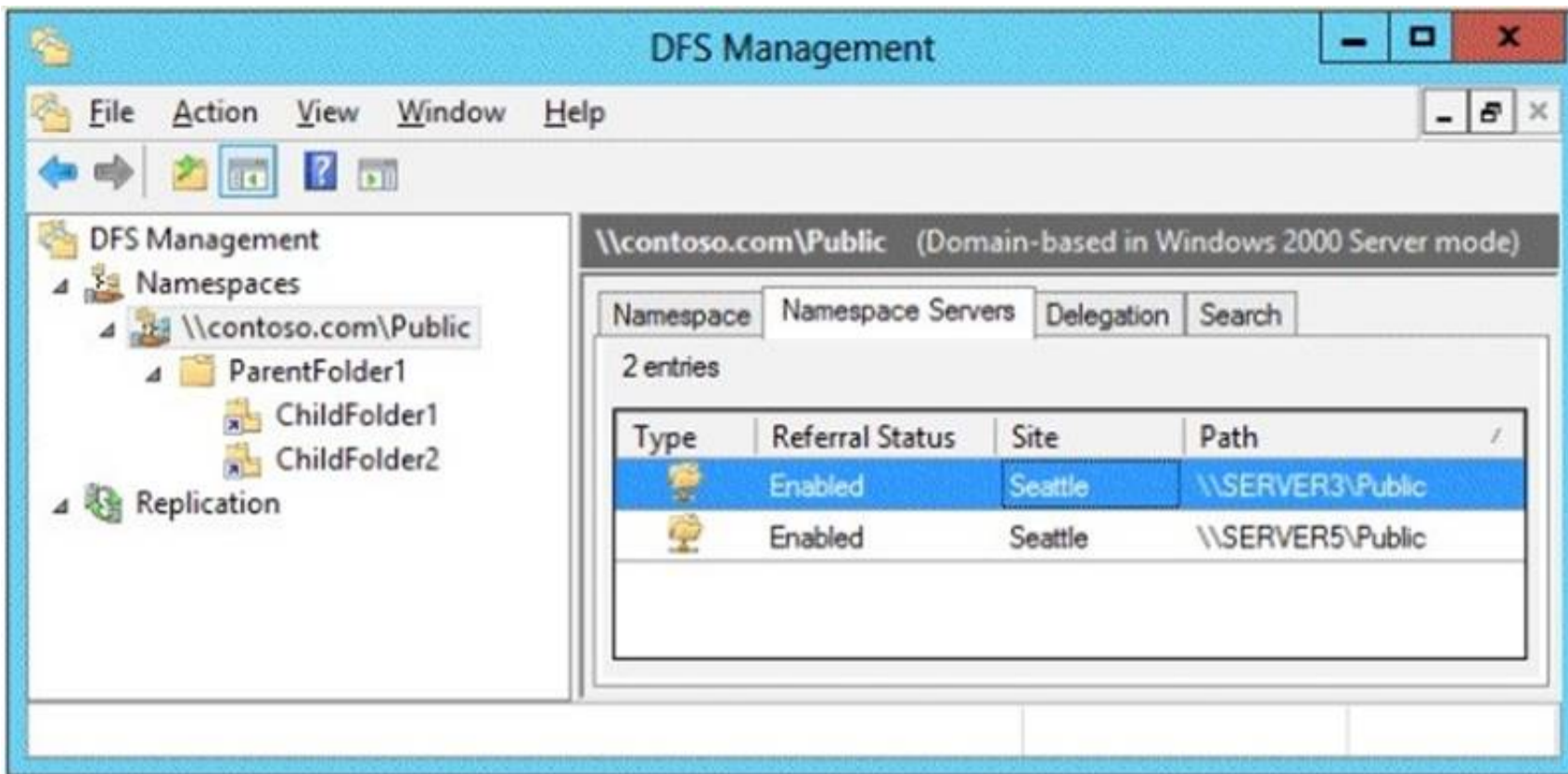
<http://technet.microsoft.com/en-us/library/cc754461%28v=ws.10%29.aspx>

NEW QUESTION 21

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The functional level of both the domain and the forest is Windows Server 2008 R2.

The domain contains a domain-based Distributed File System (DFS) namespace that is configured as shown in the exhibit. (Click the Exhibit button.)



You need to enable access-based enumeration on the DFS namespace. What should you do first?

- A. Raise the domain functional level.
- B. Raise the forest functional level.
- C. Install the File Server Resource Manager role service on Server3 and Server5.
- D. Delete and recreate the namespace.

Answer: D

Explanation:

Access-based enumeration is only supported on a Domain-based Namespace in Windows Server 2008 Mode. This type of Namespace requires a minimum Windows Server 2003 forest functional level and a minimum Windows Server 2008 domain functional level.

The exhibit indicates that the current namespace is a Domain-based Namespace in Windows Server 2000 Mode. To migrate a domain-based namespace from Windows 2000 Server mode to Windows Server 2008 mode, you must export the namespace to a file, delete the namespace, recreate it in Windows Server 2008 mode, and then import the namespace settings.

Reference:

<http://msdn.microsoft.com/en-us/library/cc770287.aspx> <http://msdn.microsoft.com/en-us/library/cc753875.aspx>

NEW QUESTION 24

DRAG DROP - (Topic 1)

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 is configured as a Network Policy Server (NPS) server and as a DHCP server.

You need to log all DHCP clients that have windows Firewall disabled.

Which three actions should you perform in sequence? To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a connection request policy.	
Create a network policy.	
Create a remediation server group.	
Create a Windows Security Health Validator (WSHV) configuration.	
Create a health policy.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

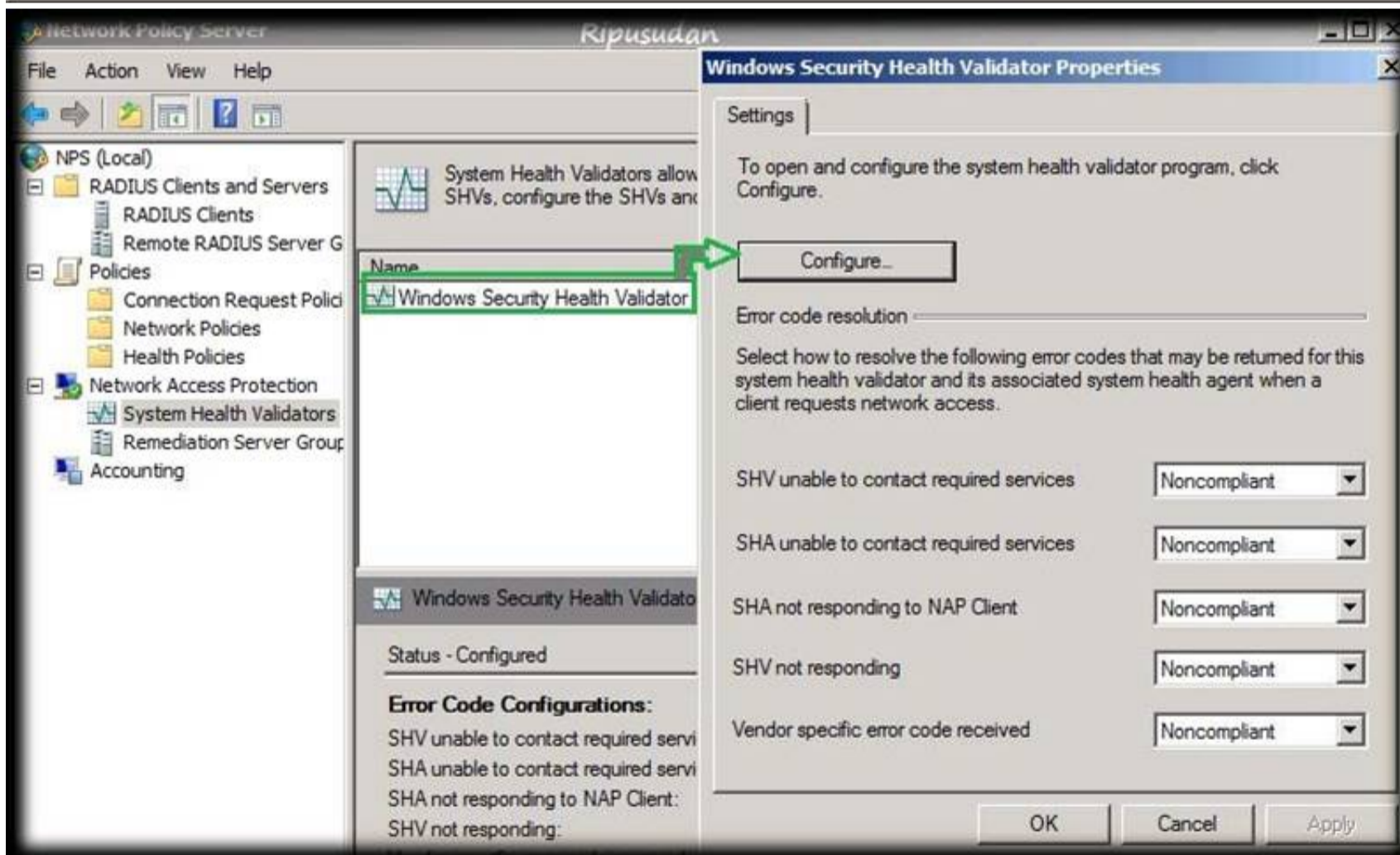
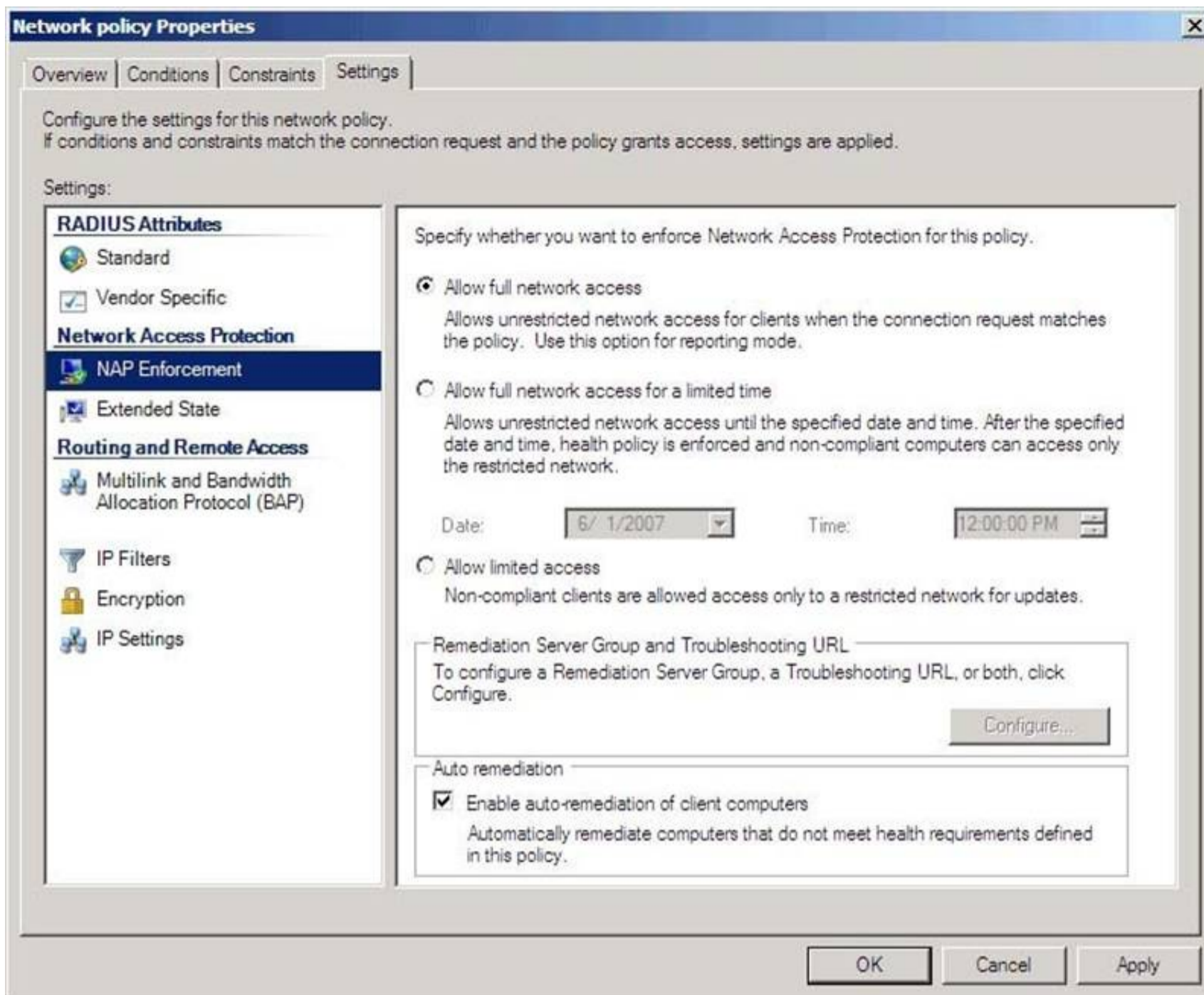
<http://technet.microsoft.com/es-es/library/dd314198%28v=ws.10%29.aspx>

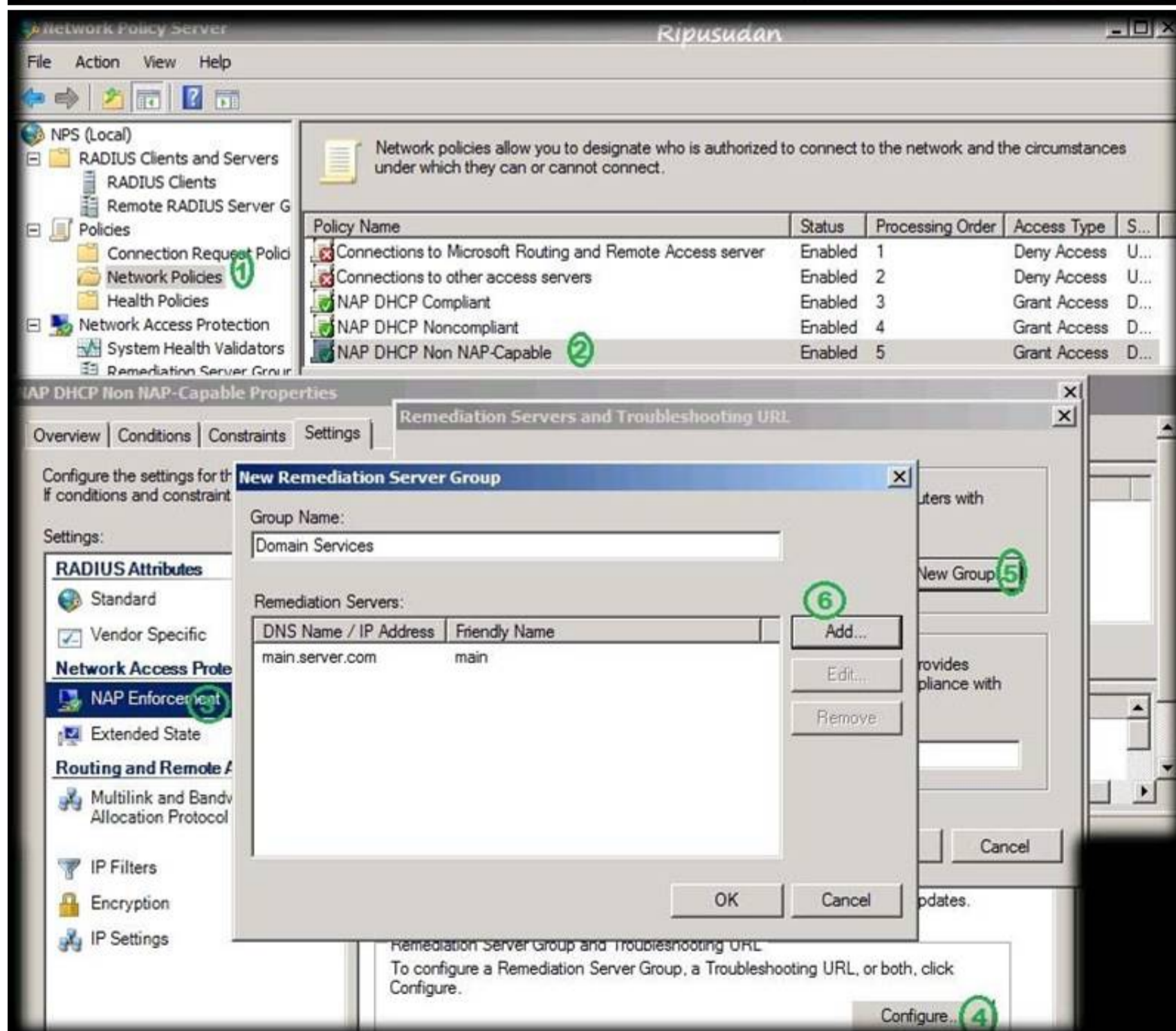
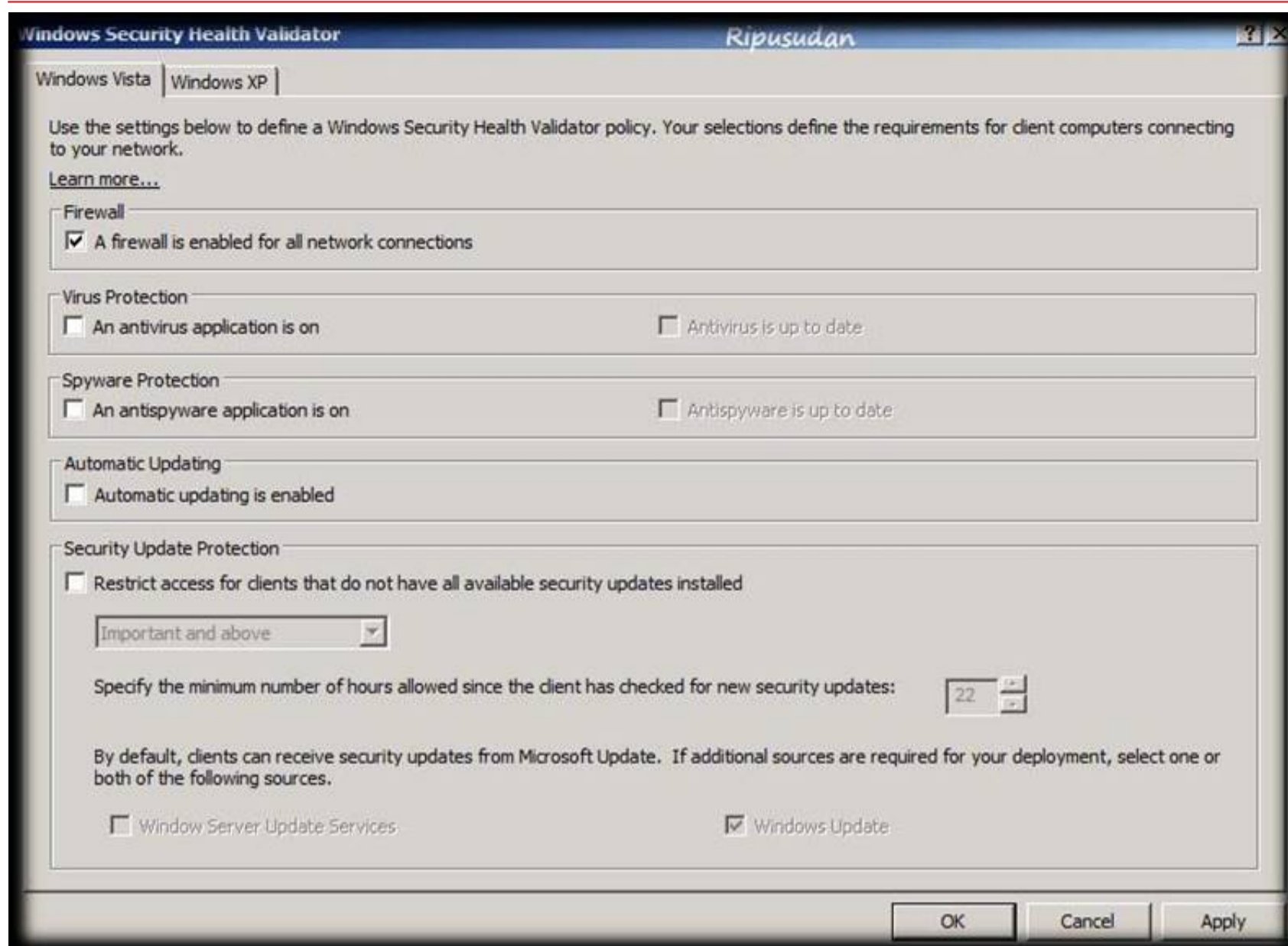
<http://technet.microsoft.com/es-es/magazine/2009.05.goat.aspx>

<http://technet.microsoft.com/es-es/library/dd314173%28v=ws.10%29.aspx>

<http://ripusudan.wordpress.com/2013/03/19/how-to-configure-nap-enforcement-for-dhcp/> <http://technet.microsoft.com/es-es/magazine/2009.05.goat.aspx>

<http://technet.microsoft.com/en-us/library/dd125379%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/cc772356%28v=ws.10%29.aspx>





* With NPS, you can create client health policies using SHVs that allow NAP to detect, enforce, and remediate client computer configurations. WSHA and WSHV provide the following functionality for NAP-capable computers: The client computer has firewall software installed and enabled.
 * Example measurements of health include:
 The operational status of Windows Firewall. Is the firewall enabled or disabled?

In NAP terminology, verifying that a computer meets your defined health requirements is called health policy validation. NPS performs health policy validation for NAP.

NEW QUESTION 25

- (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2.

On Server1, you configure a custom Data Collector Set (DCS) named DCS1. DCS1 is configured to store performance log data in C:\Logs.

You need to ensure that the contents of C:\Logs are deleted automatically when the folder reaches 100 MB in size.

What should you configure?

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

Answer: B

Explanation:

To configure data management for a Data Collector Set

1. In Windows Performance Monitor, expand Data Collector Sets and click User Defined.

2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click Data Manager.

3. On the Data Manager tab, you can accept the default values or make changes according to your data retention policy. See the table below for details on each option.

When Minimum free disk or Maximum folders is selected, previous data will be deleted according to the Resource policy you choose (Delete largest or Delete oldest) when the limit is reached. When Apply policy before the data collector set starts is selected, previous data will be deleted according to your selections before the data collector set creates its next log file.

When Maximum root path size is selected, previous data will be deleted according to your selections when the root log folder size limit is reached.

4. Click the Actions tab. You can accept the default values or make changes. See the table below for details on each option.

5. When you have finished making your changes, click OK.

NEW QUESTION 29

DRAG DROP - (Topic 1)

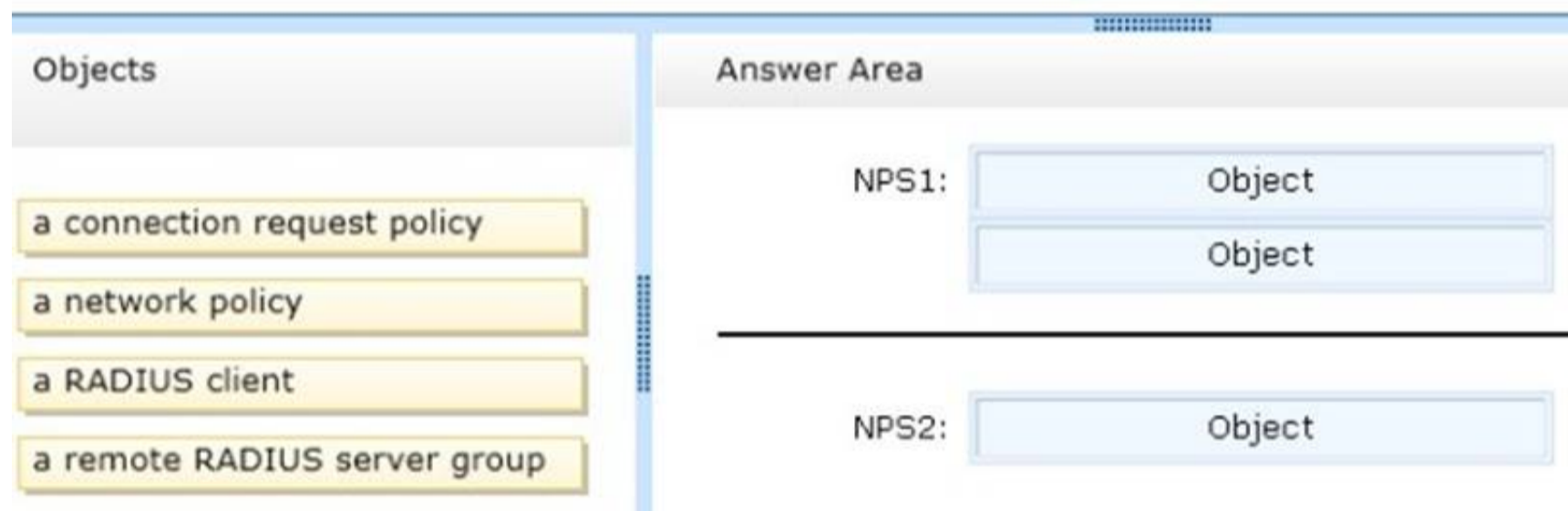
Your network contains an Active Directory forest named contoso.com. The forest contains a Network Policy Server (NPS) server named NPS1 and a VPN server named VPN1. VPN1 forwards all authentication requests to NPS1.

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?

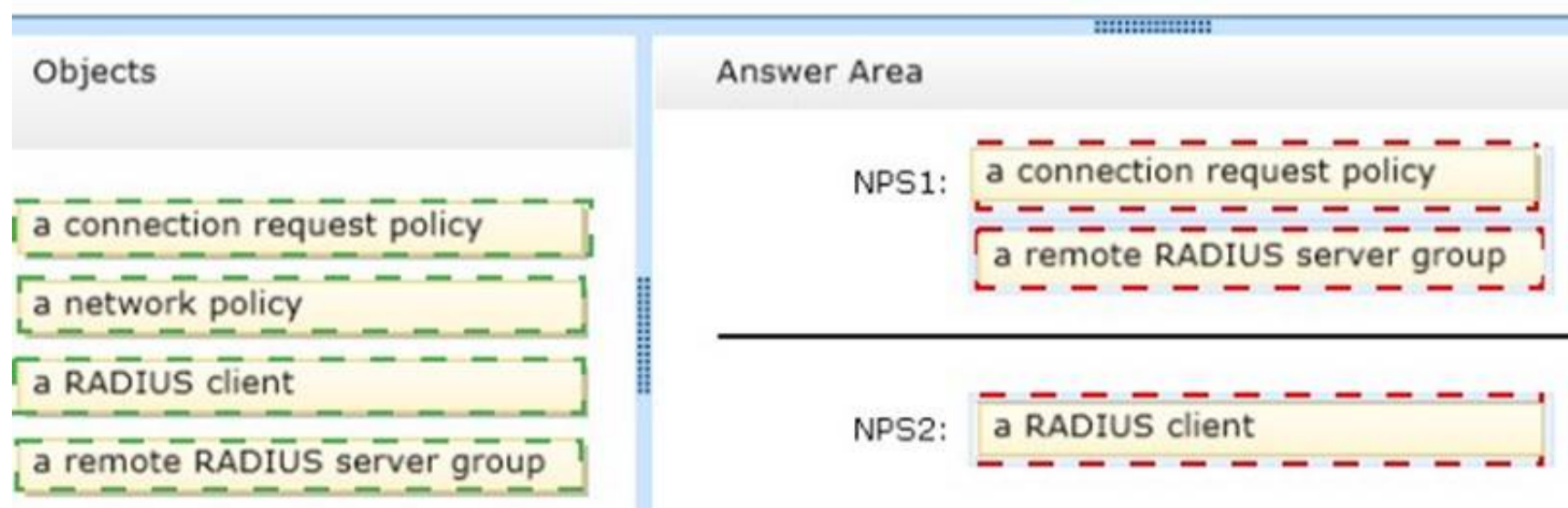
To answer, drag the appropriate objects to the correct NPS servers. Each object may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 32

- (Topic 1)

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. Recover the items by using Active Directory Recycle Bin.
- B. Modify the Recycled attribute of Group1.
- C. Perform tombstone reanimation.
- D. Perform an authoritative restore.
- E. Perform a non- authoritative restore.

Answer: A

Explanation:

Active Directory Recycle Bin helps minimize directory service downtime by enhancing your ability to preserve and restore accidentally deleted Active Directory objects without restoring Active Directory data from backups, restarting Active Directory Domain Services (AD DS), or rebooting domain controllers.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion. For example, restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains.

NEW QUESTION 33

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All user accounts reside in an organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preference of GPO1 to add a shortcut named Link1 to the desktop of each user.

You discover that when a user deletes Link1, the shortcut is removed permanently from the desktop.

You need to ensure that if a user deletes Link1, the shortcut is added to the desktop again. What should you do?

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

Answer: B

Explanation:

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

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

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

References:

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

NEW QUESTION 35

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. All servers run Windows Server 2012 R2.

You need to collect the error events from all of the servers on Server1. The solution must ensure that when new servers are added to the domain, their error events are collected automatically on Server1.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

Answer: BC

Explanation:

To set up a Source-Initiated Subscription with Windows Server 2003/2008 so that events of interest from the Security event log of several domain controllers can be forwarded to an administrative workstation.

* Group Policy

The forwarding computer needs to be configured with the address of the server to which the events are forwarded. This can be done with the following group policy setting:

Computer configuration-Administrative templates-Windows components-Event forwarding- Configure the server address, refresh interval, and issue certificate authority of a target subscription manager.

* Edit the GPO and browse to Computer Configuration | Policies | Administrative Templates

| Windows Components | Event Forwarding - Configure the server address, refresh interval, and issuer certificate authority of a target Subscription Manager.

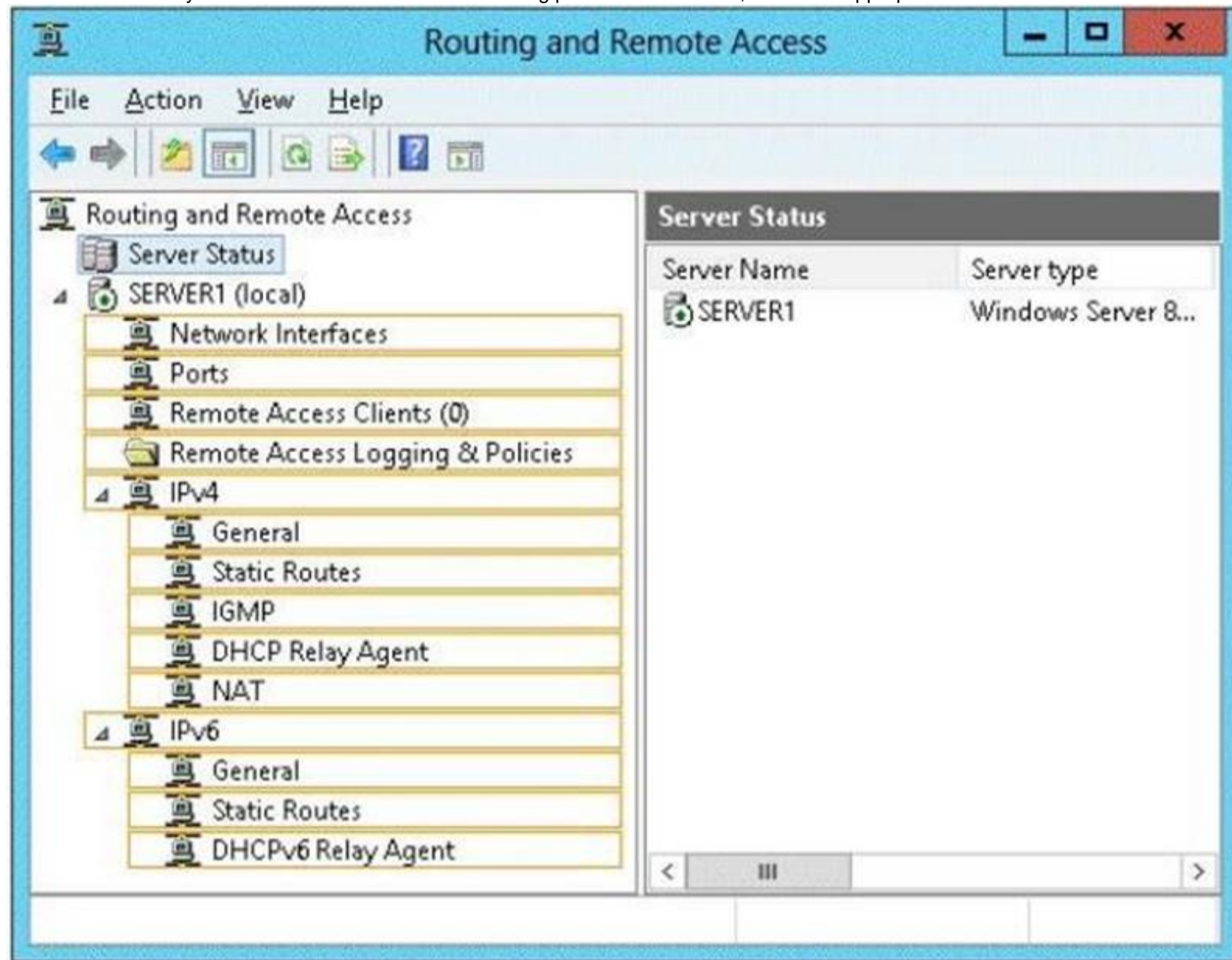
NEW QUESTION 38

HOTSPOT - (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has two network adapters and is located in a perimeter network.

You need to install the RIP version 2 routing protocol on Server1.

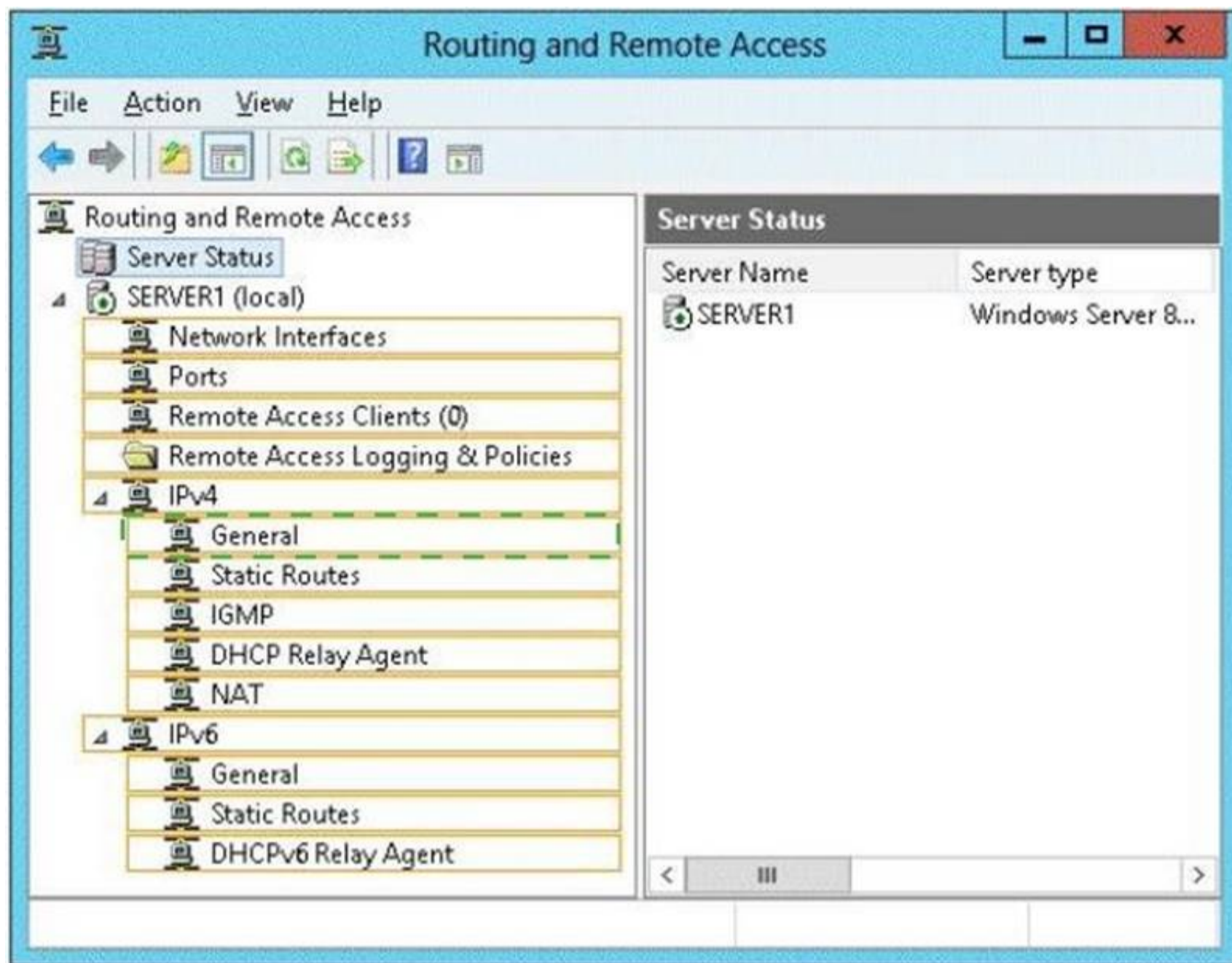
Which node should you use to add the RIP version 2 routing protocol? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 40

- (Topic 1)

Your network contains two Active Directory domains named contoso.com and adatum.com.

The network contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the DNS Server server role installed. Server1 has a copy of the contoso.com DNS zone.

You need to configure Server1 to resolve names in the adatum.com domain. The solution must meet the following requirements:

Prevent the need to change the configuration of the current name servers that host zones for adatum.com. Minimize administrative effort.

Which type of zone should you create?

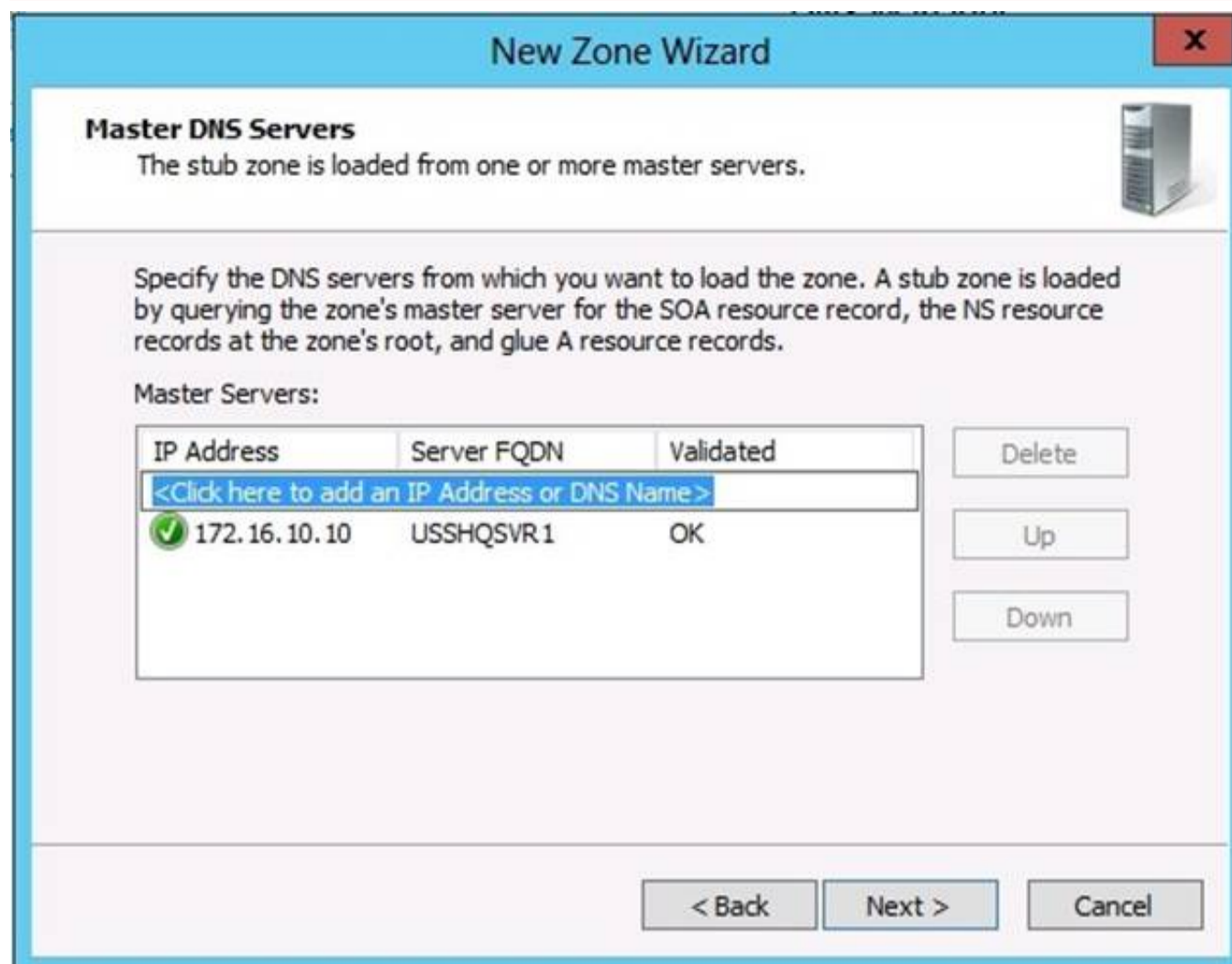
- A. Secondary
- B. Stub
- C. Reverse lookup
- D. Primary

Answer: B

Explanation:

When a zone that this DNS server hosts is a stub zone, this DNS server is a source only for information about the authoritative name servers for this zone. The zone at this server must be obtained from another DNS server that hosts the zone. This DNS server must have network access to the remote DNS server to copy the authoritative name server information about the zone.

A stub zone is a copy of a zone that contains only necessary resource records (Start of Authority (SOA), Name Server (NS), and Address/Host (A) record) in the master zone and acts as a pointer to the authoritative name server. The stub zone allows the server to forward queries to the name server that is authoritative for the master zone without going up to the root name servers and working its way down to the server. While a stub zone can improve performance, it does not provide redundancy or load sharing.



You can use stub zones to:

Keep delegated zone information current. By updating a stub zone for one of its child zones regularly, the DNS server that hosts both the parent zone and the stub zone will maintain a current list of authoritative DNS servers for the child zone.

Improve name resolution. Stub zones enable a DNS server to perform recursion using the stub zone's list of name servers, without having to query the Internet or an internal root server for the DNS namespace.

Simplify DNS administration. By using stub zones throughout your DNS infrastructure, you can distribute a list of the authoritative DNS servers for a zone without using secondary zones. However, stub zones do not serve the same purpose as secondary zones, and they are not an alternative for enhancing redundancy and load sharing.

There are two lists of DNS servers involved in the loading and maintenance of a stub zone: The list of master servers from which the DNS server loads and updates a stub zone. A master server may be a primary or secondary DNS server for the zone. In both cases, it will have a complete list of the DNS servers for the zone.

The list of the authoritative DNS servers for a zone. This list is contained in the stub zone using name server (NS) resource records.

When a DNS server loads a stub zone, such as widgets. tailspintoys.com, it queries the master servers, which can be in different locations, for the necessary resource records of the authoritative servers for the zone widgets. tailspintoys.com. The list of master servers may contain a single server or multiple servers, and it can be changed anytime.

References:

<http://technet.microsoft.com/en-us/library/cc771898.aspx> <http://technet.microsoft.com/en-us/library/cc754190.aspx> <http://technet.microsoft.com/en-us/library/cc730980.aspx>

NEW QUESTION 45

- (Topic 1)

You have a server named Server 1.

You enable BitLocker Drive Encryption (BitLocker) on Server 1.

You need to change the password for the Trusted Platform Module (TPM) chip. What should you run on Server1?

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

Answer: B

Explanation:

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

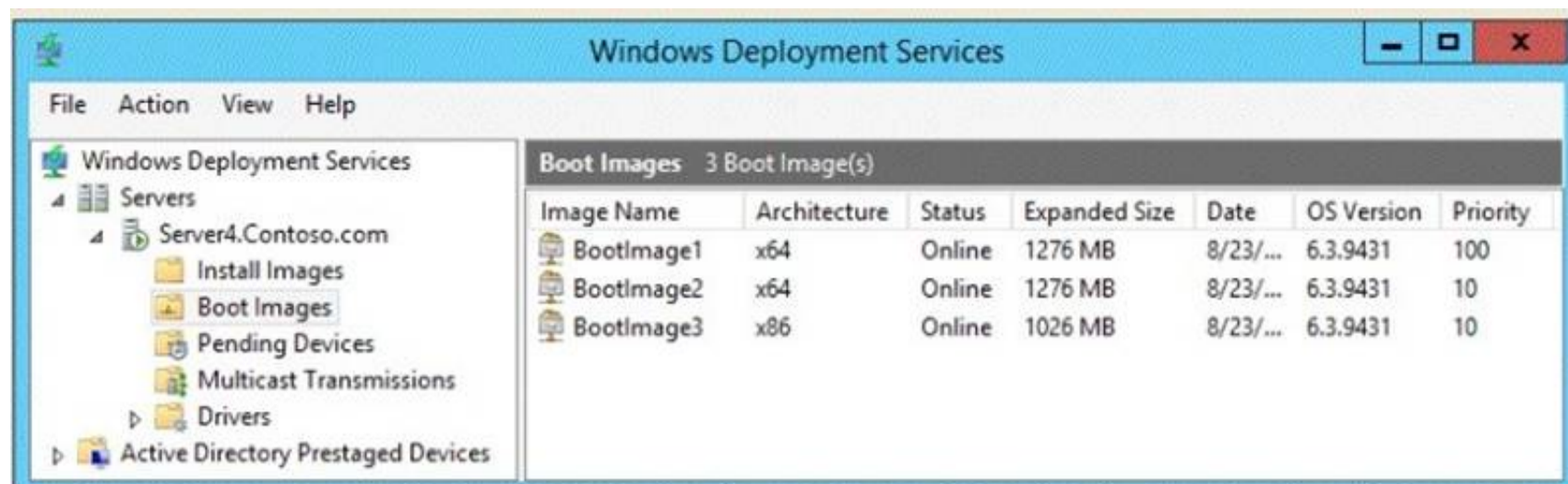
Use the ConvertTo-TpmOwnerAuthcmdlet to create an owner authorization value. You can specify a new owner authorization value or specify a file that contains the new value.

NEW QUESTION 48

HOTSPOT - (Topic 1)

You have a server named Server4 that runs Windows Server 2012 R2. Server4 has the Windows Deployment Services server role installed.

Server4 is configured as shown in the exhibit. (Click the Exhibit button.)



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

Answer Area

When you connect to Windows Deployment Services (WDS) from an x64 client computer, you can select ...

When you connect to Windows Deployment Services (WDS) from an x64 client computer, the default image will be ...

Answer Area

When you connect to Windows Deployment Services (WDS) from an x64 client computer, you can select ...

- BootImage3 only.
- BootImage1 and BootImage2 only.
- BootImage2 and BootImage3 only.
- BootImage1, BootImage2, and BootImage3

When you connect to Windows Deployment Services (WDS) from an x64 client computer, the default image will be ...

- BootImage1.
- BootImage2.
- BootImage3.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

When you connect to Windows Deployment Services (WDS) from an x64 client computer, you can select ...

- BootImage3 only.
- BootImage1 and BootImage2 only.
- BootImage2 and BootImage3 only.
- BootImage1, BootImage2, and BootImage3

When you connect to Windows Deployment Services (WDS) from an x64 client computer, the default image will be ...

- BootImage1.
- BootImage2.
- BootImage3.

NEW QUESTION 52

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a read-only domain controller (RODC) named RODC1.

You create a global group named RODC_Admins.

You need to provide the members of RODC_Admins with the ability to manage the hardware and the software on RODC1. The solution must not provide RODC_Admins with the ability to manage Active Directory objects.

What should you do?

- A. From Active Directory Site and Services, configure the Security settings of the RODC1 server object.
- B. From Windows PowerShell, run the Set-ADAccountControlcmdlet.
- C. From a command prompt, run the dsmgmt local roles command.
- D. From Active Directory Users and Computers, configure the Member Of settings of the RODC1 account.

Answer: C

Explanation:

RODC: using the dsmgmt.exe utility to manage local administrators

One of the benefits of RODC is that you can add local administrators who do not have full access to the domain administration. This gives them the ability to manage the server but not add or change active directory objects unless those roles are delegated. Adding this type of user is done using the dsmdmt.exe utility at the command prompt.

NEW QUESTION 57

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.

Client computers run either Windows 7 or Windows 8. All of the client computers have an application named App1 installed.

The domain contains a Group Policy object (GPO) named GPO1 that is applied to all of the client computers.

You need to add a system variable named App1Data to all of the client computers. Which Group Policy preference should you configure?

- A. Environment
- B. Ini Files
- C. Data Sources
- D. Services

Answer: A

Explanation:

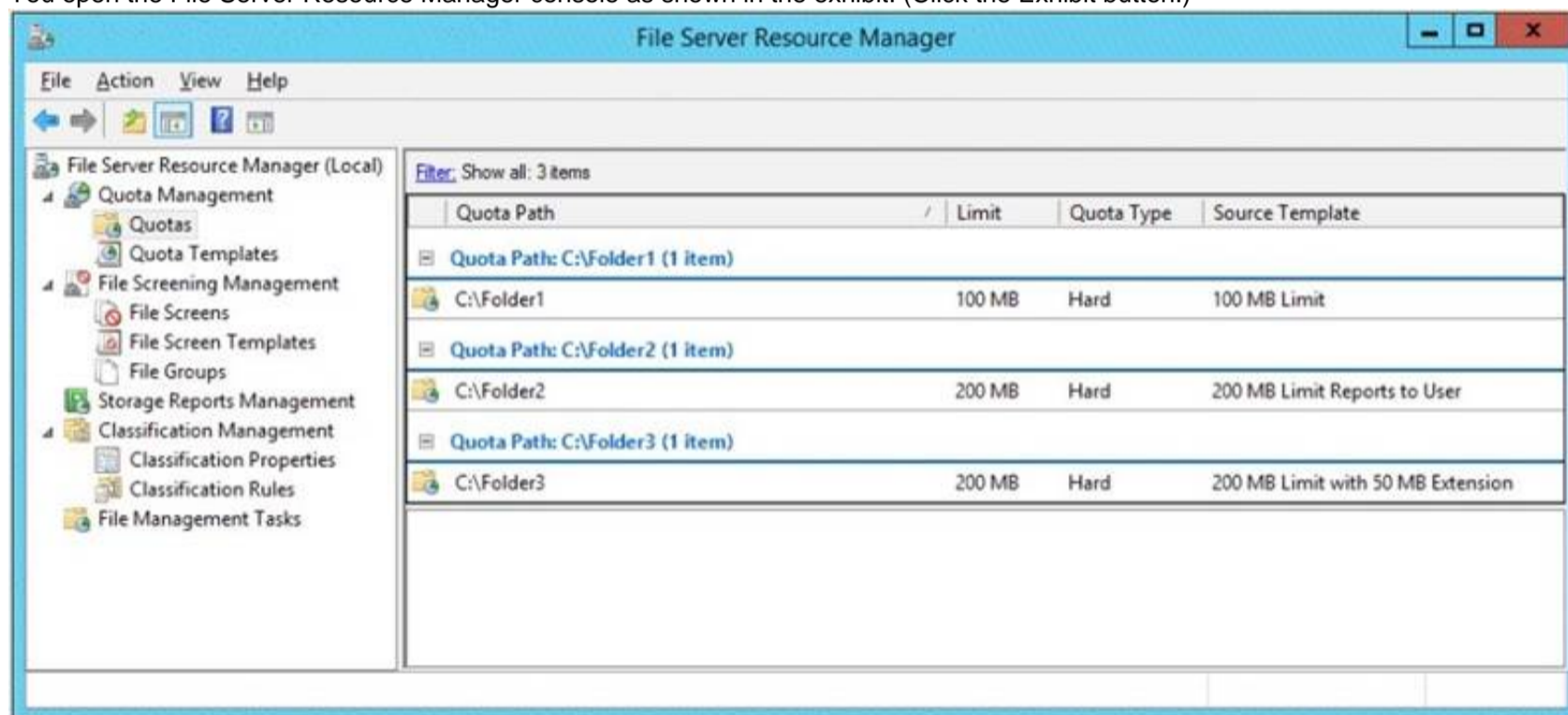
Environment Variable preference items allow you to create, update, replace, and delete user and system environment variables or semicolon-delimited segments of the PATH variable. Before you create an Environment Variable preference item, you should review the behavior of each type of action possible with this extension.

NEW QUESTION 60

- (Topic 1)

You have a file server that has the File Server Resource Manager role service installed.

You open the File Server Resource Manager console as shown in the exhibit. (Click the Exhibit button.)



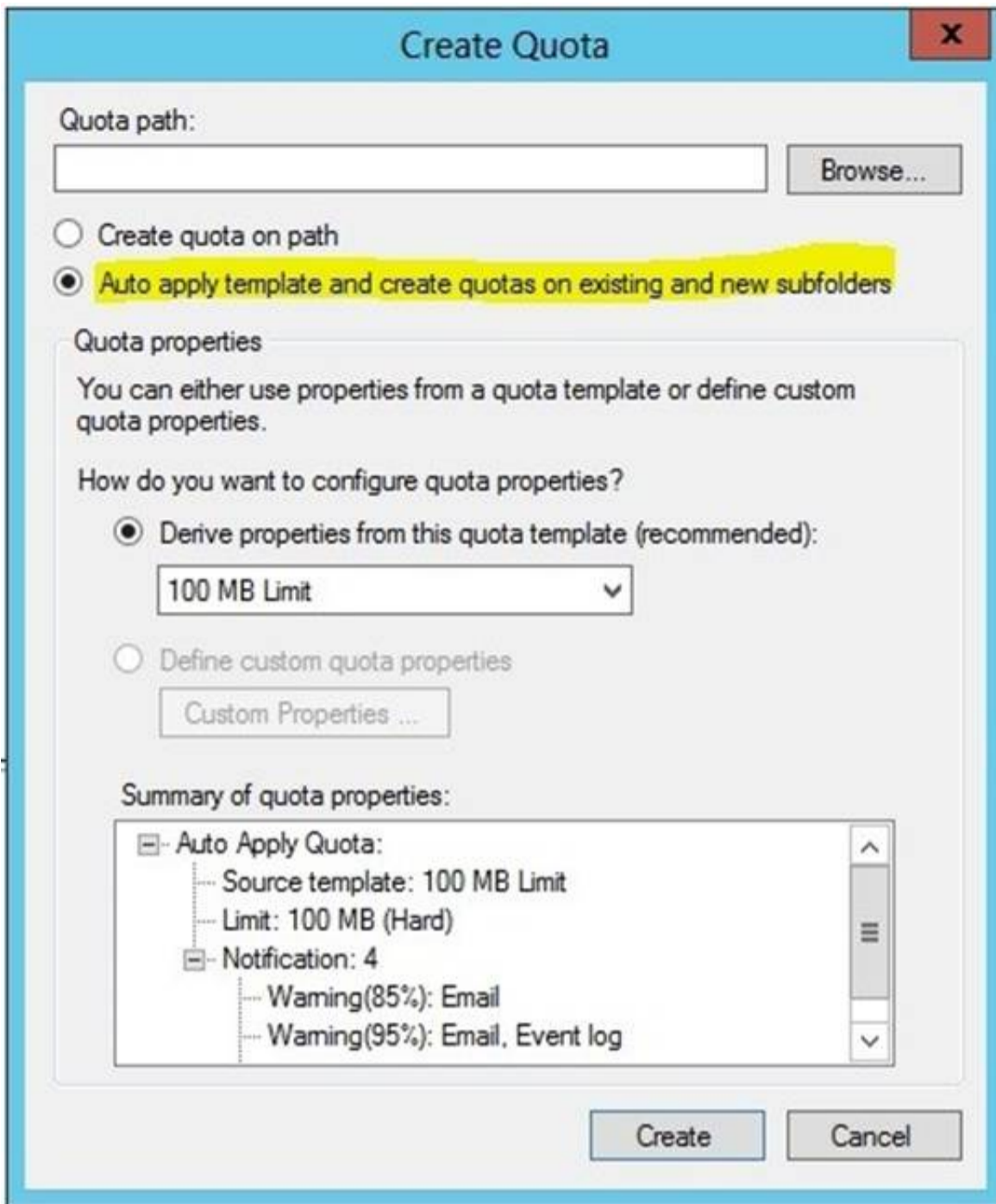
You need to ensure that all of the folders in Folder1 have a 100-MB quota limit. What should you do?

- A. Run the Update FsrmQuotacmdlet.
- B. Run the Update-FsrmAutoQuotacmdlet.
- C. Create a new quota for Folder1.
- D. Modify the quota properties of Folder1.

Answer: C

Explanation:

By using auto apply quotas, you can assign a quota template to a parent volume or folder. Then File Server Resource Manager automatically generates quotas that are based on that template. Quotas are generated for each of the existing subfolders and for subfolders that you create in the future.



Ref: <http://technet.microsoft.com/en-us/library/cc731577.aspx>

NEW QUESTION 64

- (Topic 1)

Your network contains two servers named Server1 and Server2 that run windows Server 2012 R2. Server1 and Server2 have the Windows Server Update Services server role installed.

Server1 synchronizes from Microsoft Update. Server2 is a Windows Server Update Services (WSUS) replica of Server1.

You need to configure replica downstream servers to send Server1 summary information about the computer update status.

What should you do?

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

Answer: A

Explanation:

WSUS Reporting Rollup Sample Tool

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

Reference: <http://technet.microsoft.com/en-us/windowsserver/bb466192.aspx>

NEW QUESTION 65

DRAG DROP - (Topic 1)

Your network contains an Active Directory forest named contoso.com. All domain controllers run Windows Server 2008 R2.

The schema is upgraded to Windows Server 2012 R2.

Contoso.com contains two servers. The servers are configured as shown in the following table.

Server name	Operating system	Role
Server1	Windows Server 2012 R2	Web Server (IIS) server role Network Load Balancing (NLB) feature
Server2	Windows Server 2012 R2	Web Server (IIS) server role Network Load Balancing (NLB) feature

Server1 and Server2 host a load-balanced application pool named AppPool1.

You need to ensure that AppPool1 uses a group Managed Service Account as its identity. Which three actions should you perform?

To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Run the Install-ADServiceAccount cmdlet.	
Modify the settings of AppPool1.	
Run the New-ADServiceAccount cmdlet.	
Install a domain controller that runs Windows Server 2012 R2.	
Run the Set-ADServiceAccount cmdlet.	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Note: Box 1:

Group Managed Service Accounts Requirements:

At least one Windows Server 2012 Domain Controller

A Windows Server 2012 or Windows 8 machine with the ActiveDirectory PowerShell module, to create/manage the gMSA.

A Windows Server 2012 or Windows 8 domain member to run/use the gMSA. Box 2:

To create a new managed service account

? On the domain controller, click Start, and then click Run. In the Open box, type dsa. msc, and then click OK to open the Active Directory Users and Computers snap-in. Confirm that the Managed Service Account container exists.

? Click Start, click All Programs, click Windows PowerShell 2.0, and then click the Windows PowerShell icon.

? Run the following command: New-ADServiceAccount [- SAMAccountName<String>] [-Path <String>].

Box 3:

Configure a service account for Internet Information Services

Organizations that want to enhance the isolation of IIS applications can configure IIS application pools to run managed service accounts.

To use the Internet Information Services (IIS) Manager snap-in to configure a service to use a managed service account

? Click Start, point to Administrative Tools, and then click Internet Information

Services (IIS) Manager.

? Double-click <Computer name>, double-click Application Pools, right-click <Pool

Name>, and click Advanced Settings.

? In the Identity box, click ..., click Custom Account, and then click Set.

? Type the name of the managed service account in the format domainname\accountname.

NEW QUESTION 67

- (Topic 1)

You manage a server that runs Windows Server 2012 R2. The server has the Windows Deployment Services server role installed.

You have a desktop computer that has the following configuration:

? Computer name: Computer1

? Operating system: Windows 8

? MAC address: 20-CF-30-65-D0-87

? GUID: 979708BF-C04B-4525-9FE0-C4150BB6C618

You need to configure a pre-staged device for Computer1 in the Windows Deployment Services console.

Which two values should you assign to the device ID? (Each correct answer presents a complete solution. Choose two.)

- A. 20CF3065D08700000000000000000000
B. 979708BFC04B45259FE0C4150BB6C618
C. 979708BF-C04B-452S-9FE0-C4150BB6C618
D. 00000000000000000000000020CF306SD087
E. 00000000-0000-0000-0000-C41S0BB6C618

Answer: CD

Explanation:

In the text box, type the client computer's MAC address preceded with twenty zeros or the globally unique identifier (GUID) in the format: {XXXXXXXX-XXXX-XXXX-XXX-XXXXXXXXXXXX}.

* To add or remove pre-staged client to/from AD DS, specify the name of the computer or the device ID, which is a GUID, media access control (MAC) address, or Dynamic Host Configuration Protocol (DHCP) identifier associated with the computer.

* Example: Remove a device by using its ID from a specified domain

This command removes the pre-staged device that has the specified ID. The cmdlet searches the domain named TSQA.contoso.com for the device.

Windows PowerShell

PS C:\> Remove-WdsClient -DeviceID "5a7a1def-2e1f-4a7b-a792-ae5275b6ef92" -Domain

-DomainName "TSQA.contoso.com"

NEW QUESTION 70

- (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

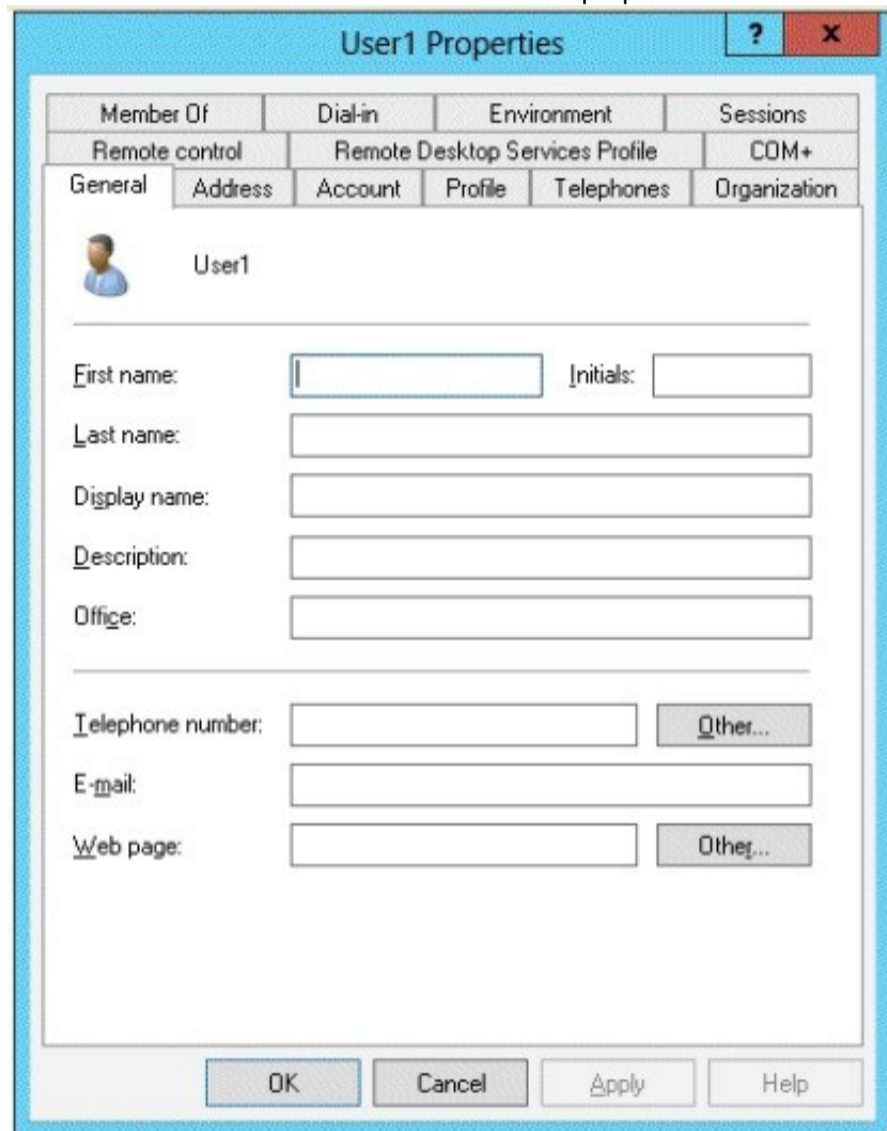
Explanation:

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 75

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. You create a user account named User1. The properties of User1 are shown in the exhibit. (Click the Exhibit button.)



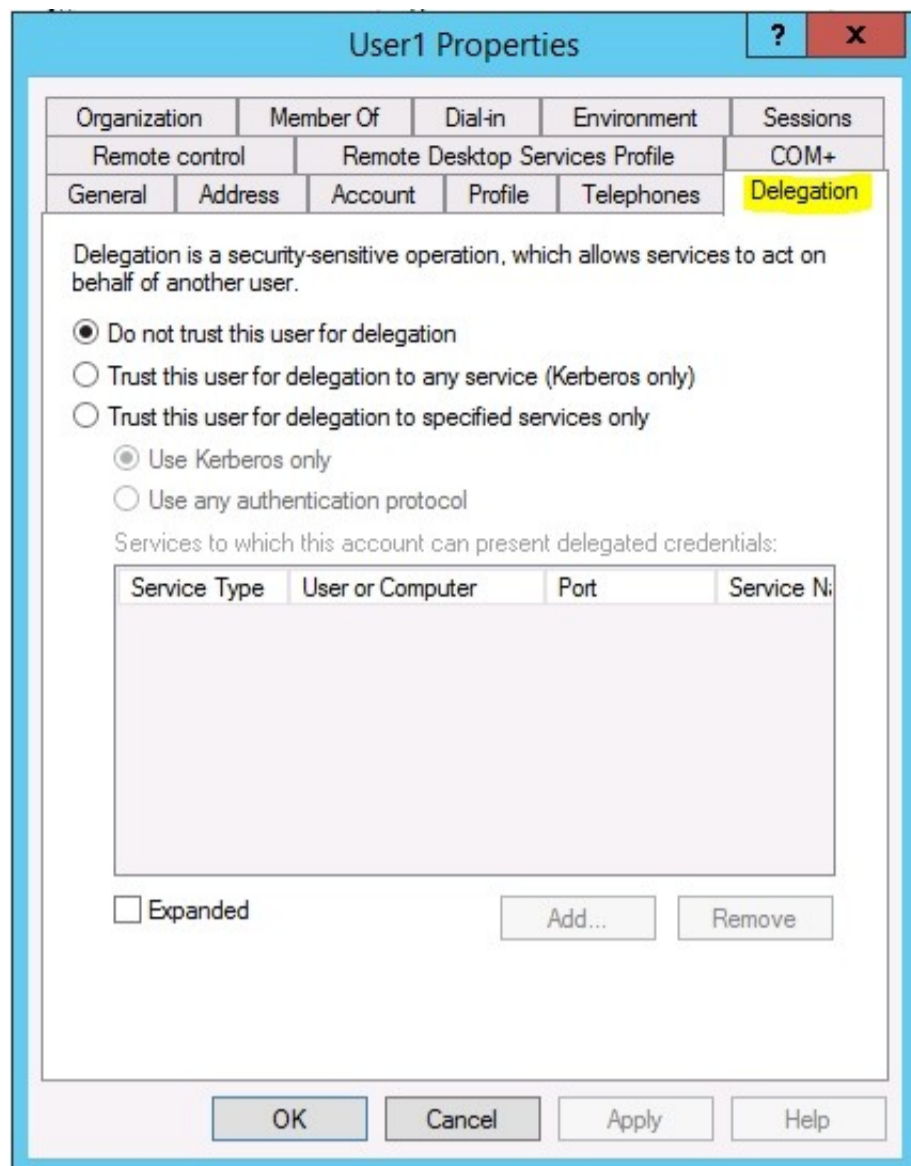
You plan to use the User1 account as a service account. The service will forward authentication requests to other servers. You need to ensure that you can view the Delegation tab from the properties of the User1 account. What should you do first?

- A. Configure the Name Mappings of User1.
- B. Modify the user principal name (UPN) of User1.
- C. Configure a Service Principal Name (SPN) for User1.
- D. Modify the Security settings of User1.

Answer: C

Explanation:

If you cannot see the Delegation tab, do one or both of the following:
 Register a Service Principal Name (SPN) for the user account with the Setspn utility in the support tools on your CD. Delegation is only intended to be used by service accounts, which should have registered SPNs, as opposed to a regular user account which typically does not have SPNs.
 Raise the functional level of your domain to Windows Server 2003. For more information, see Related Topics.



References:

<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>
<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>
[http://technet.microsoft.com/en-us/library/cc739474\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc739474(v=ws.10).aspx)
<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>

NEW QUESTION 77

- (Topic 2)

You have a DNS server named Server1.

Server1 has a primary zone named contoso.com.

Zone Aging/Scavenging is configured for the contoso.com zone.

One month ago, an administrator removed a server named Server2 from the network.

You discover that a static resource record for Server2 is present in contoso.com. Resource records for decommissioned client computers are removed automatically from contoso.com.

You need to ensure that the static resource records for all of the servers are removed automatically from contoso.com.

What should you modify?

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

Answer: B

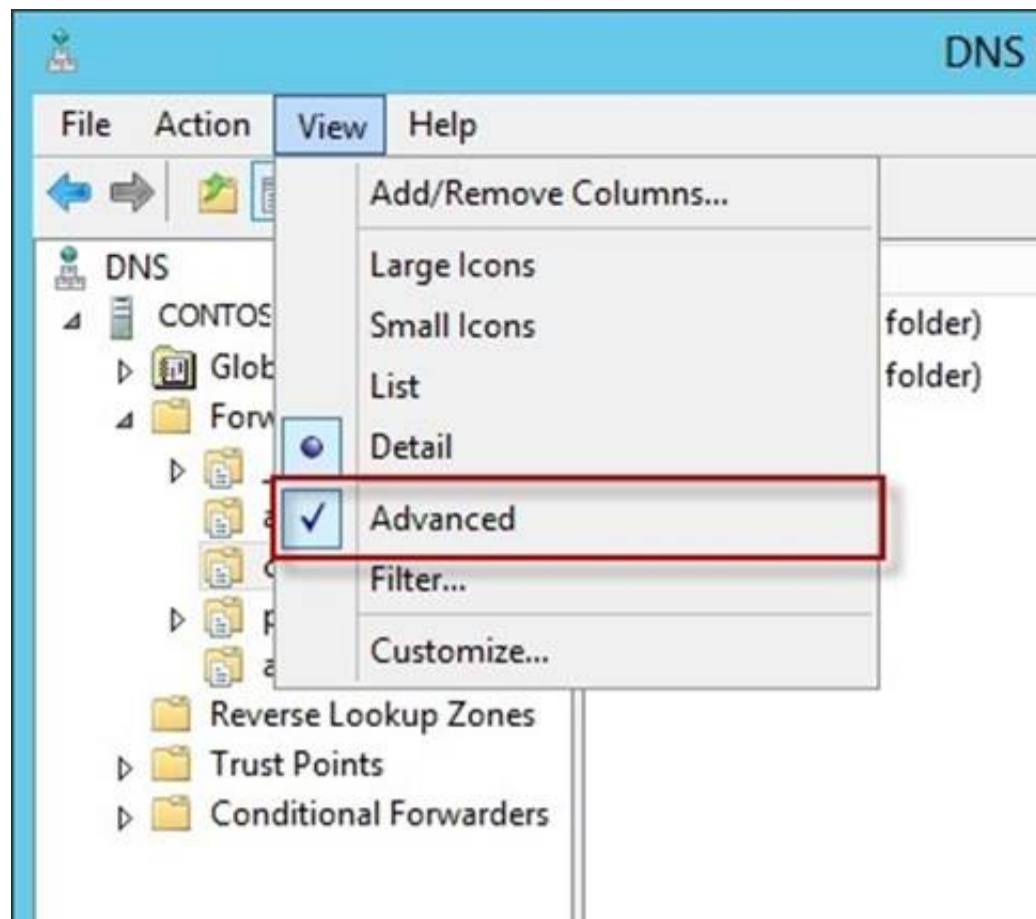
Explanation:

Reset and permit them to use a current (non-zero) time stamp value. This enables these records to become aged and scavenged.

You can use this procedure to change how a specific resource record is scavenged.

A stale record is a record where both the No-Refresh Interval and Refresh Interval have passed without the time stamp updating.

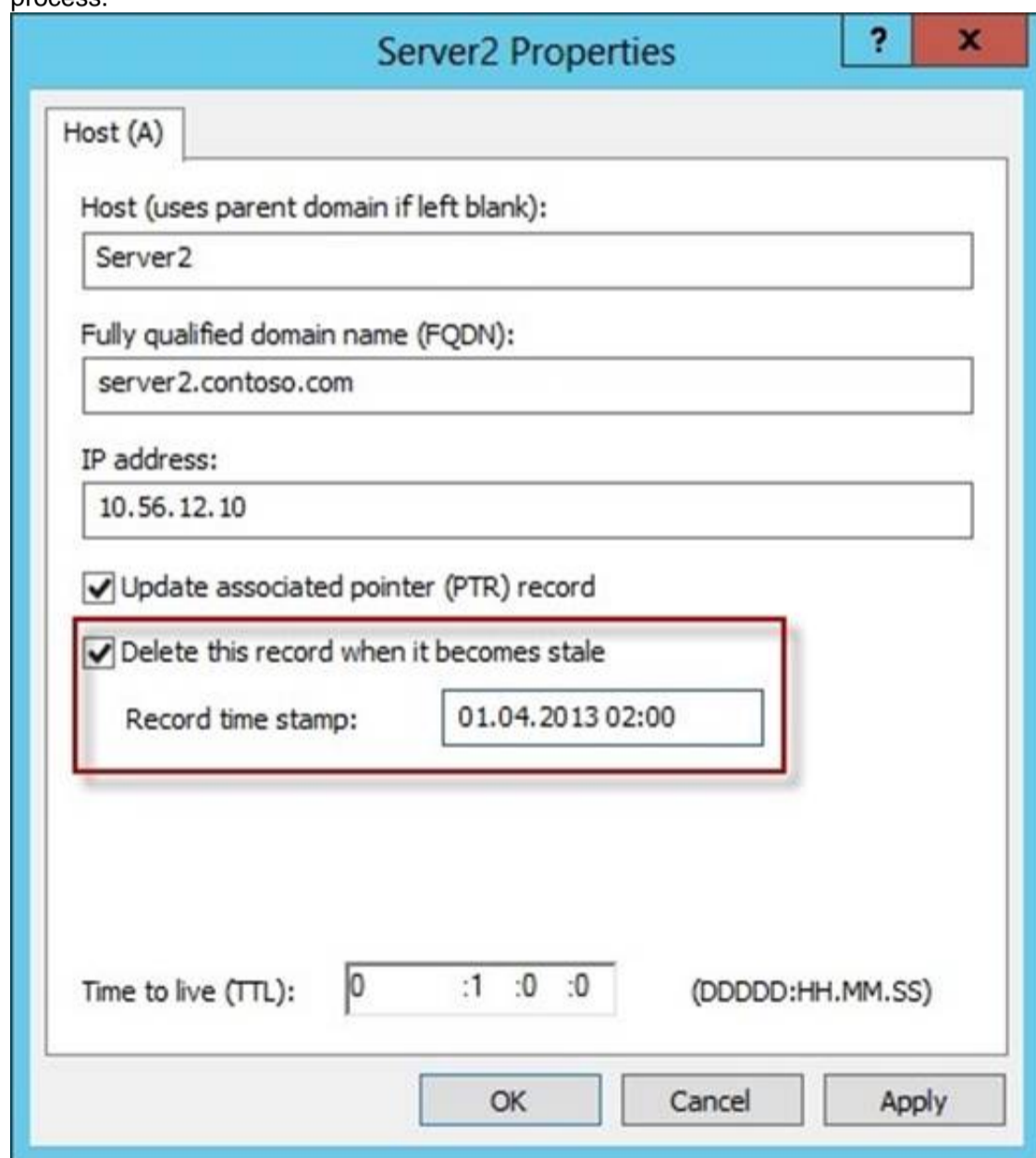
DNS->View->Advanced



Depending on the how the resource record was originally added to the zone, do one of the following:

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

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



References:

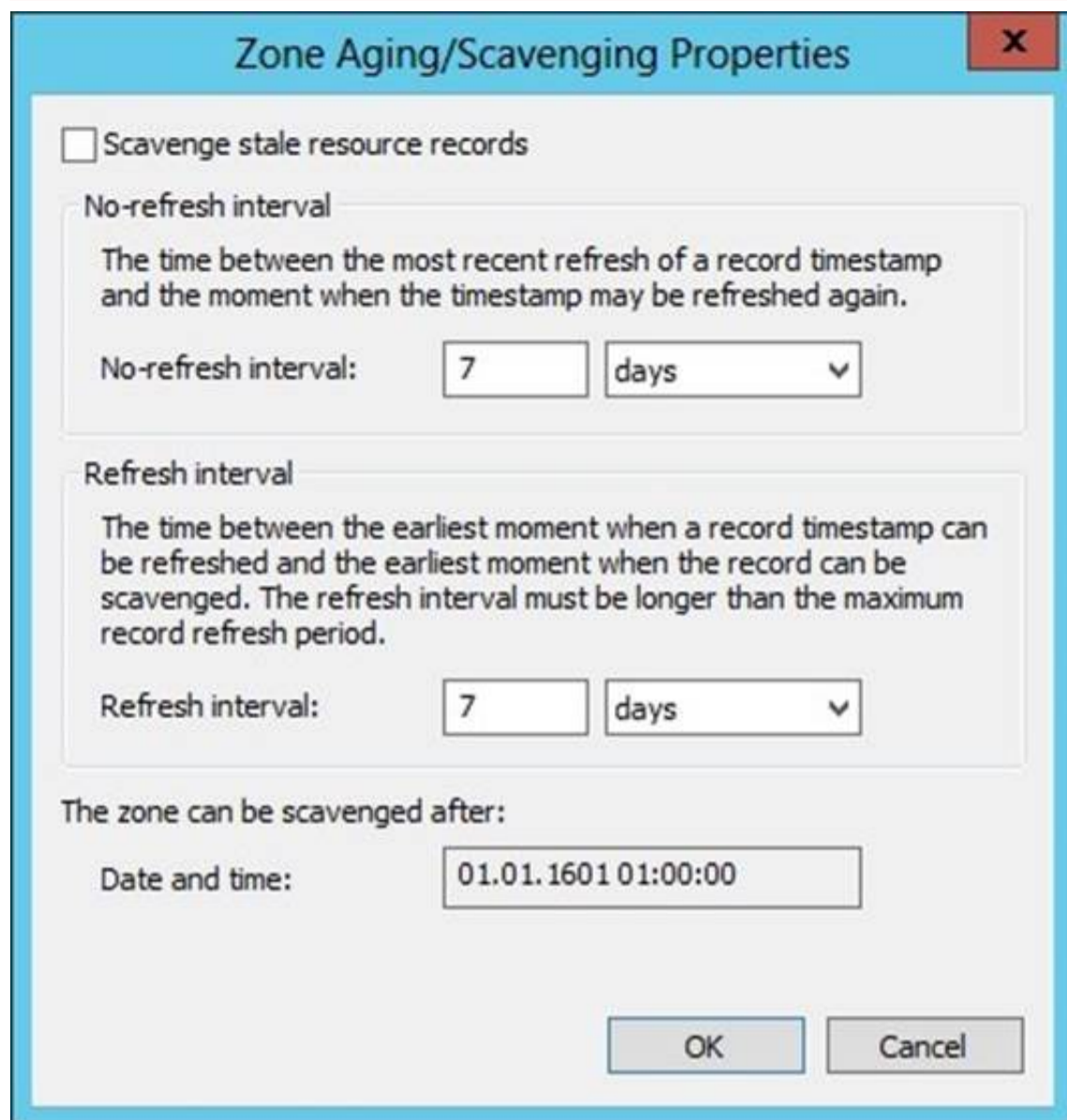
<http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx>

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

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

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

Scavenging and aging must be enabled both at the DNS server and on the zone. Scavenging is disabled by default.



Zone Aging/Scavenging Properties

☐ Scavenge stale resource records

No-refresh interval
 The time between the most recent refresh of a record timestamp and the moment when the timestamp may be refreshed again.

No-refresh interval:

Refresh interval
 The time between the earliest moment when a record timestamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period.

Refresh interval:

The zone can be scavenged after:

Date and time:

DNS scavenging depends on the following two settings:

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

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

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

References:

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

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

<http://technet.microsoft.com/en-us/library/cc771570.aspx>

<http://technet.microsoft.com/en-us/library/cc771677.aspx>

[http://technet.microsoft.com/en-us/library/cc758321\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc758321(v=ws.10).aspx)

NEW QUESTION 82

- (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Server Update Services server role installed.

Server1 stores update files locally in C:\Updates.

You need to change the location in which the update files are stored to D:\Updates. What should you do?

- A. From the Update Services console, run the Windows Server Update Services Configuration Wizard.
- B. From a command prompt, run wsusutil.exe and specify the movecontent parameter.
- C. From the Update Services console, configure the Update Files and Languages option.
- D. From a command prompt, run wsusutil.exe and specify the export parameter.

Answer: B

Explanation:

You might need to change the location where WSUS stores updates locally. This might be required if the disk becomes full and there is no longer any room for new updates. You might also have to do this if the disk where updates are stored fails and the replacement disk uses a new drive letter.

You accomplish this move with the movecontent command of WSUSutil.exe, a command-line tool that is copied to the file system of the WSUS server during WSUS Setup. By default, Setup copies WSUSutil.exe to the following location: WSUSInstallationDrive:\Program Files\Microsoft Windows Server Update Services\Tools\

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.

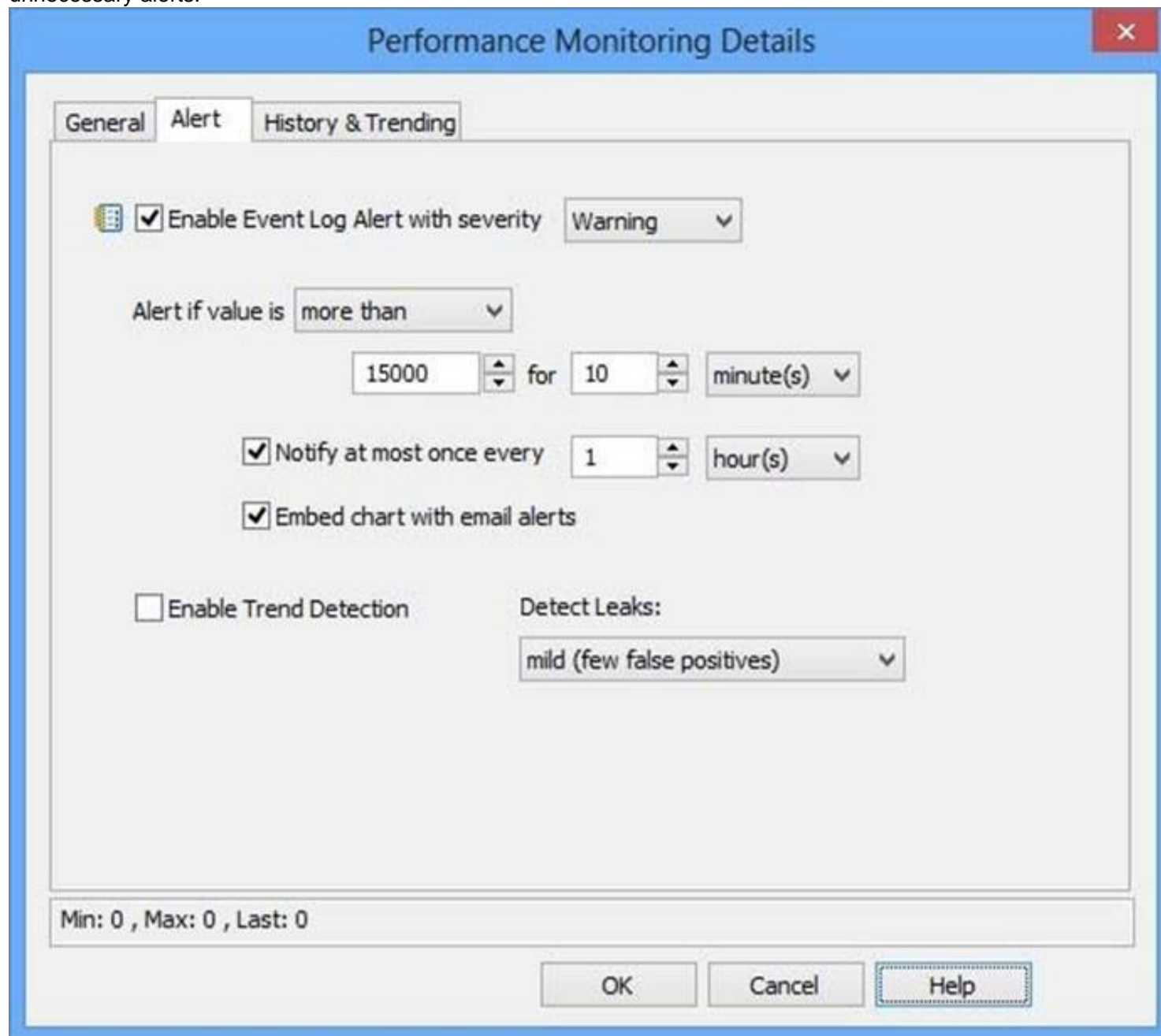
Which type of data collector should you create?

- 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.



The image shows the 'Performance Monitoring Details' dialog box with the 'Alert' tab selected. The 'General' tab is also visible. The 'Alert' tab contains the following settings:

- ☒ 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)

At the bottom, there are buttons for 'OK', 'Cancel', and 'Help'. A status bar at the bottom left shows 'Min: 0 , Max: 0 , Last: 0'.

NEW QUESTION 87

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

A domain controller named DC1 runs Windows Server 2012 R2. DC1 is backed up daily. During routine maintenance, you delete a group named Group1.

You need to recover Group1 and 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. Perform an authoritative restore of Group1.
- B. Mount the most recent Active Directory backup.
- C. Use the Recycle Bin to restore Group1.
- D. Reactivate the tombstone of 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.

There is another approach you should be aware of. Tombstone reanimation (which has nothing to do with zombies) provides the only way to recover deleted objects without taking a DC offline, and it's the only way to recover a deleted object's identity information, such as its objectGUID and objectSid attributes. It neatly solves the problem of recreating a deleted user or group and having to fix up all the old access control list (ACL) references, which contain the objectSid of the deleted object.

Restores domain controllers to a specific point in time, and marks objects in Active Directory as being authoritative with respect to their replication partners.

NEW QUESTION 89

- (Topic 2)

Your network contains a Network Policy Server (NPS) server named Server1. The network contains a server named SQL1 that has Microsoft SQL Server 2008 R2 installed. All servers run Windows Server 2012 R2.

You configure NPS on Server1 to log accounting data to a database on SQL1.

You need to ensure that the accounting data is captured if SQL1 fails. The solution must minimize cost.

What should you do?

- A. Implement Failover Clustering.
- B. Implement database mirroring.
- C. Run the Accounting Configuration Wizard.

D. Modify the SQL Server Logging properties.

Answer: C

Explanation:

In Windows Server 2008 R2, an accounting configuration wizard is added to the Accounting node in the NPS console. By using the Accounting Configuration wizard, you can configure the following four accounting settings:

- ? SQL logging only. By using this setting, you can configure a data link to a SQL Server that allows NPS to connect to and send accounting data to the SQL server. In addition, the wizard can configure the database on the SQL Server to ensure that the database is compatible with NPS SQL server logging.
- ? Text logging only. By using this setting, you can configure NPS to log accounting data to a text file.
- ? Parallel logging. By using this setting, you can configure the SQL Server data link and database. You can also configure text file logging so that NPS logs simultaneously to the text file and the SQL Server database.
- ? SQL logging with backup. By using this setting, you can configure the SQL Server data link and database. In addition, you can configure text file logging that NPS uses if SQL Server logging fails.

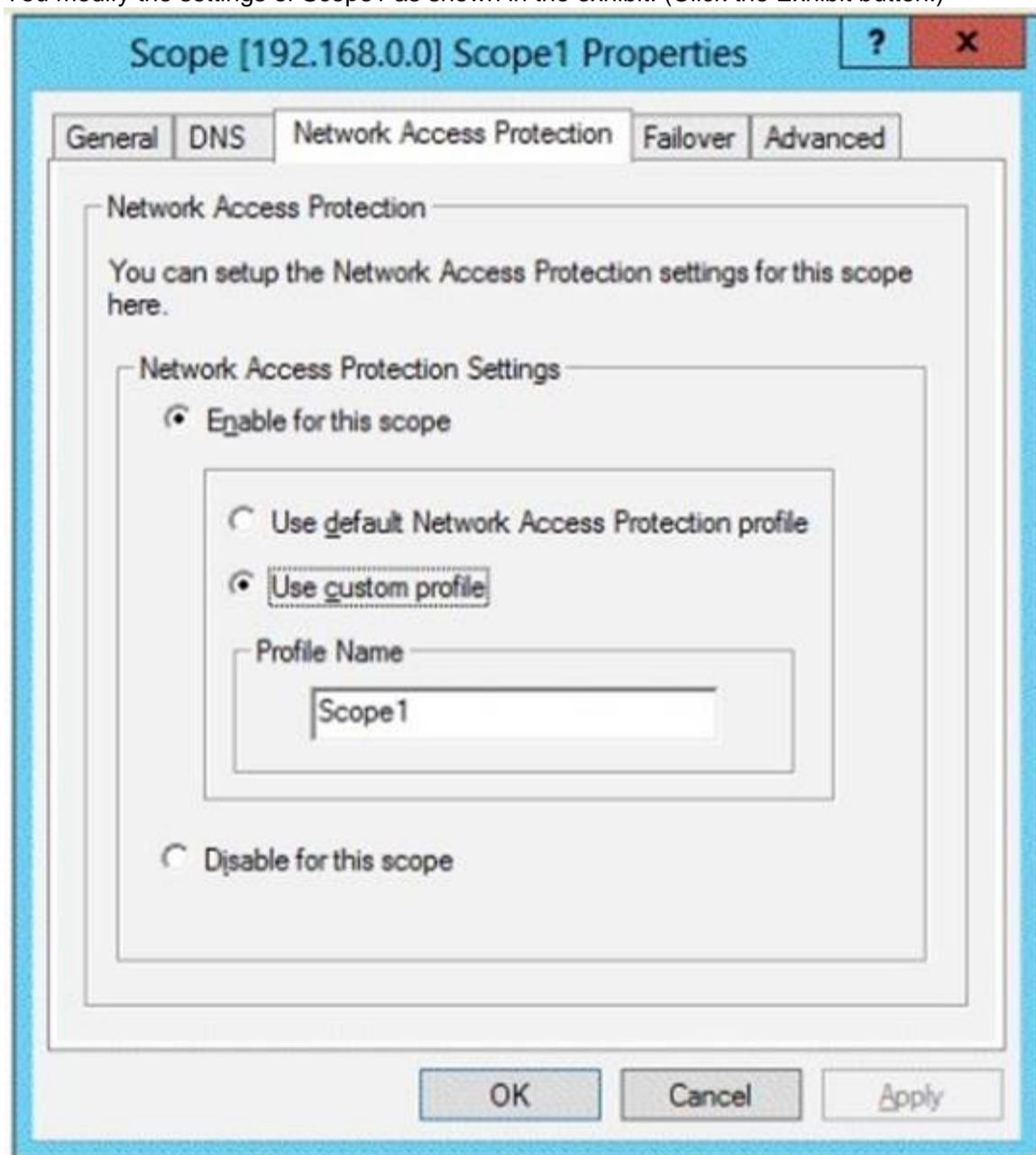
NEW QUESTION 93

- (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.)



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.

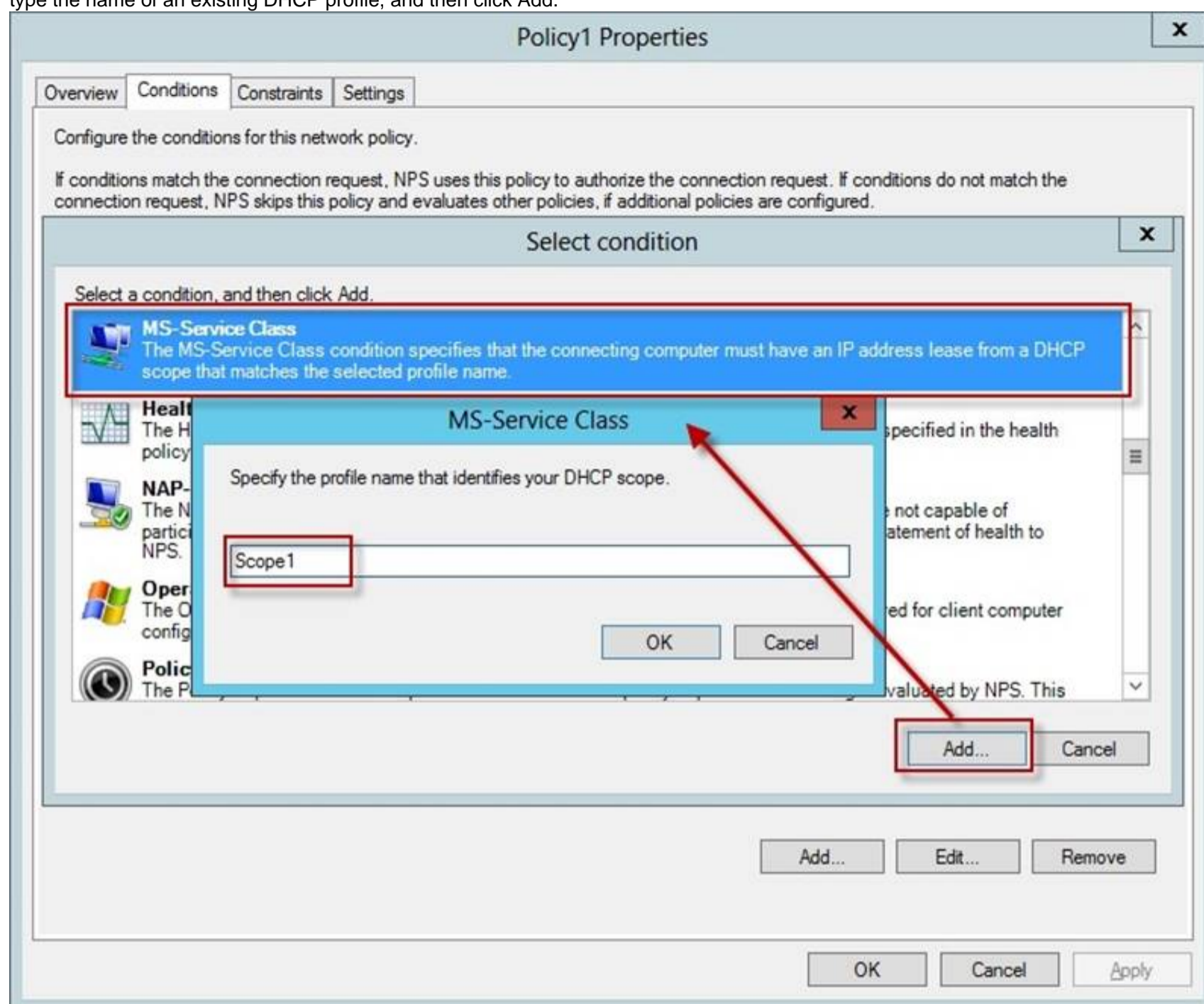
Open the NPS console, double-click Policies, click Network Policies, and then double-click the policy you want to configure.

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.



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/cc731560(v=ws.10).aspx)
[http://technet.microsoft.com/en-us/library/cc731220\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731220(v=ws.10).aspx)

NEW QUESTION 94

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2. All client computers run Windows 7.

You need to ensure that user settings are saved to \\Server1\Users\. What should you do?

- A. From the properties of each user account, configure the Home folder settings.
- B. From a Group Policy object (GPO), configure the Folder Redirection settings.
- C. From the properties of each user account, configure the User profile settings.
- D. From a Group Policy object (GPO), configure the Drive Maps preference.

Answer: C

Explanation:

If a computer is running Windows 2000 Server or later on a network, users can store their profiles on the server. These profiles are called roaming user profiles.

NEW QUESTION 96

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. You have a standard primary zone named adatum.com.

You need to provide a user named User1 the ability to modify records in the zone. Other users must be prevented from modifying records in the zone. What should you do first?

- A. Run the Zone Signing Wizard for the zone.
- B. From the properties of the zone, modify the start of authority (SOA) record.
- C. From the properties of the zone, change the zone type.
- D. Run the New Delegation Wizard for the zone.

Answer: C

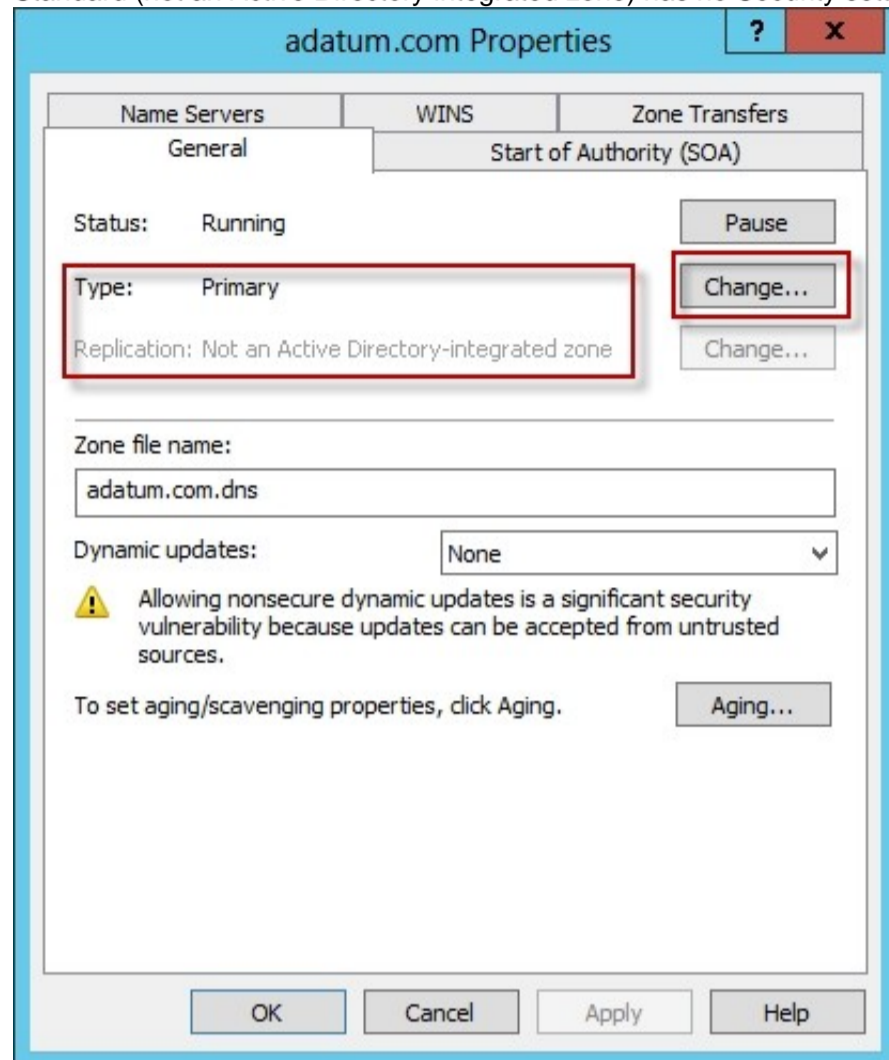
Explanation:

The Zone would need to be changed to a AD integrated zone When you use directory- integrated zones, you can use access control list (ACL) editing to secure a dnsZone object container in the directory tree. This feature provides detailed access to either the zone or a specified resource record in the zone. For example, an

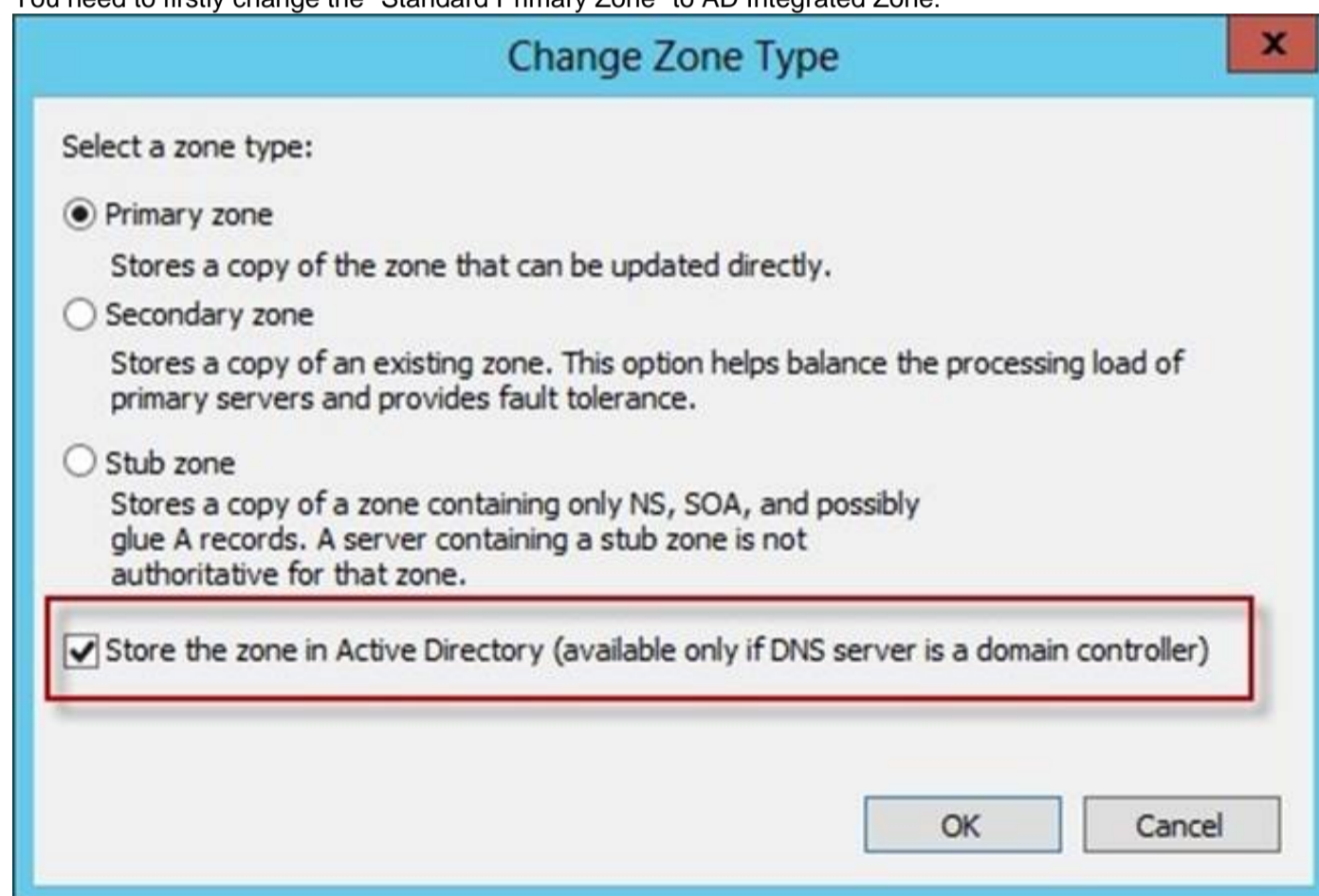
ACL for a zone resource record can be restricted so that dynamic updates are allowed only for a specified client computer or a secure group, such as a domain administrators group. This security feature is not available with standard primary zones.

DNS update security is available only for zones that are integrated into Active Directory. After you integrate a zone, you can use the access control list (ACL) editing features that are available in the DNS snap-in to add or to remove users or groups from the ACL for a specific zone or for a resource record.

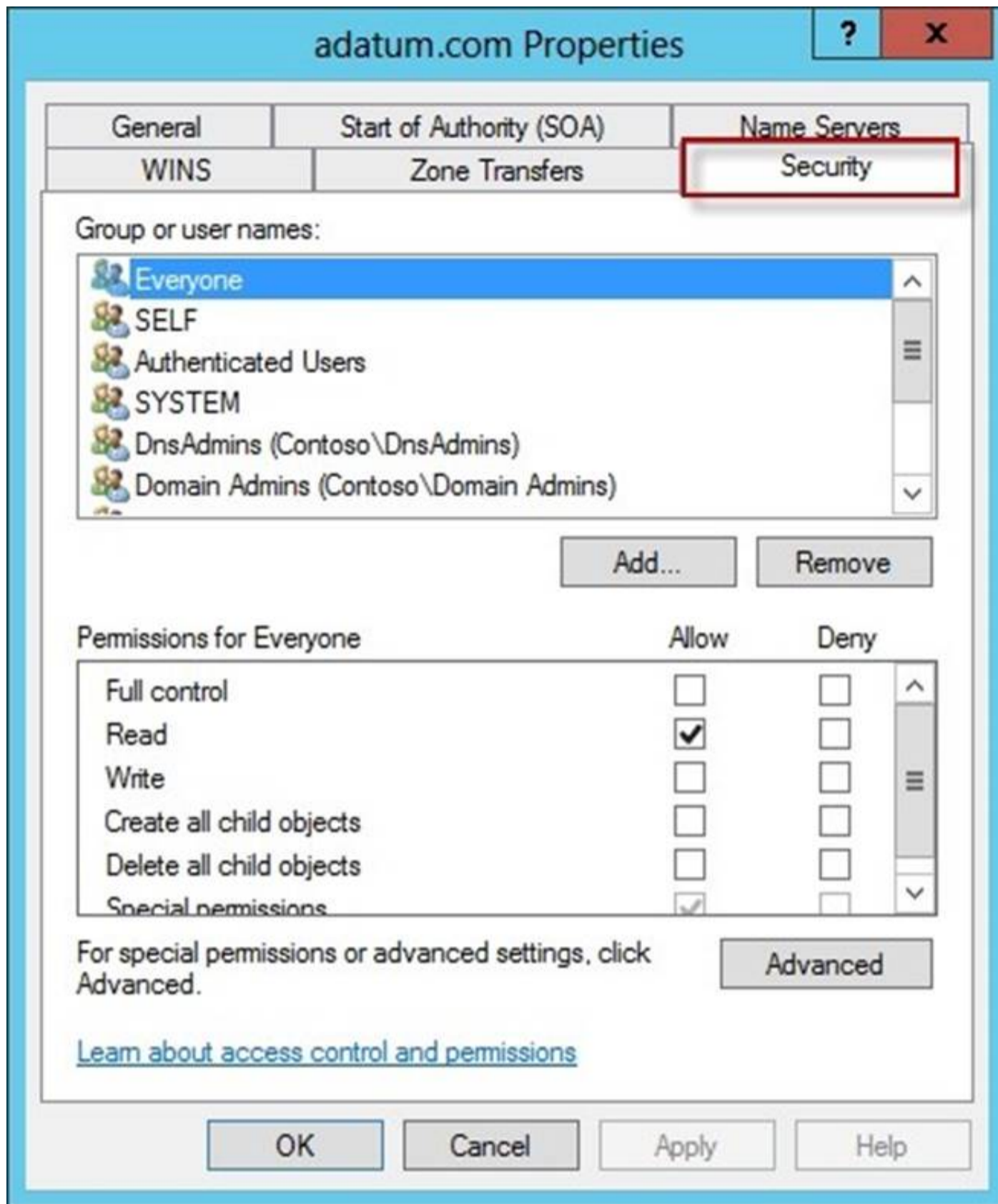
Standard (not an Active Directory integrated zone) has no Security settings:



You need to firstly change the "Standard Primary Zone" to AD Integrated Zone:



Now there's Security tab:



References:

<http://technet.microsoft.com/en-us/library/cc753014.aspx> <http://technet.microsoft.com/en-us/library/cc726034.aspx> <http://support.microsoft.com/kb/816101>

NEW QUESTION 99

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. The domain contains 10 domain controllers that run Windows Server 2012 R2.

You plan to create a new Active Directory-integrated zone named contoso.com. You need to ensure that the new zone will be replicated to only four of the domain controllers.

What should you do first?

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

Answer: A

Explanation:

Application directory partitions

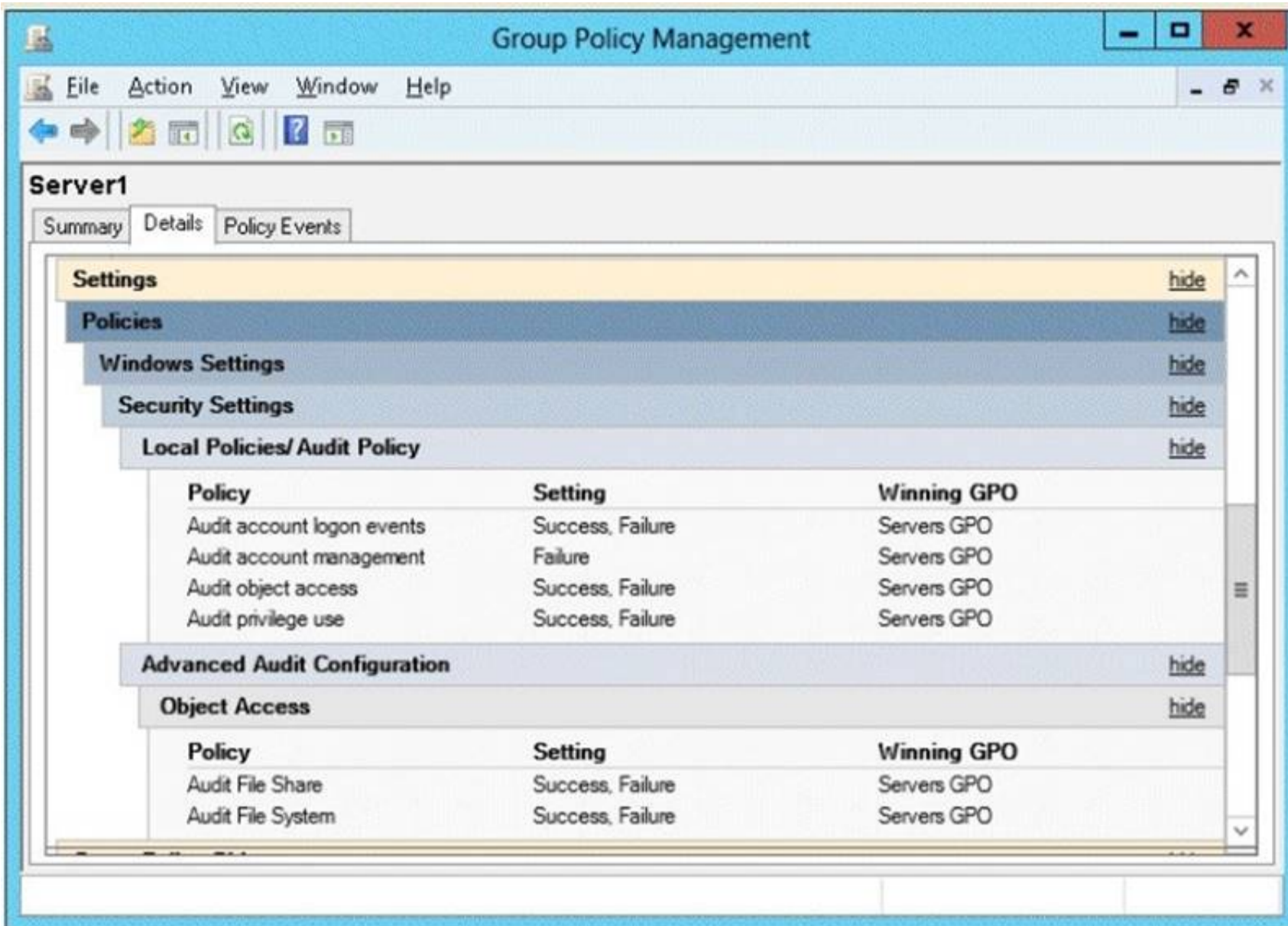
An application directory partition is a directory partition that is replicated only to specific domain controllers. A domain controller that participates in the replication of a particular application directory partition hosts a replica of that partition. Only domain controllers running Windows Server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

NEW QUESTION 104

- (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.)



You need to ensure that an entry is added to the event log whenever a local user account is created or deleted on Server1. What should you do?

- A. In Servers GPO, modify the Advanced Audit Configuration settings.
- B. On Server1, attach a task to the security log.
- C. In Servers GPO, modify the Audit Policy settings.
- D. On Server1, attach a task to the system log.

Answer: A

Explanation:

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. The following procedure shows how to prevent conflicts by blocking the application of any basic audit policy settings.

Enabling Advanced Audit Policy Configuration

Basic and advanced audit policy configurations should not be mixed. As such, it's best practice to enable Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings in Group Policy to make sure that basic auditing is disabled. The setting can be found under Computer Configuration\Policies\Security Settings\Local Policies\Security Options, and sets the SCENoApplyLegacyAuditPolicy registry key to prevent basic auditing being applied using Group Policy and the Local Security Policy MMC snap-in.

In Windows 7 and Windows Server 2008 R2, the number of audit settings for which success and failure can be tracked has increased to 53. Previously, there were nine basic auditing settings under Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy. These 53 new settings allow you to select only the behaviors that you want to monitor and exclude audit results for behaviors that are of little or no concern to you, or behaviors that create an excessive number of log entries. In addition, because Windows 7 and Windows Server 2008 R2 security audit policy can be applied by using domain Group Policy, audit policy settings can be modified, tested, and deployed to selected users and groups with relative simplicity.

Audit Policy settings

Any changes to user account and resource permissions. Any failed attempts for user logon.

Any failed attempts for resource access. Any modification to the system files.

Advanced Audit Configuration Settings

Audit compliance with important business-related and security-related rules by tracking precisely defined activities, such as:

? A group administrator has modified settings or data on servers that contain finance information.

? An employee within a defined group has accessed an important file.

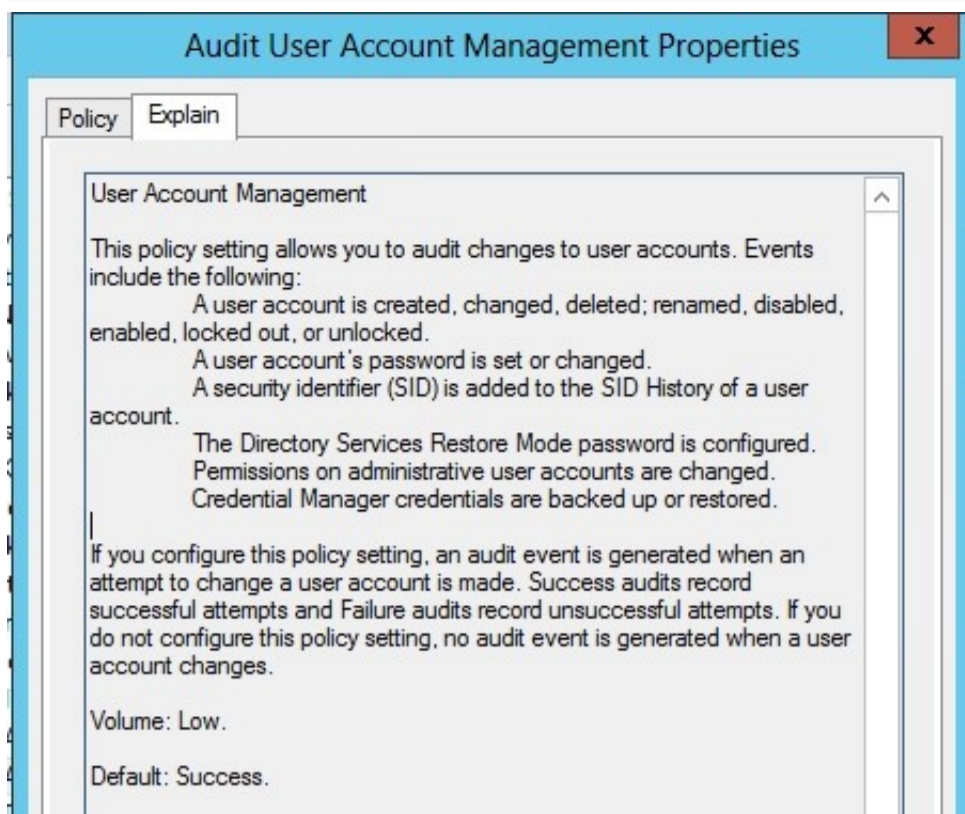
? The correct system access control list (SACL) is applied to every file and folder or registry key on a computer or file share as a verifiable safeguard against undetected access.

In Servers GPO, modify the Audit Policy settings - enabling audit account management setting will generate events about account creation, deletion and so on.

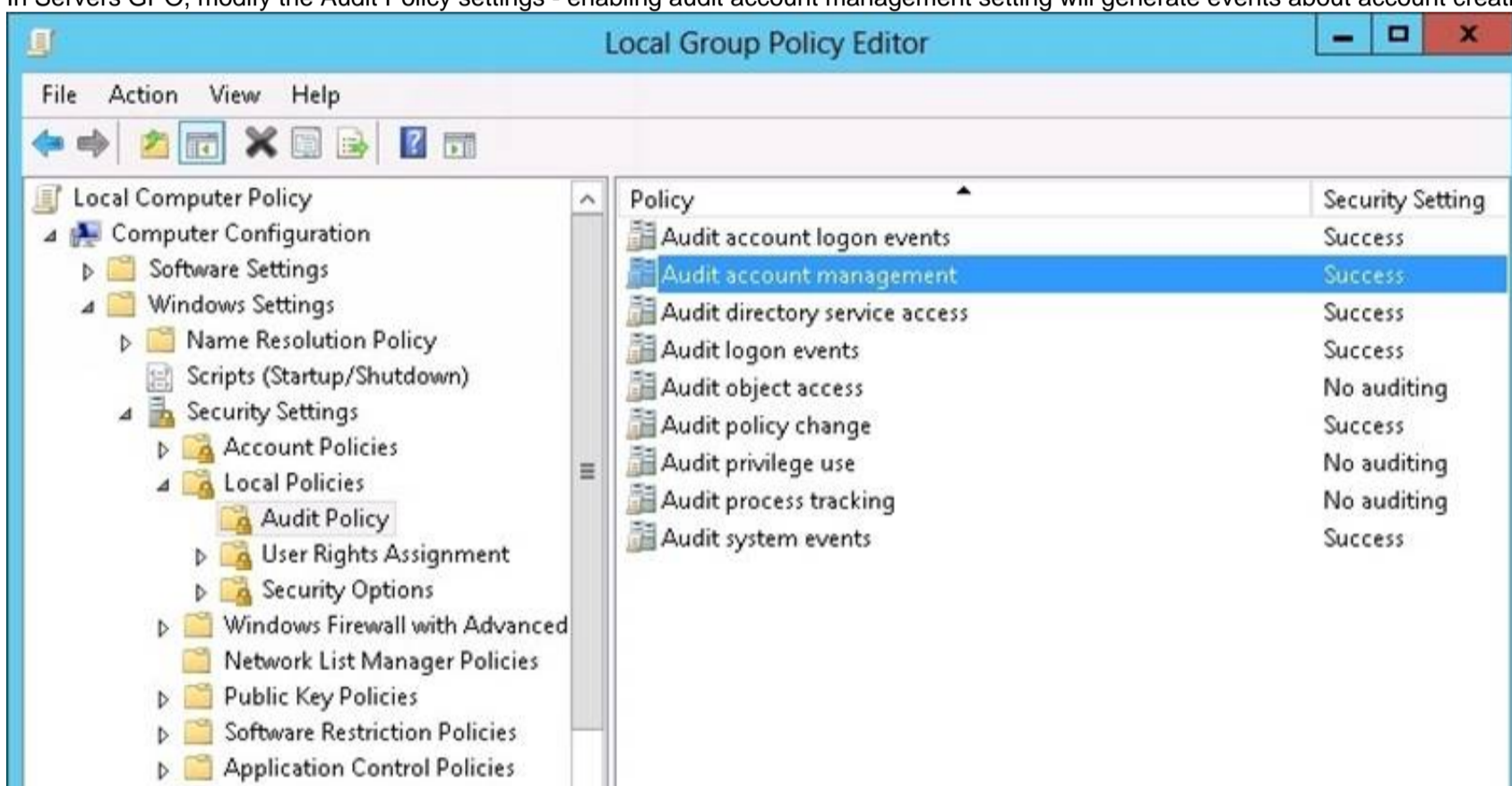
Advanced Audit Configuration Settings

Advanced Audit Configuration Settings -> Audit Policy

-> Account Management -> Audit User Account Management



In Servers GPO, modify the Audit Policy settings - enabling audit account management setting will generate events about account creation, deletion and so on.



ence:

<http://blogs.technet.com/b/abizerh/archive/2010/05/27/tracing-down-user-and-computer-account-deletion-in-active-directory.aspx>

<http://technet.microsoft.com/en-us/library/dd772623%28v=ws.10%29.aspx>

[http://technet.microsoft.com/en-us/library/jj852202\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/jj852202(v=ws.10).aspx)

<http://www.petri.co.il/enable-advanced-audit-policy-configuration-windows-server.htm>

<http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx>

http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx#BKMK_step2

NEW QUESTION 108

HOTSPOT - (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains 30 user accounts that are used for network administration. The user accounts are members of a domain global group named Group1.

You identify the security requirements for the 30 user accounts as shown in the following table.

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

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

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

Answer Area

Security setting	Configured by using
Minimum password length	<input type="text"/>
Account is sensitive and cannot be delegated	<input type="text"/>
User cannot change password	<input type="text"/>
Password never expires	<input type="text"/>

Security setting	Configured by using
Minimum password length	<input type="text"/> PSO User account properties
Account is sensitive and cannot be delegated	<input type="text"/> PSO User account properties
User cannot change password	<input type="text"/> PSO User account properties
Enforce password history	<input type="text"/> PSO User account properties

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

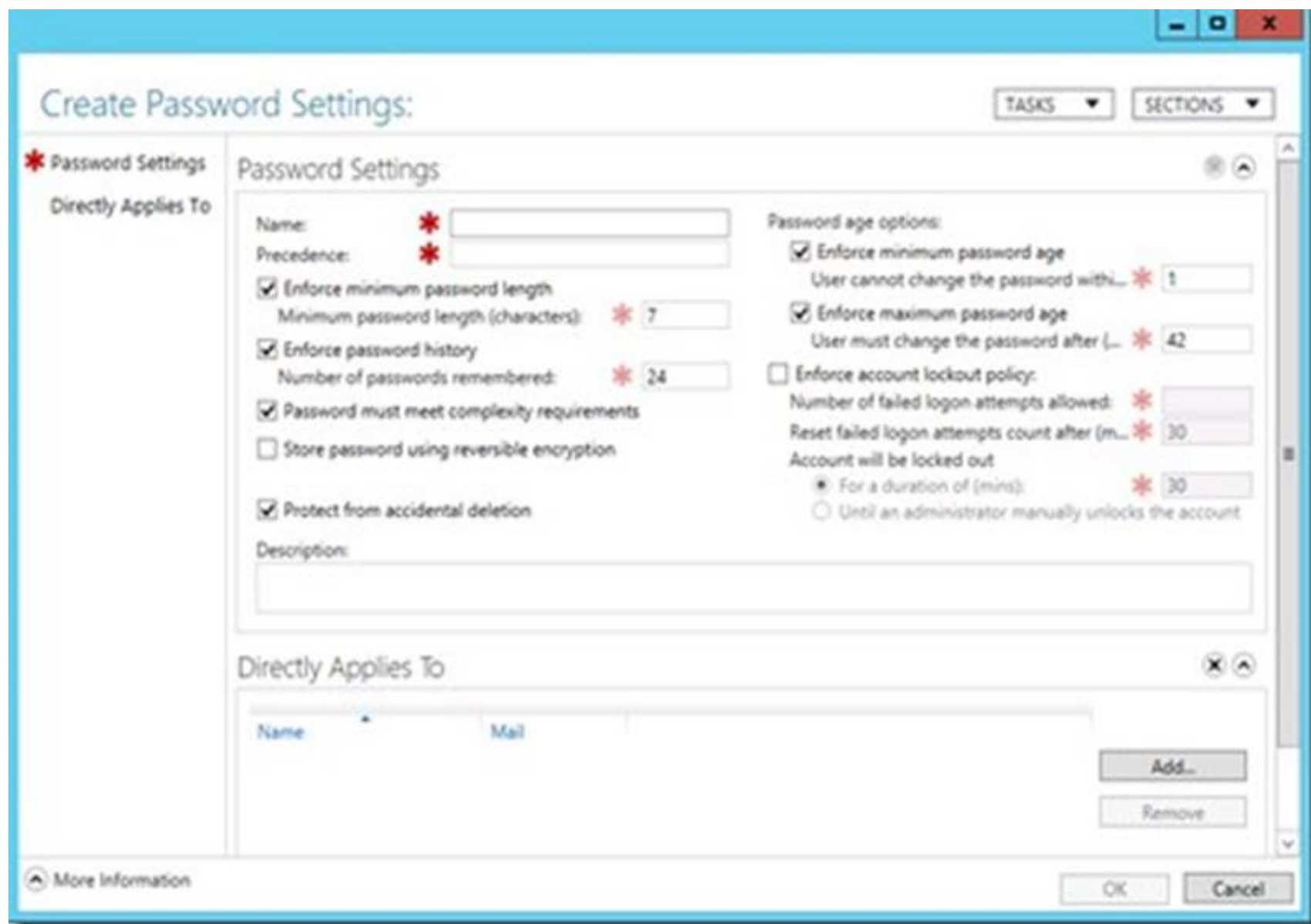
Box 1: PSO

Box 2: User Account Properties Box 3: User Account Properties Box 4: PSO

Note:

* Password Setting Object (PSO) is another name for Fine Grain Password Policies.

* Here you can see all the settings that go into a PSO.



NEW QUESTION 109

- (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. You discover that the performance of Server1 is poor. The results of a performance report generated on Server1 are shown in the following table.

Counter	Value
Processor(_Total)\% DPC Time	35
Processor(_Total)\% Interrupt Time	51
Processor(_Total)\% User Time	12
Processor(_Total)\% Privileged Time	2
Processor Information(_Total)\% Processor Time	100
Memory\Available Bytes	7,341,024,329
Memory\Pages/sec	125

You need to identify the cause of the performance issue. What should you identify?

- A. Driver malfunction
- B. Insufficient RAM
- C. Excessive paging
- D. NUMA fragmentation

Answer: A

Explanation:

Processor: %DPC Time. Much like the other values, this counter shows the amount of time that the processor spends servicing DPC requests. DPC requests are more often than not associated with the network interface.

Processor: % Interrupt Time. This is the percentage of time that the processor is spending on handling Interrupts. Generally, if this value exceeds 50% of the processor time you may have a hardware issue. Some components on the computer can force this issue and not really be a problem. For example a programmable I/O card like an old disk controller card, can take up to 40% of the CPU time. A NIC on a busy IIS server can likewise generate a large percentage of processor activity.

Processor: % User Time. The value of this counter helps to determine the kind of processing that is affecting the system. Of course the resulting value is the total amount of non-idle time that was spent on User mode operations. This generally means application code.

Processor: %Privilege Time. This is the amount of time the processor was busy with Kernel mode operations. If the processor is very busy and this mode is high, it is usually an indication of some type of NT service having difficulty, although user mode programs can make calls to the Kernel mode NT components to occasionally cause this type of performance issue.

Memory: Pages/sec. This value is often confused with Page Faults/sec. The Pages/sec counter is a combination of Pages Input/sec and Pages Output/sec counters. Recall that Page Faults/sec is a combination of hard page faults and soft page faults. This counter, however, is a general indicator of how often the system is using the hard drive to store or retrieve memory associated data.

References:
<http://technet.microsoft.com/en-us/library/cc768048.aspx>

NEW QUESTION 111

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

An organizational unit (OU) named OU1 contains 200 client computers that run Windows 8 Enterprise. A Group Policy object (GPO) named GPO1 is linked to OU1.

You make a change to GPO1.

You need to force all of the computers in OU1 to refresh their Group Policy settings immediately. The solution must minimize administrative effort.

Which tool should you use?

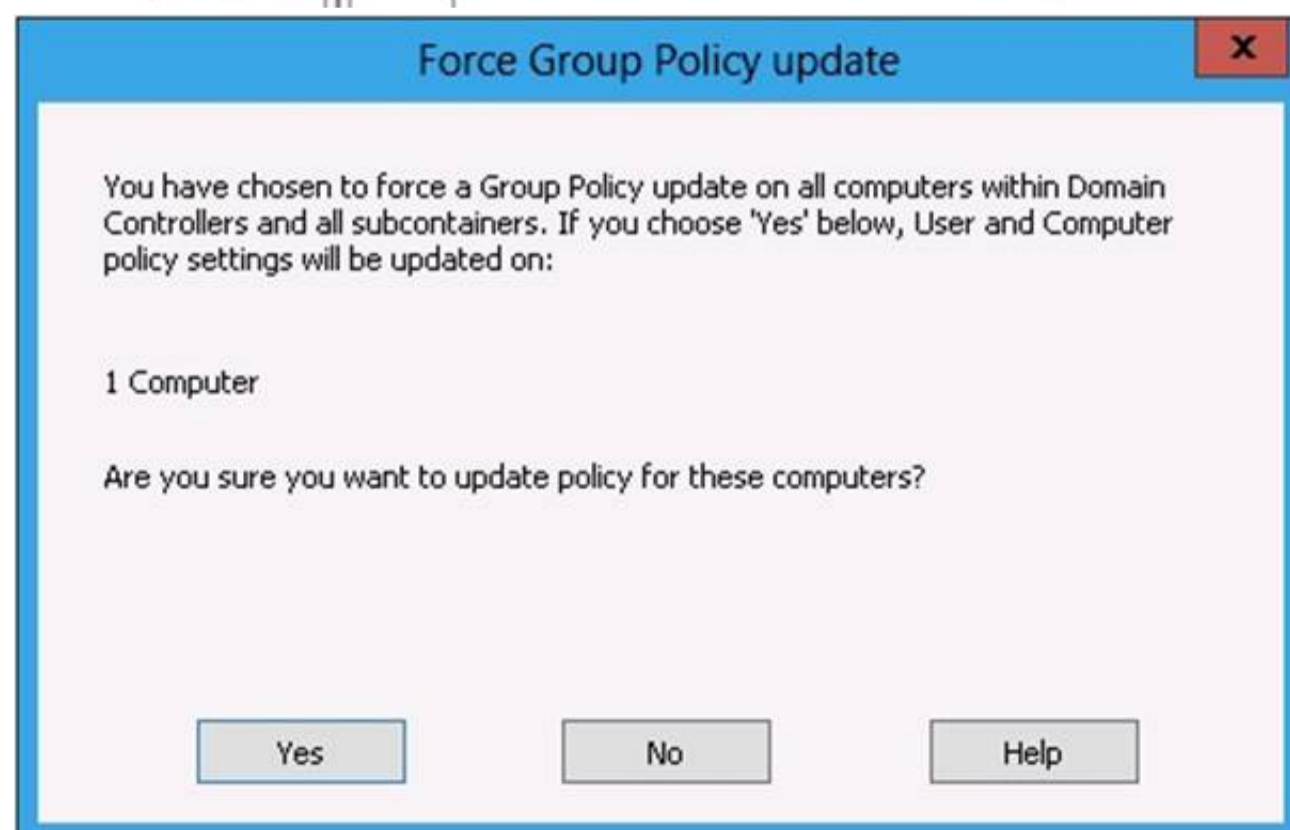
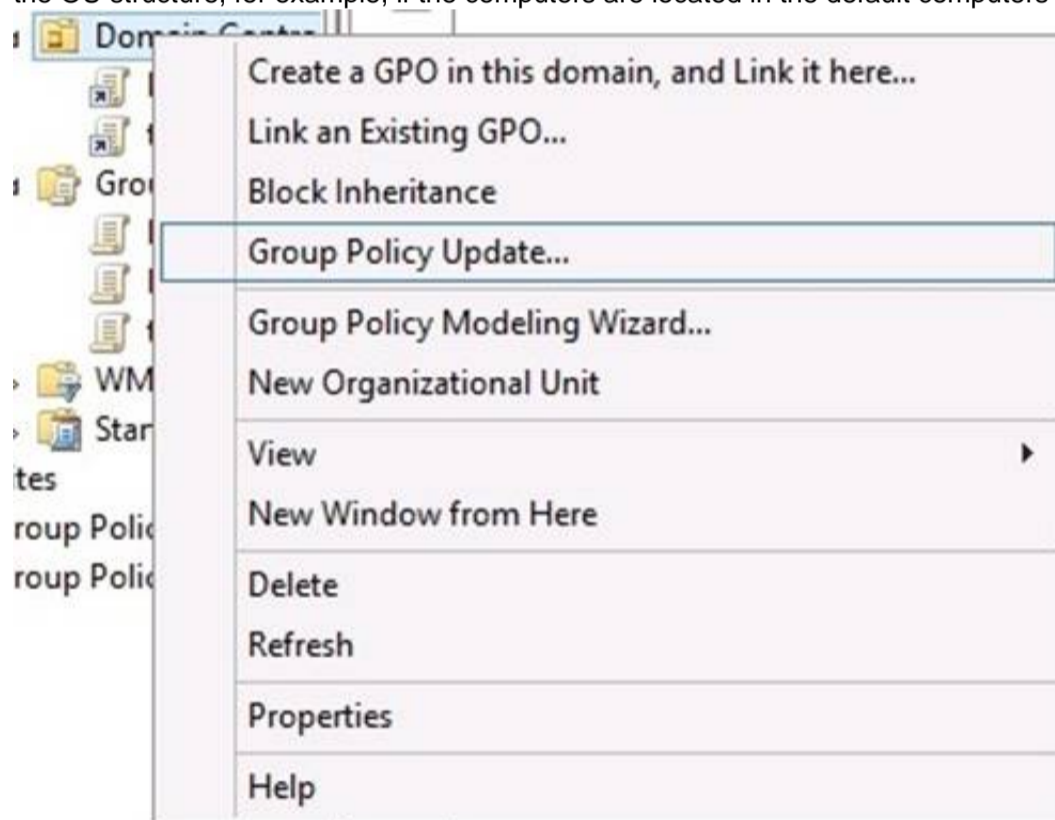
- A. The Secedit command
- B. Group Policy Management Console (GPMC)
- C. Server Manager
- D. The Gpupdate command

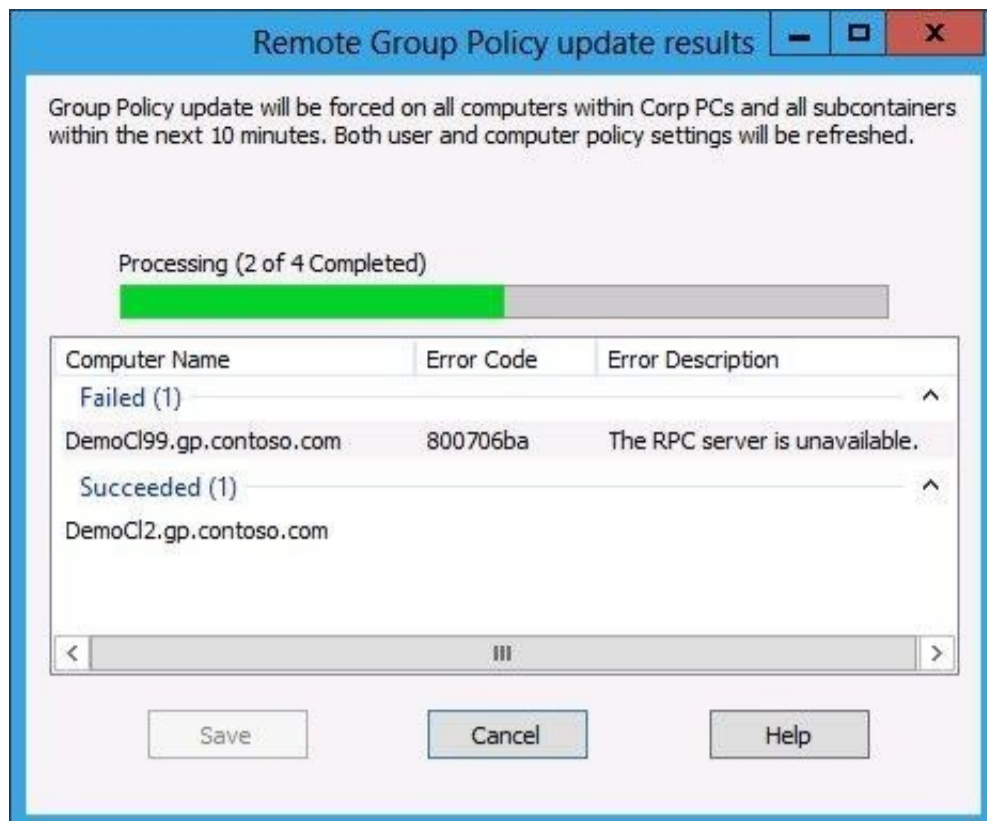
Answer: B

Explanation:

In the previous versions of Windows, this was accomplished by having the user run GpUpdate.exe on their computer.

Starting with Windows Server® 2012 and Windows® 8, you can now remotely refresh Group Policy settings for all computers in an OU from one central location through the Group Policy Management Console (GPMC). Or you can use the Invoke-GPUdatecmdlet to refresh Group Policy for a set of computers, not limited to the OU structure, for example, if the computers are located in the default computers container.





<http://technet.microsoft.com/en-us/library/jj134201.aspx>

<http://blogs.technet.com/b/grouppolicy/archive/2012/11/27/group-policy-in-windows-server-2012-using-remote-gpupdate.aspx>

NEW QUESTION 112

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named IT and an OU named Sales. All of the help desk user accounts are located in the IT OU. All of the sales user accounts are located in the Sales OU. The Sales OU contains a global security group named G_Sales. The IT OU contains a global security group named G_HelpDesk.

You need to ensure that members of G_HelpDesk can perform the following tasks:

? Reset the passwords of the sales users.

? Force the sales users to change their password at their next logon.

What should you do?

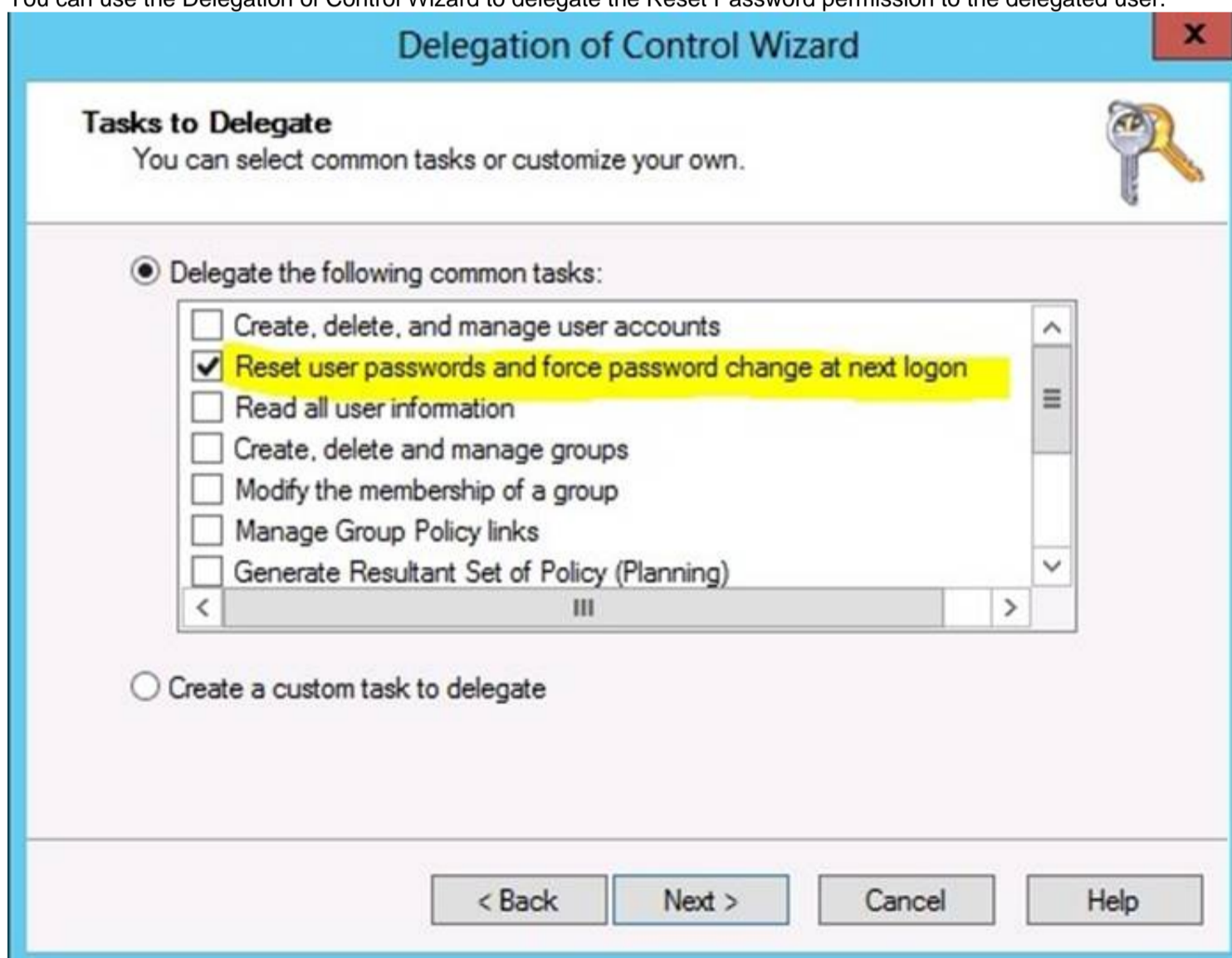
- A. Run the Set-ADAccountPasswordcmdlet and specify the -identity parameter.
- B. Right-click the Sales OU and select Delegate Control.
- C. Right-click the IT OU and select Delegate Control.
- D. Run the Set-ADFineGrainedPasswordPolicycmdlet and specify the -identity parameter.

Answer: B

Explanation:

G_HelpDesk members need to be allowed to delegate control on the Sales OU as it contains the sales users (G_Sales)

You can use the Delegation of Control Wizard to delegate the Reset Password permission to the delegated user.



References:

<http://support.microsoft.com/kb/296999/en-us>

<http://support.microsoft.com/kb/296999/en-us>
<http://technet.microsoft.com/en-us/library/cc732524.aspx>

NEW QUESTION 114

DRAG DROP - (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed.

All of the VPN servers on your network use Server1 for RADIUS authentication. You create a security group named Group1.

You need to configure Network Policy and Access Services (NPAS) to meet the following requirements:

? Ensure that only the members of Group1 can establish a VPN connection to the VPN servers.

? Allow only the members of Group1 to establish a VPN connection to the VPN

servers if the members are using client computers that run Windows 8 or later. Which type of policy should you create for each requirement?

To answer, drag the appropriate policy types to the correct requirements. Each policy type 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.

Policy Types	Answer Area
Connection Request Policies	Ensure that only the members of Group1 can establish a VPN connection to the VPN servers. Policy type
Health Policies	
Network Policies	Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later. Policy type

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy Types	Answer Area
Connection Request Policies	Ensure that only the members of Group1 can establish a VPN connection to the VPN servers. Network Policies
Health Policies	
Network Policies	Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later. Network Policies

NEW QUESTION 117

- (Topic 2)

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	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. What should you do?

- A. Transfer the schema master to DC6.
- B. Transfer the PDC emulator to DC5.
- C. Transfer the schema master to DC4.
- D. Transfer the PDC emulator to DC2.

Answer: D

Explanation:

A deployed Windows Server 2012 domain controller (virtualized or physical) that hosts the PDC emulator role (DC1). To verify whether the PDC emulator role is hosted on a Windows Server 2012 domain controller, run the following Windows PowerShell command:
Get-ADComputer (Get-ADDomainController –Discover –Service "PrimaryDC").name
–Propertyoperatingsystemversion|fl
Reference: http://technet.microsoft.com/en-us/library/hh831734.aspx#steps_deploy_vdc

NEW QUESTION 119

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

Answer: C

Explanation:

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

NEW QUESTION 120

- (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 122

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.

Server1 and Server2 are nodes in a Hyper-V cluster named Cluster1. Cluster1 hosts 10 virtual machines. All of the virtual machines run Windows Server 2012 R2 and are members of the domain.

You need to ensure that the first time a service named Service1 fails on a virtual machine, the virtual machine is moved to a different node.

You configure Service1 to be monitored from Failover Cluster Manager. What should you configure on the virtual machine?

- A. From the General settings, modify the Startup type.
- B. From the General settings, modify the Service status.
- C. From the Recovery settings of Service1, set the First failure recovery action to Take No Action.
- D. From the Recovery settings of Service1, set the First failure recovery action to Restart the Service.

Answer: C

Explanation:

Configure the virtual machine to take no action through Hyper-V if the physical computer shuts down by modifying the Automatic Stop Action setting to None.

Virtual machine state must be managed through the Failover Clustering feature.

Virtual machine application monitoring and management

In clusters running Windows Server 2012, administrators can monitor services on clustered virtual machines that are also running Windows Server 2012. This functionality extends the high-level monitoring of virtual machines that is implemented in Windows Server 2008 R2 failover clusters. If a monitored service in a virtual machine fails, the service can be restarted, or the clustered virtual machine can be restarted or moved to another node (depending on service restart settings and cluster failover settings).

This feature increases the uptime of high availability services that are running on virtual machines within a failover cluster.

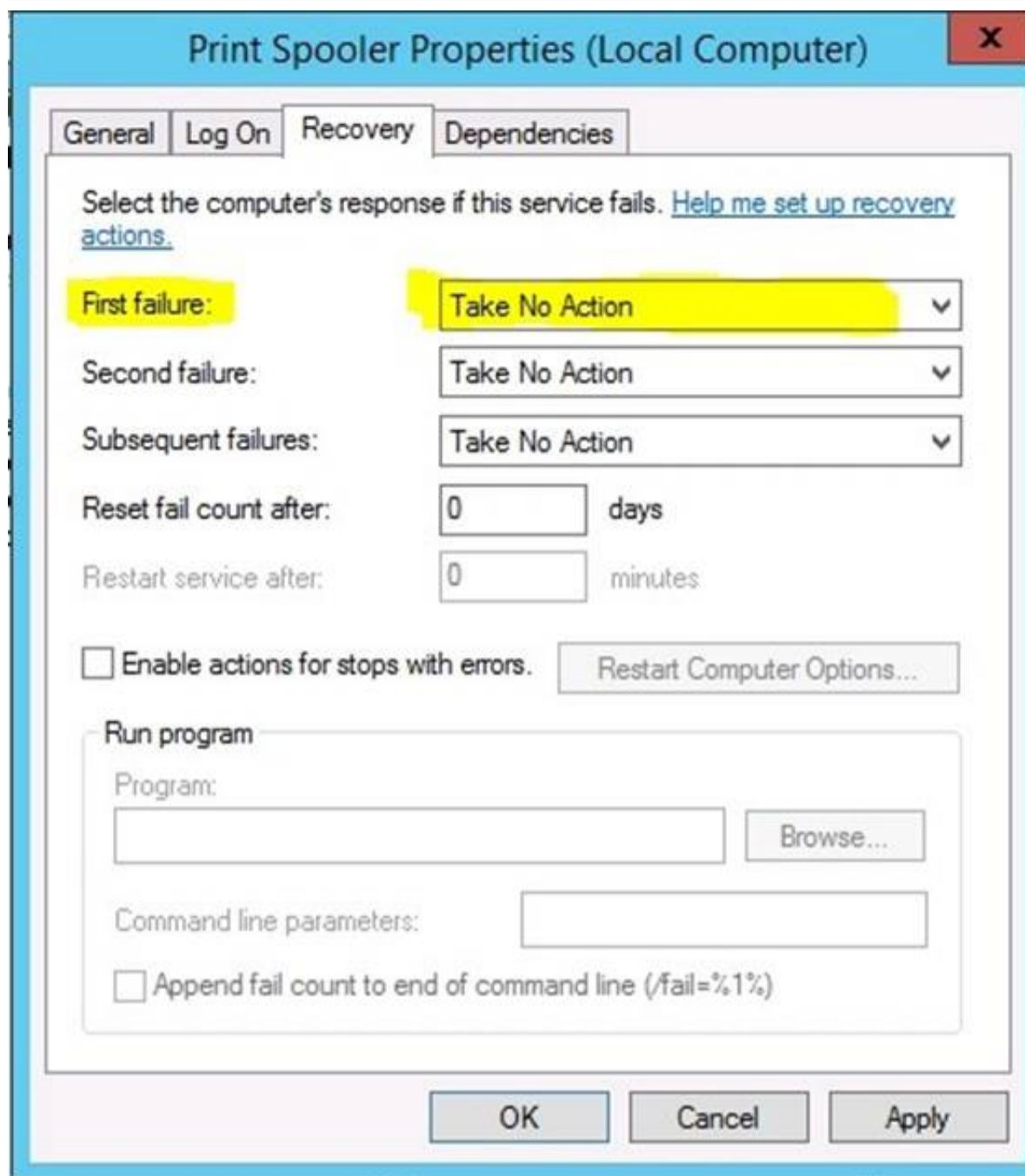
Windows Server 2012 Failover Cluster introduces a new capability for Hyper-V virtual machines (VMs), which is a basic monitoring of a service within the VM which causes the VM to be rebooted should the monitored service fail three times. For this feature to work the following must be configured:

? Both the Hyper-V servers must be Windows Server 2012 and the guest OS running in the VM must be Windows Server 2012.

? The host and guest OSs are in the same or at least trusting domains.

? The Failover Cluster administrator must be a member of the local administrator's group inside the VM.

Ensure the service being monitored is set to Take No Action (see screen shot below) within the guest VM for Subsequent failures (which is used after the first and second failures) and is set via the Recovery tab of the service properties within the Services application (services. msc).



Print Spooler Properties (Local Computer)

General Log On **Recovery** Dependencies

Select the computer's response if this service fails. [Help me set up recovery actions.](#)

First failure: Take No Action

Second failure: Take No Action

Subsequent failures: Take No Action

Reset fail count after: 0 days

Restart service after: 0 minutes

☐ Enable actions for stops with errors. Restart Computer Options...

Run program

Program: Browse...

Command line parameters:

☐ Append fail count to end of command line (/fail=%1%)

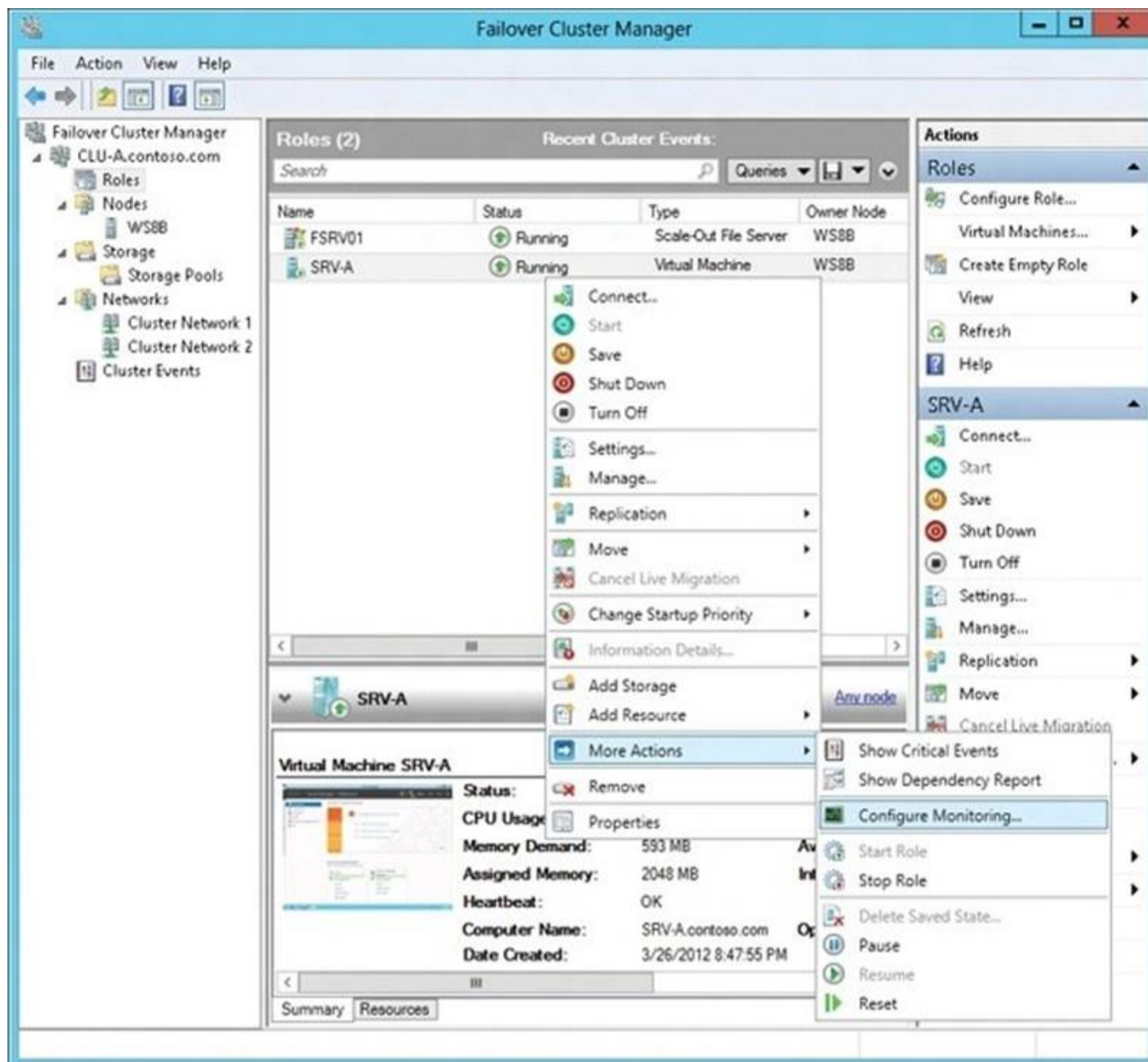
OK Cancel Apply

Within the guest VM, ensure the Virtual Machine Monitoring firewall exception is enabled for the Domain network by using the Windows Firewall with Advanced Security application or by using the Windows PowerShell command below: `Set-NetFirewallRule -DisplayGroup "Virtual Machine Monitoring" -Enabled True`. After the above is true, enabling the monitoring is a simple process:

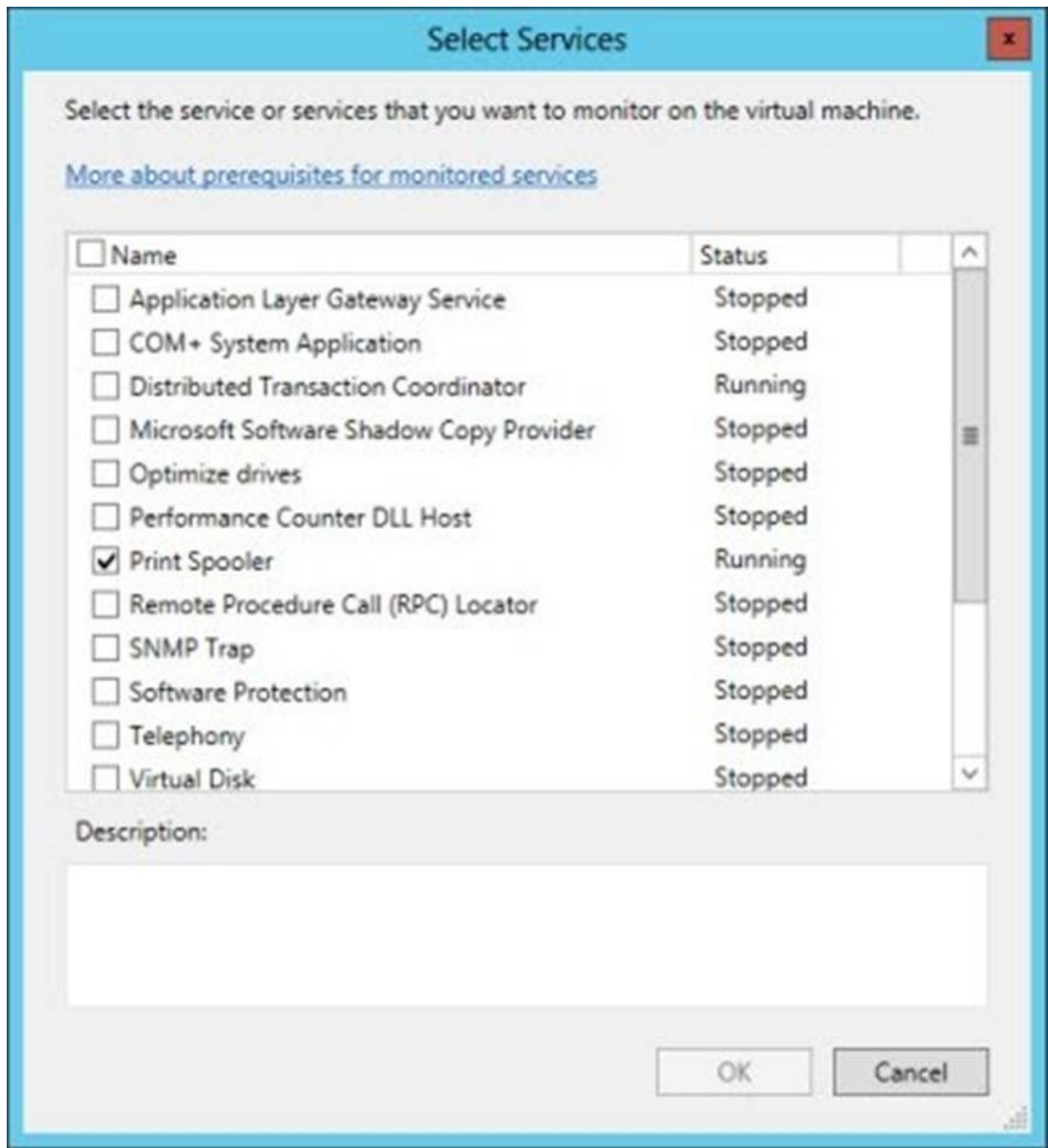
? Launch the Failover Cluster Manager tool.

? Navigate to the cluster - Roles.

? Right click on the virtual machine role you wish to enable monitoring for and under More Actions select Configure Monitoring.



? The services running inside the VM will be gathered and check the box for the services that should be monitored and click OK.



You are done!

Monitoring can also be enabled using the Add-ClusterVMMonitoredItemcmdlet and - VirtualMachine, with the -Service parameters, as the example below shows:

PS C:\Windows\system32> Add-ClusterVMMonitoredItem -VirtualMachine savdaltst01 - Service spooler

References:

<http://sportstoday.us/technology/windows-server-2012---continuous-availability-%28part-4%29---failover-clustering-enhancements---virtual-machine-monitoring-.aspx>

<http://windowsitpro.com/windows-server-2012/enable-windows-server-2012-failover-cluster-hyper-v-vm-monitoring>

<http://technet.microsoft.com/en-us/library/cc742396.aspx>

NEW QUESTION 123

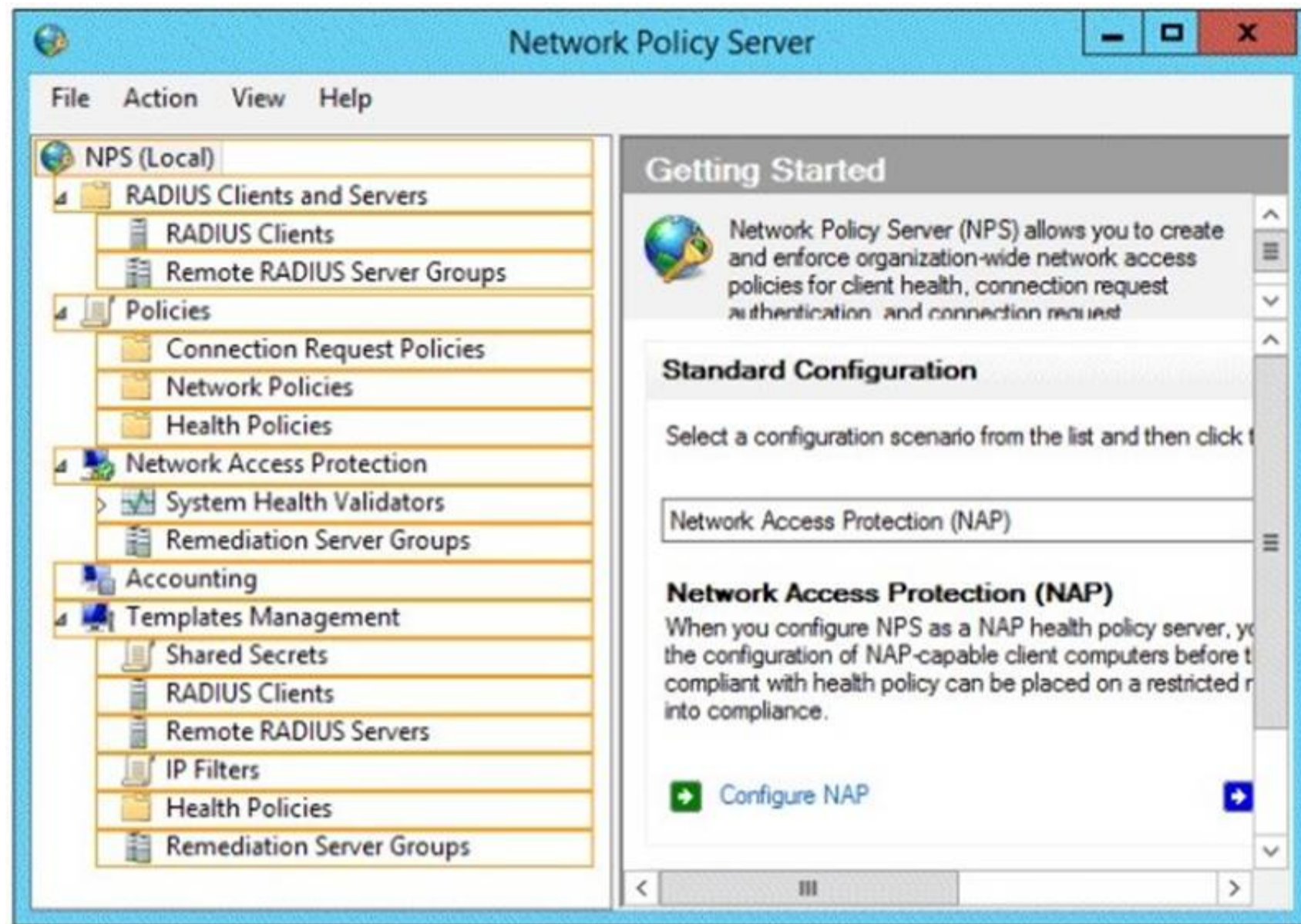
HOTSPOT - (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has the Network Policy Server server role installed. The domain contains a server named Server2 that is configured for RADIUS accounting.

Server1 is configured as a VPN server and is configured to forward authentication requests to Server2.

You need to ensure that only Server2 contains event information about authentication requests from connections to Server1.

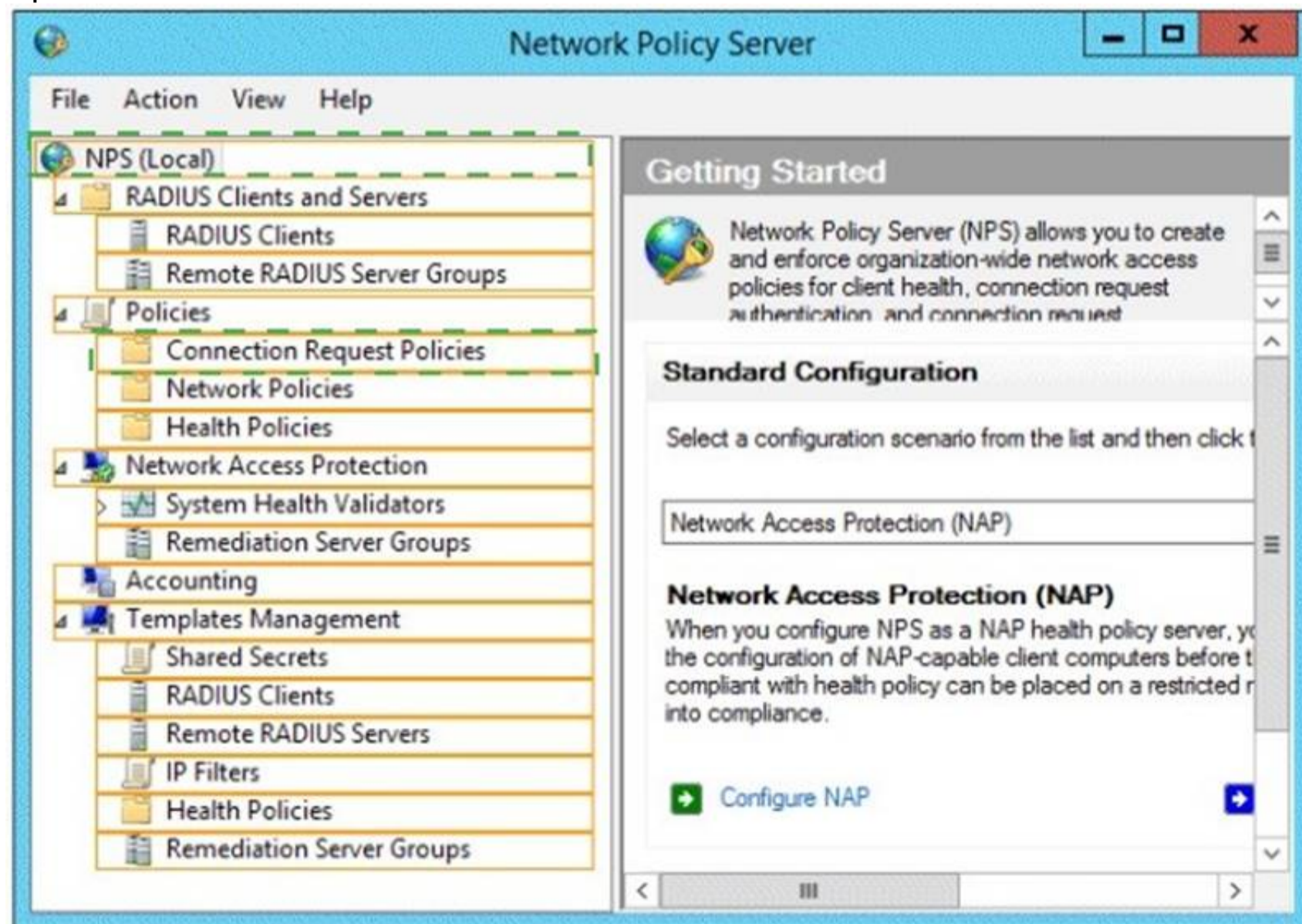
Which two nodes should you configure from the Network Policy Server console? To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 126

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. All domain controllers run Windows Server 2012 R2. The domain contains a virtual

machine named DC2.

On DC2, you run Get-ADDCCloningExcludedApplicationList and receive the output shown in the following table.

Name	Type
App1	Service

You need to ensure that you can clone DC2.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- ☐ A. Create an empty file named DCCloneConfig.xml.
- ☐ B. Add the following information to the DCCloneConfigSchema.xsd file:
- ```
<AllowList>
 <Allow>
 <Name>App1</Name>
 <Type>Service</Type>
 </Allow>
</AllowList>
```
- ☐ C. Create an empty file named CustomDCCloneAllowList.xml.
- ☐ D. Create a file named DCCloneConfig.xml that contains the following information:
- ```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```
- ☐ E. Create a file named CustomDCCloneAllowList.xml that contains the following information:
- ```
<AllowList>
 <Allow>
 <Name>App1</Name>
 <Type>Service</Type>
 </Allow>
</AllowList>
```

- A. Option A  
 B. Option B  
 C. Option C  
 D. Option D  
 E. Option E

**Answer:** AE

#### Explanation:

Because domain controllers provide a distributed environment, you could not safely clone an Active Directory domain controller in the past.

Before, if you cloned any server, the server would end up with the same domain or forest, which is unsupported with the same domain or forest. You would then have to run sysprep, which would remove the unique security information before cloning and then promote a domain controller manually. When you clone a domain controller, you perform safe cloning, which a cloned domain controller automatically runs a subset of the sysprep process and promotes the server to a domain controller automatically.

The four primary steps to deploy a cloned virtualized domain controller are as follows:

? Grant the source virtualized domain controller the permission to be cloned by adding the source virtualized domain controller to the Cloneable Domain Controllers group.

? Run Get-ADDCCloningExcludedApplicationListcmdlet in Windows PowerShell to determine which services and applications on the domain controller are not compatible with the cloning.

? Run New-ADDCCloneConfigFile to create the clone configuration file, which is stored in the C:\Windows\NTDS.

? In Hyper-V, export and then import the virtual machine of the source domain controller.

Run Get-ADDCCloningExcludedApplicationListcmdlet In this procedure, run the Get- ADDCCloningExcludedApplicationListcmdlet on the source virtualized domain controller to identify any programs or services that are not evaluated for cloning. You need to run the Get-ADDCCloningExcludedApplicationListcmdlet before the New- ADDCCloneConfigFilecmdlet because if the New-ADDCCloneConfigFilecmdlet detects an excluded application, it will not create a DCCloneConfig.xml file. To identify applications or services that run on a source domain controller which have not been evaluated for cloning. Get-ADDCCloningExcludedApplicationList

Get-ADDCCloningExcludedApplicationList -GenerateXml

The clone domain controller will be located in the same site as the source domain controller unless a different site is specified in the DCCloneConfig.xml file.

Note:

? The Get-ADDCCloningExcludedApplicationListcmdlet searches the local domain controller for programs and services in the installed programs database, the services control manager that are not specified in the default and user defined inclusion list. The applications in the resulting list can be added to the user defined

exclusion list if they are determined to support cloning. If the applications are not cloneable, they should be removed from the source domain controller before the clone media is created. Any application that appears in cmdlet output and is not included in the user defined inclusion list will force cloning to fail.

? The Get-ADDCCloningExcludedApplicationListcmdlet needs to be run before the New- ADDCCloneConfigFilecmdlet is used because if the New- ADDCCloneConfigFilecmdlet detects an excluded application, it will not create a DCCloneConfig.xml file.

? DCCloneConfig.xml is an XML configuration file that contains all of the settings the cloned DC will take when it boots. This includes network settings, DNS, WINS, AD site name, new DC name and more. This file can be generated in a few different ways.

The New-ADDCCloneConfigcmdlet in PowerShell By hand with an XML editor

By editing an existing config file, again with an XML editor (Notepad is not an XML editor.)

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

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

Name

WLMS
Type

Service

PS C:\Users\Administrator.DC01>
```

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

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

Name

WLMS
Type

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>
```

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

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

Name

WLMS
Type

Service

CustomDCCloneAllowList - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<dc:CustomDCCloneAllowList xmlns:dc="uri:microsoft.com:schemas:CustomDCCloneAllowList">
 <Allow>
 <Name>WLMS</Name>
 <Type>Service</Type>
 </Allow>
</dc:CustomDCCloneAllowList>
```

You can populate the XML file. . . . doesn't need to be empty. . . .

```
Administrator: Windows PowerShell
PS C:\Users\Administrator.DC01> New-ADDCCloneConfigFile -Static -IPv4Address 10.10.10.202 -IPv4DefaultGateway 10.10.10.1
-IPv4SubnetMask 255.255.255.0 -IPv4DNSResolver 10.10.10.73,10.10.10.202 -CloneComputerName DC02 -SiteName Default-First
-Site-Name
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or later.
Passed: The domain controller hosting the PDC FSMO role (DC01.accusource.local) was located and running Windows Server 2012 or later.

Verifying authorization: Checking if this domain controller is a member of the 'Cloneable Domain Controllers' group...
Located the local domain controller: (DC01.accusource.local).
Querying the 'Cloneable Domain Controllers' group...
Pass: The local domain controller is a member of the 'Cloneable Domain Controllers' group.

Starting test: Validating the cloning allow list.
NOTE: C:\Windows\NTDS\CustomDCCloneAllowList.xml is being used as the defined inclusion list.
No excluded applications were detected.
Pass: No excluded applications were detected.

No valid clone configuration files were found at any of the supported locations.
All preliminary validation checks passed.

Starting creation of the clone configuration file...
Finding the path to the Directory Service database...
The clone configuration file was generated at:
C:\Windows\NTDS\DCCloneConfig.xml
Generating the clone configuration file content...
The clone configuration file has been created.

PS C:\Users\Administrator.DC01>
```

DCCloneConfig - Notepad

File Edit Format View Help

```
<?xml version="1.0"?>
<d3c:DCCloneConfig xmlns:d3c="uri:microsoft.com:schemas:DCCloneConfig">
 <ComputerName>DC02</ComputerName>
 <SiteName>Default-First-Site-Name</SiteName>
 <IPSettings>
 <IPv4Settings>
 <StaticSettings>
 <Address>10.10.10.202</Address>
 <SubnetMask>255.255.255.0</SubnetMask>
 <DefaultGateway>10.10.10.1</DefaultGateway>
 <DNSResolver>10.10.10.73</DNSResolver>
 <DNSResolver>10.10.10.202</DNSResolver>
 </StaticSettings>
 </IPv4Settings>
 </IPSettings>
</d3c:DCCloneConfig>
```

References:

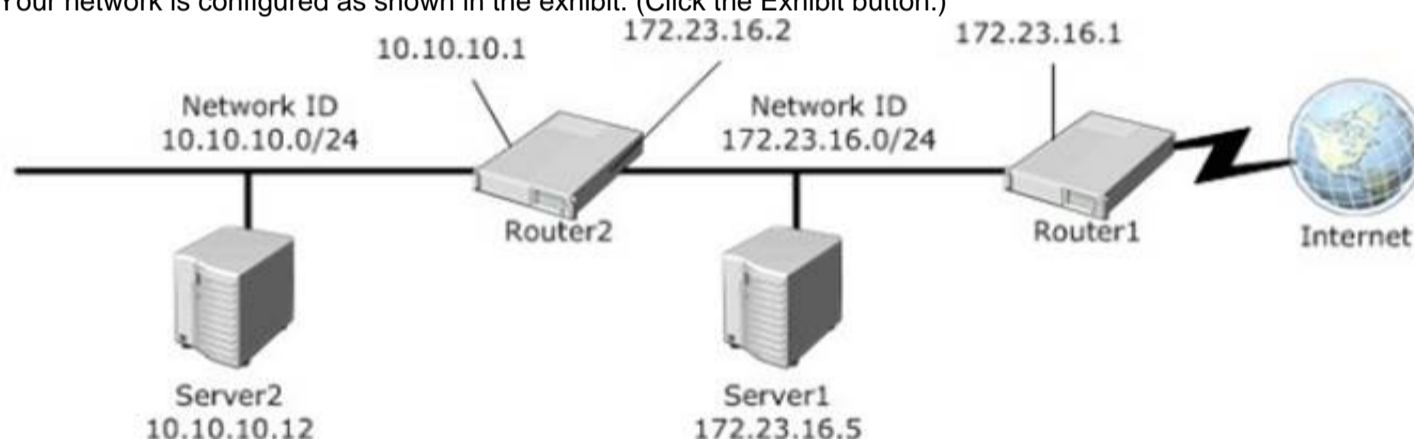
<http://technet.microsoft.com/en-us/library/hh831734.aspx>

<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>

#### NEW QUESTION 128

- (Topic 2)

Your network is configured as shown in the exhibit. (Click the Exhibit button.)



Server1 regularly accesses Server2.

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

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

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

**Answer:** A

#### Explanation:

Destination - specifies either an IP address or host name for the network or host. subnetmask - specifies a subnet mask to be associated with this route entry. If subnetmask

is not specified, 255.255.255.255 is used.

gateway - specifies either an IP address or host name for the gateway or router to use when forwarding.

costmetric - assigns an integer cost metric (ranging from 1 through 9,999) to be used in calculating the fastest, most reliable, and/or least expensive routes. If costmetric is not specified, 1 is used.

interface - specifies the interface to be used for the route that uses the interface number. If an interface is not specified, the interface to be used for the route is determined from the gateway IP address.

References:

<http://support.microsoft.com/kb/299540/en-us>

<http://technet.microsoft.com/en-us/library/cc757323%28v=ws.10%29.aspx>

#### NEW QUESTION 130

HOTSPOT - (Topic 2)

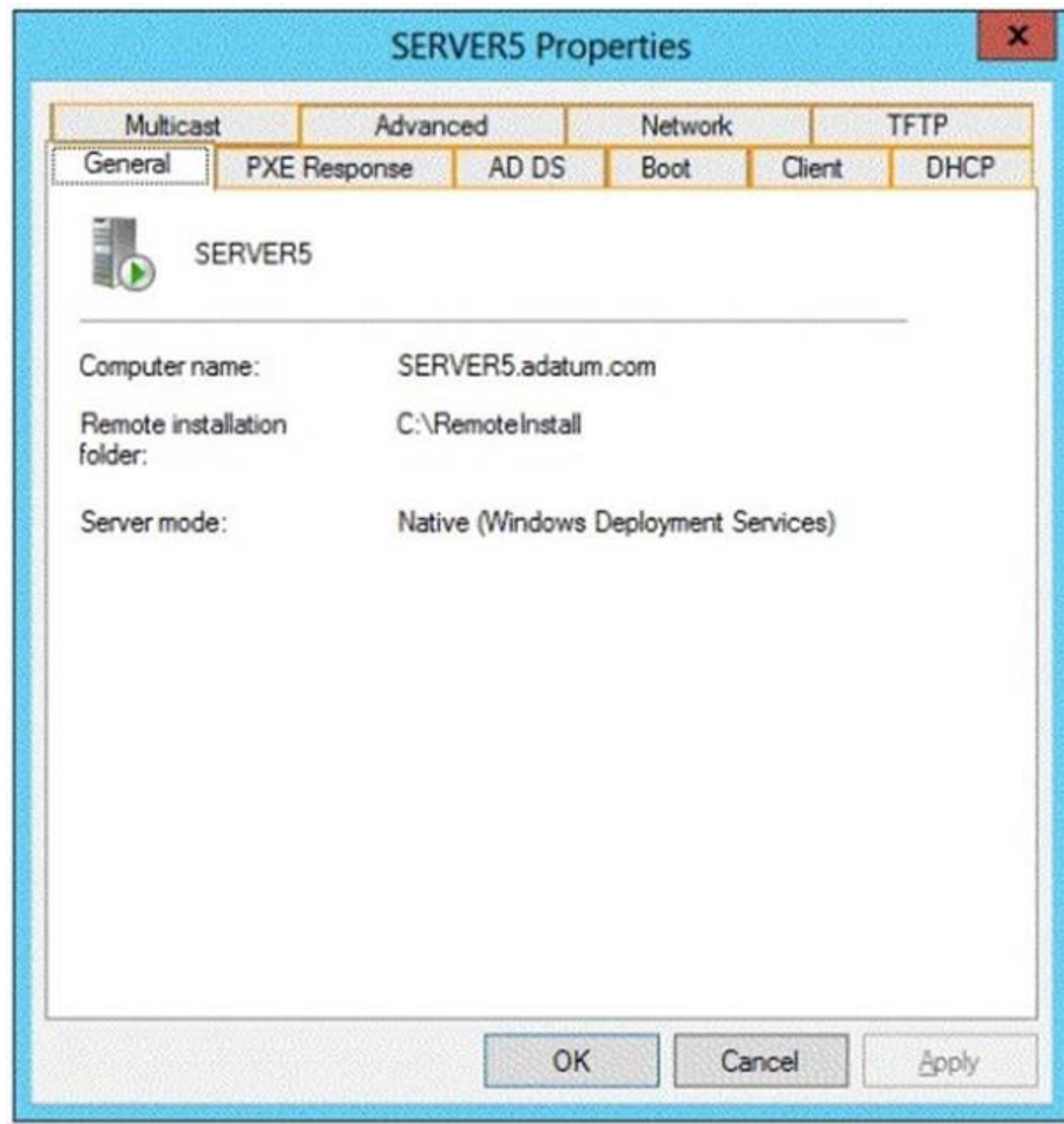
You have a server named Servers that runs Windows Server 2012 R2. Servers has the Windows Deployment Services server role installed.

Server5 contains several custom images of Windows 8.

You need to ensure that when 32-bit client computers start by using PXE, the computers automatically install an image named Image 1.

What should you configure?

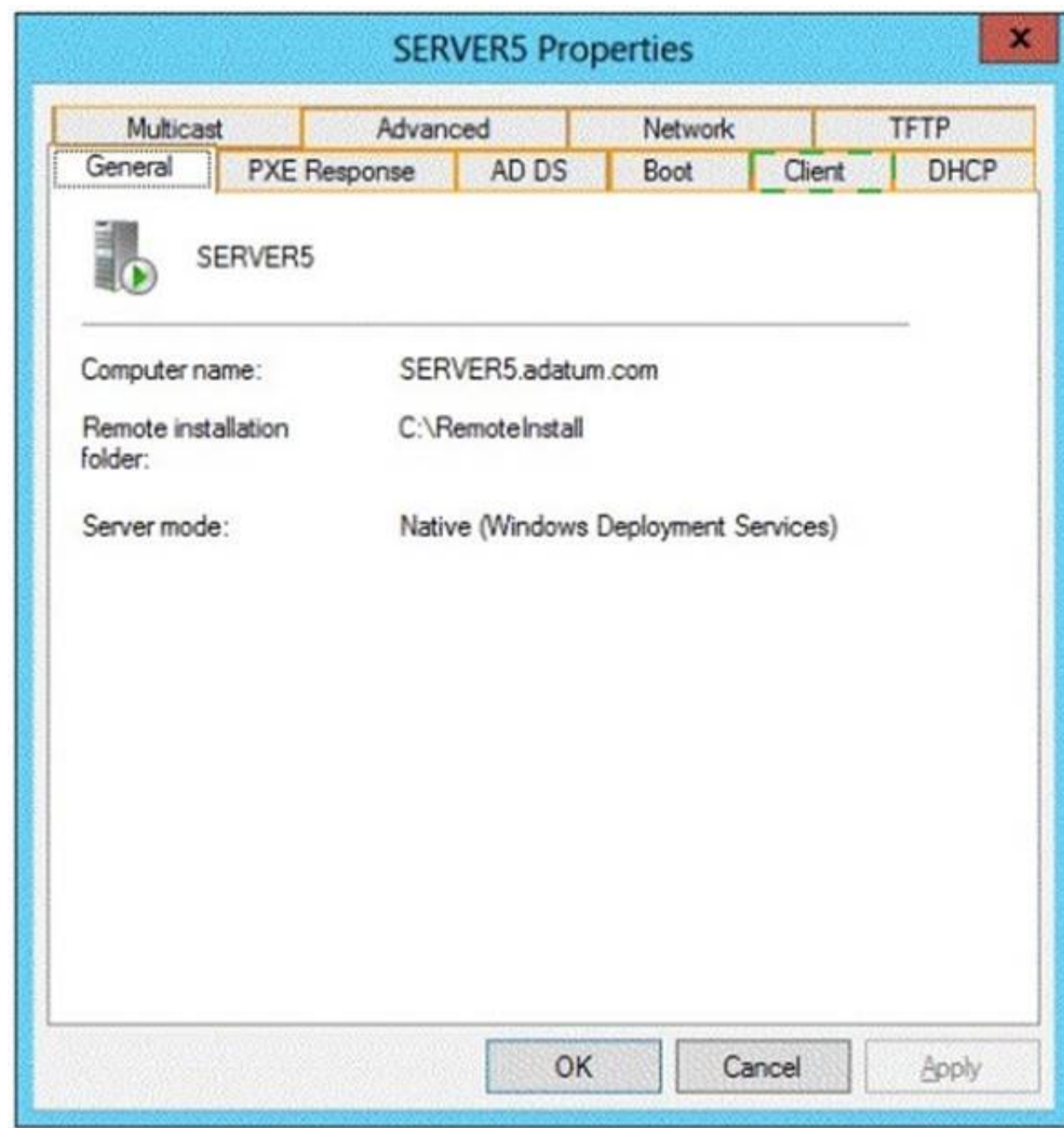
To answer, select the appropriate tab in the answer area.



- A. Mastered
- B. Not Mastered

**Answer:** A

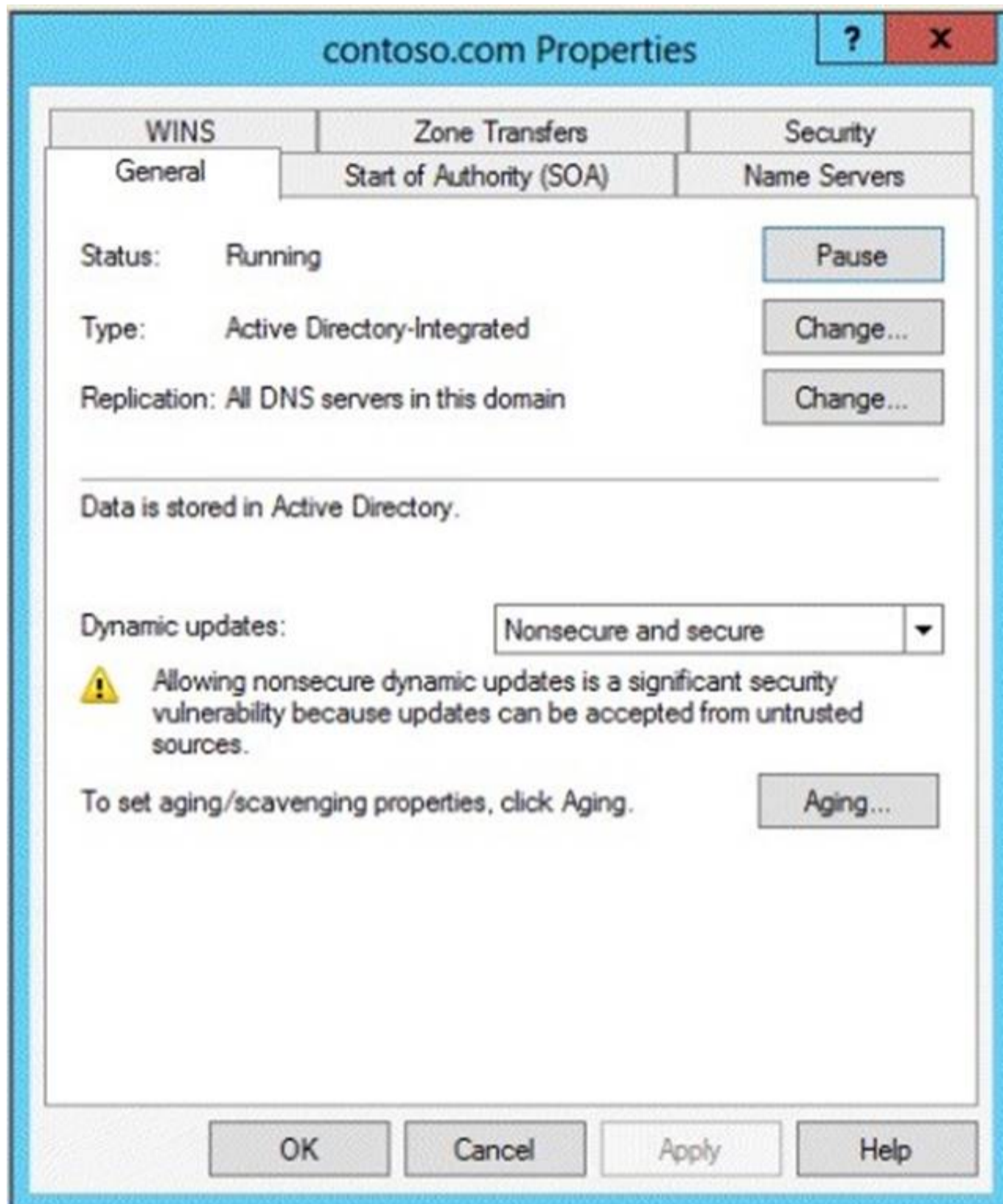
**Explanation:**



#### NEW QUESTION 132

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1. DC1 is a DNS server for contoso.com. The properties of the contoso.com zone are configured as shown in the exhibit. (Click the Exhibit button.)



The domain contains a server named Server1 that is part of a workgroup named Workgroup. Server1 is configured to use DC1 as a DNS server. You need to ensure that Server1 dynamically registers a host (A) record in the contoso.com zone. What should you configure?

- A. The workgroup name of Server1
- B. The Security settings of the contoso.com zone
- C. The Dynamic updates setting of the contoso.com zone
- D. The primary DNS suffix of Server1

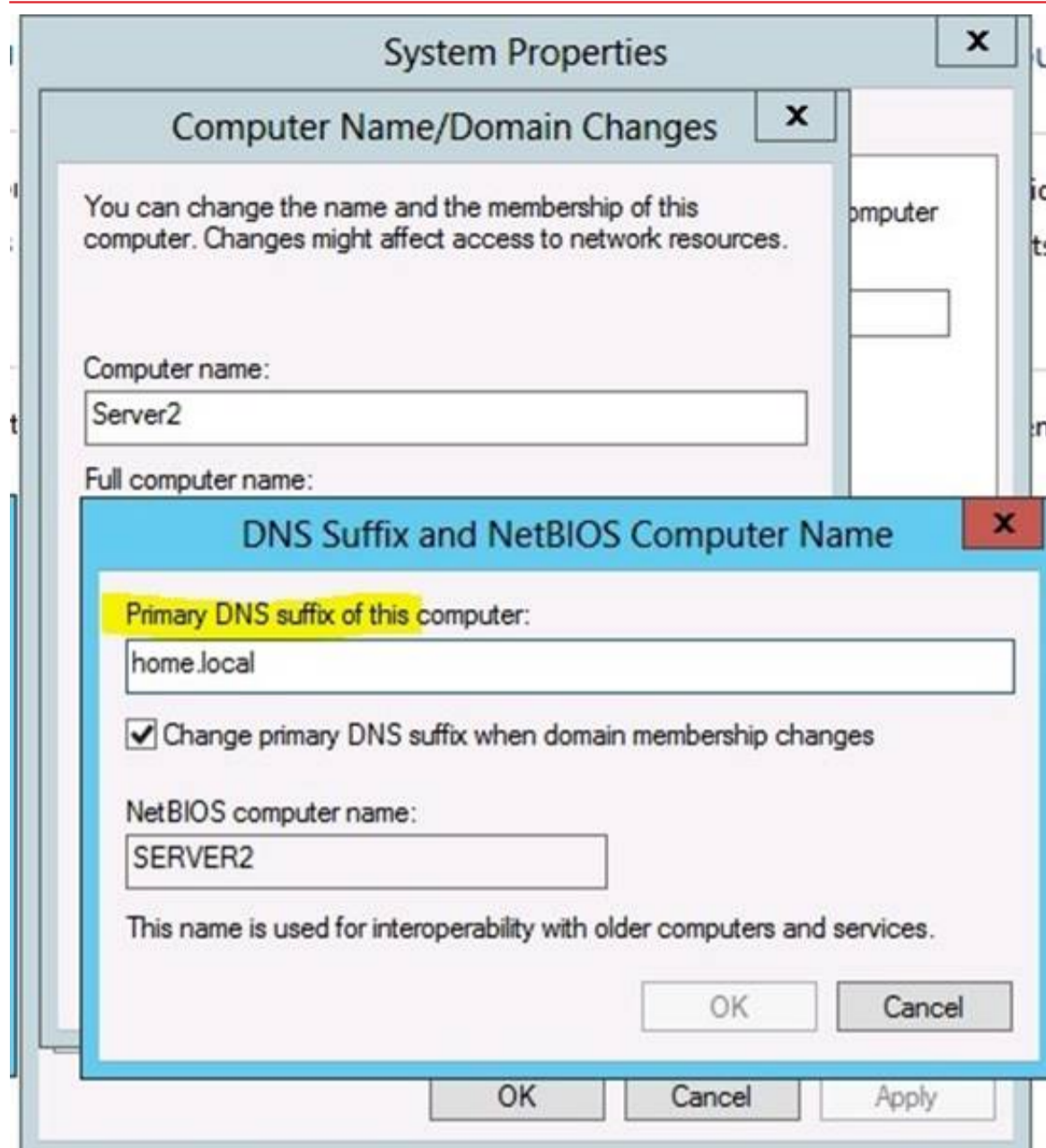
**Answer: D**

**Explanation:**

When any computer or a standalone server is added to a domain as a member, the network identifies that computer with its Fully Qualified Domain Name or FQDN. A Fully Qualified Domain Name consist of a hostname and the DNS suffix separated by a "." called period. An example for this can be server01.msftdomain.com where "server01" is the hostname of the computer and "msftdomain.com" is the DNS suffix which follows the hostname. A complete FQDN of a client computer or a member server uniquely identifies that computer in the entire domain.

Primary DNS suffix must manually be added in Windows 8 computer to change its hostname to Fully Qualified Domain Name so that it becomes eligible to send queries and receive responses from the DNS server. Following are the steps which can be implemented to add primary DNS suffix to a Windows 8 computer hostname:

- ? Log on to Windows 8 computer with administrator account.
- ? From the options available on the screen click Control Panel.
- ? On the opened window click More Settings from the left pane.
- ? On the next window click System and Security category and on the appeared window click System.
- ? On View basic information about your computer window click Change settings under Computer name, domain, and workgroup settings section.
- ? On System Properties box make sure that Computer Name tab is selected and click Change button.
- ? On Computer Name/Domain Changes box click More button.
- ? On DNS Suffix and NetBIOS Computer Name box type in the DNS domain name as the DNS suffix to the Windows 8 computer under Primary DNS suffix of this computer field.
- ? Click Ok button on all the boxes and restart the computer to allow changes to take effect.



**System Properties**

**Computer Name/Domain Changes**

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:

Full computer name:

**DNS Suffix and NetBIOS Computer Name**

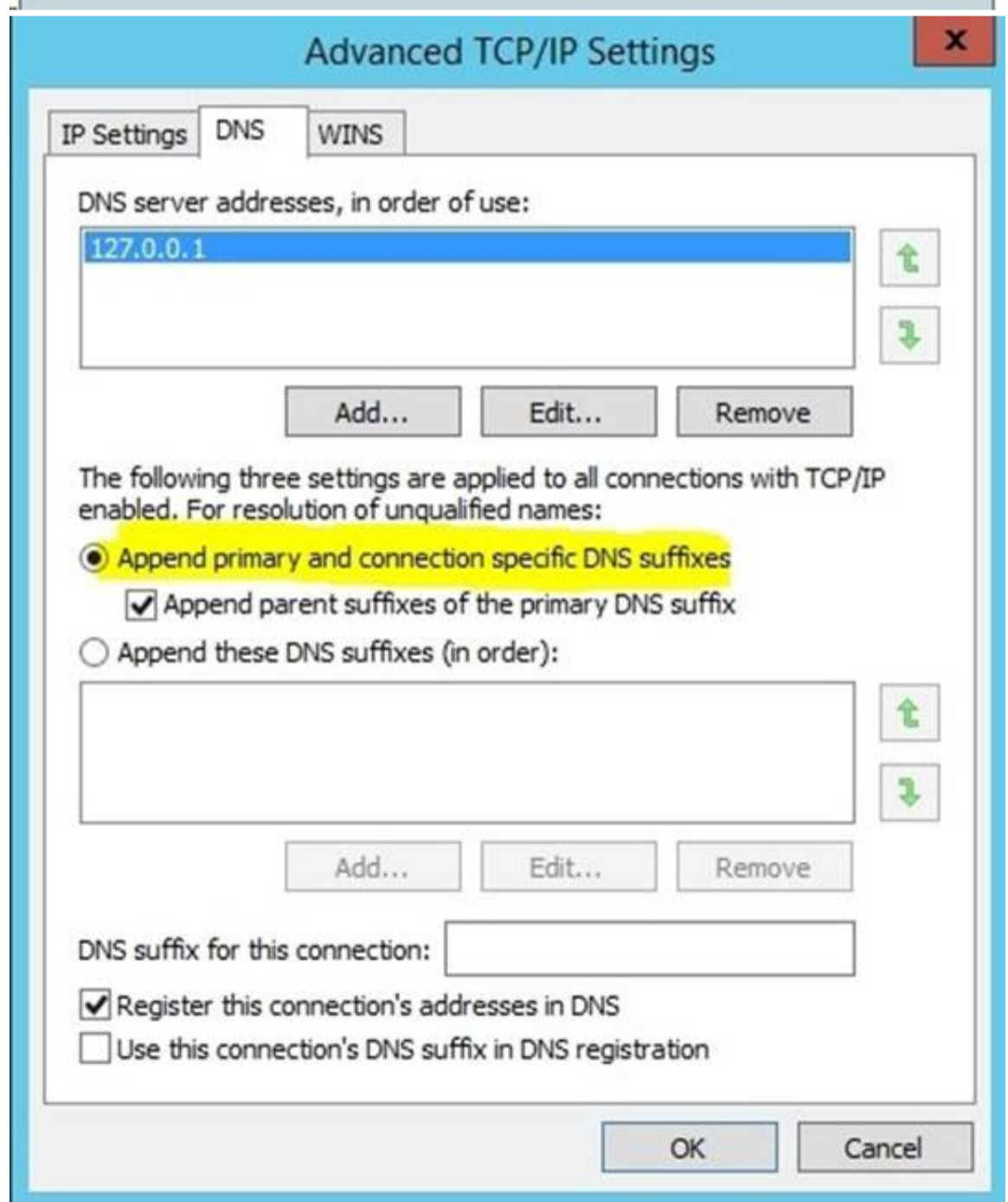
Primary DNS suffix of this computer:

☒ Change primary DNS suffix when domain membership changes

NetBIOS computer name:

This name is used for interoperability with older computers and services.

OK Cancel



**Advanced TCP/IP Settings**

IP Settings DNS WINS

DNS server addresses, in order of use:

Add... Edit... Remove

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

☒ Append primary and connection specific DNS suffixes  
☒ Append parent suffixes of the primary DNS suffix

☐ Append these DNS suffixes (in order):

Add... Edit... Remove

DNS suffix for this connection:

☒ Register this connection's addresses in DNS  
☐ Use this connection's DNS suffix in DNS registration

OK Cancel

For years, Windows DNS has supported dynamic updates, whereas a DNS client host registers and dynamically updates the resource records with a DNS server. If a host's IP address changes, the resource record (particularly the A record) for the host is automatically updated, while the host utilizes the DHCP server to dynamically update its Pointer (PTR) resource record. Therefore, when a user or service needs to contact a client PC, it can look up the IP address of the host. With larger organizations, this becomes an essential feature, especially for clients that frequently move or change locations and use DHCP to automatically obtain an IP address. For dynamic DNS updates to succeed, the zone must be configured to accept dynamic updates:



References:

<http://technet.microsoft.com/en-us/library/cc778792%28v=ws.10%29.aspx>  
<http://technet.microsoft.com/en-us/library/cc778792%28v=ws.10%29.aspx>  
<http://www.advicehow.com/adding-primary-dns-suffix-in-microsoft-windows-8/>  
<http://technet.microsoft.com/en-us/library/cc959611.aspx>

#### NEW QUESTION 136

- (Topic 2)

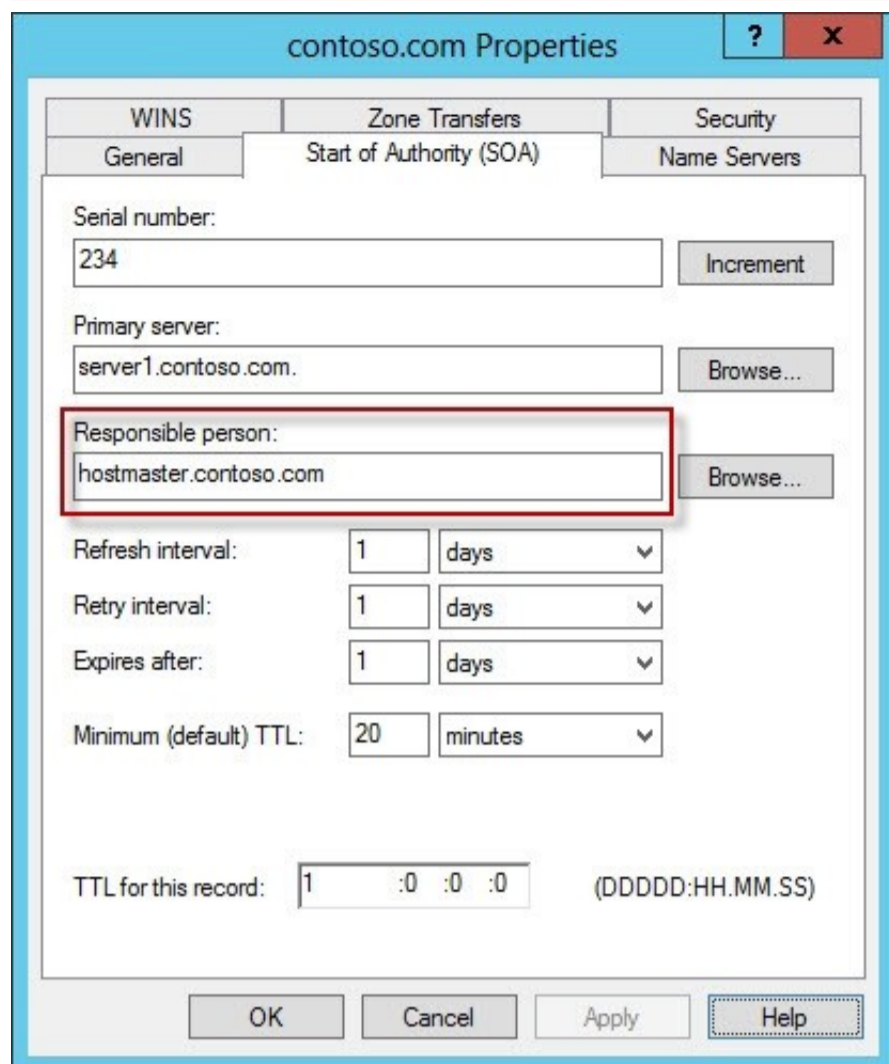
You have a DNS server named Server1 that runs Windows Server 2012 R2. On Server1, you create a DNS zone named contoso.com. You need to specify the email address of the person responsible for the zone. Which type of DNS record should you configure?

- 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.



The screenshot shows the 'contoso.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The 'Responsible person' field is highlighted with a red box and contains the text 'hostmaster.contoso.com'. Other fields include 'Serial number' (234), 'Primary server' (server1.contoso.com), 'Refresh interval' (1 days), 'Retry interval' (1 days), 'Expires after' (1 days), 'Minimum (default) TTL' (20 minutes), and 'TTL for this record' (1 :0 :0 :0).

```
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 138

- (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 .adm 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 .adm 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 140

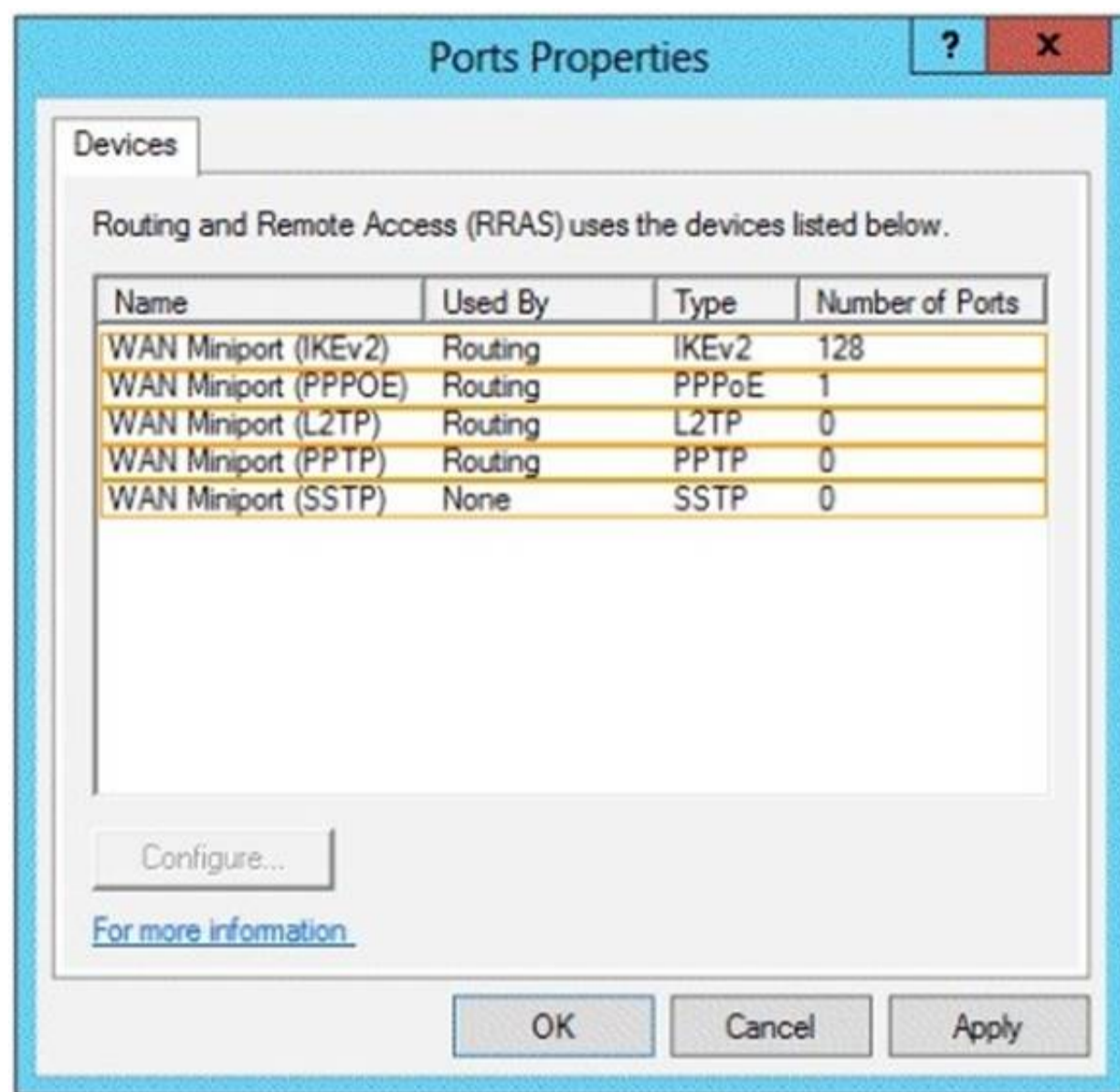
HOTSPOT - (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Access server role installed.

You need to configure the ports on Server1 to ensure that client computers can establish VPN connections to Server1. The solution must NOT require the use of certificates or pre-shared keys.

What should you modify?

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The four types of tunneling protocols used with a VPN/RAS server running on Windows Server 2012 include:

Point-to-Point Tunneling Protocol (PPTP): A VPN protocol based on the legacy Point-to-Point protocol used with modems. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality.

Layer 2 Tunneling Protocol (L2TP): Used with IPsec to provide security. L2TP supports either computer certificates or a preshared key as the authentication method for IPsec. IKEv2: IKE is short for Internet Key Exchange, which is a tunneling protocol that uses IPsec Tunnel Mode protocol. The message is encrypted with one of the following protocols by using encryption keys that are generated from the IKEv2 negotiation process.

Secure Socket Tunneling Protocol (SSTP): Introduced with Windows Server 2008, which uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls

References:

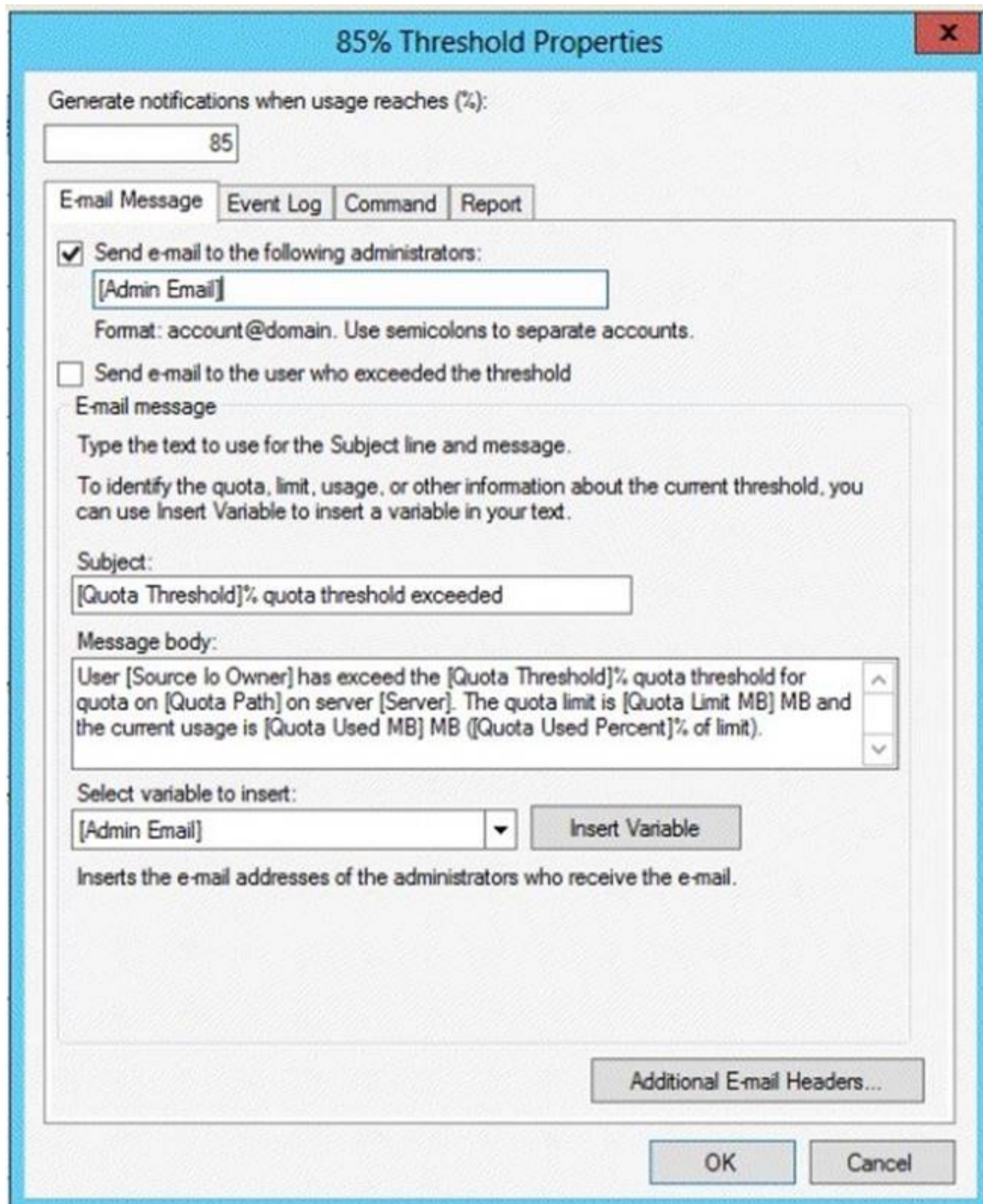
[http://en.wikipedia.org/wiki/Point-to-Point\\_Tunneling\\_Protocol](http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol)

**NEW QUESTION 144**

- (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 File Server Resource Manager role service installed.

You configure a quota threshold as shown in the exhibit. (Click the Exhibit button.)



**85% Threshold Properties**

Generate notifications when usage reaches (%):

**E-mail Message** | Event Log | Command | Report

☒ Send e-mail to the following administrators:  
  
 Format: account@domain. Use semicolons to separate accounts.

☐ Send e-mail to the user who exceeded the threshold

**E-mail message**  
 Type the text to use for the Subject line and message.  
 To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.

**Subject:**

**Message body:**

**Select variable to insert:**

Inserts the e-mail addresses of the administrators who receive the e-mail.

You need to ensure that a user named User1 receives an email notification when the threshold is exceeded. What should you do?

- A. Create a performance counter alert.
- B. Create a classification rule.
- C. Modify the members of the Performance Log Users group.
- D. Configure the File Server Resource Manager Options.

**Answer: D**

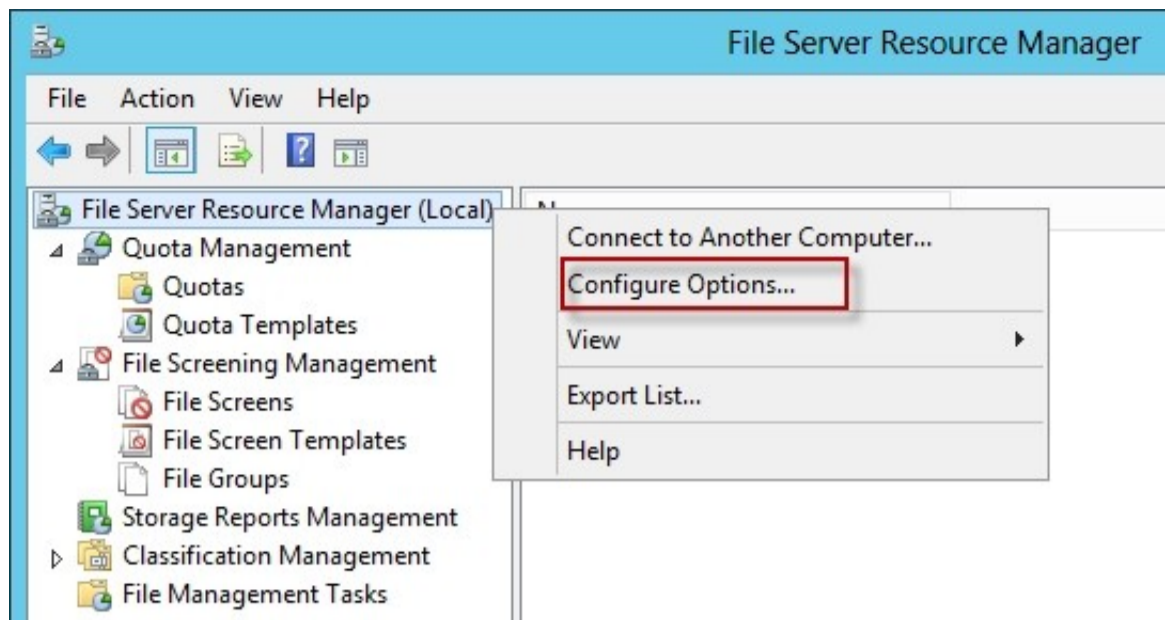
**Explanation:**

When you create quotas and file screens, you have the option of sending e-mail notifications to users when their quota limit is approaching or after they have attempted to save files that have been blocked. If you want to routinely notify certain administrators of quota and file screening events, you can configure one or more default recipients.

To send these notifications, you must specify the SMTP server to be used for forwarding the e-mail messages.

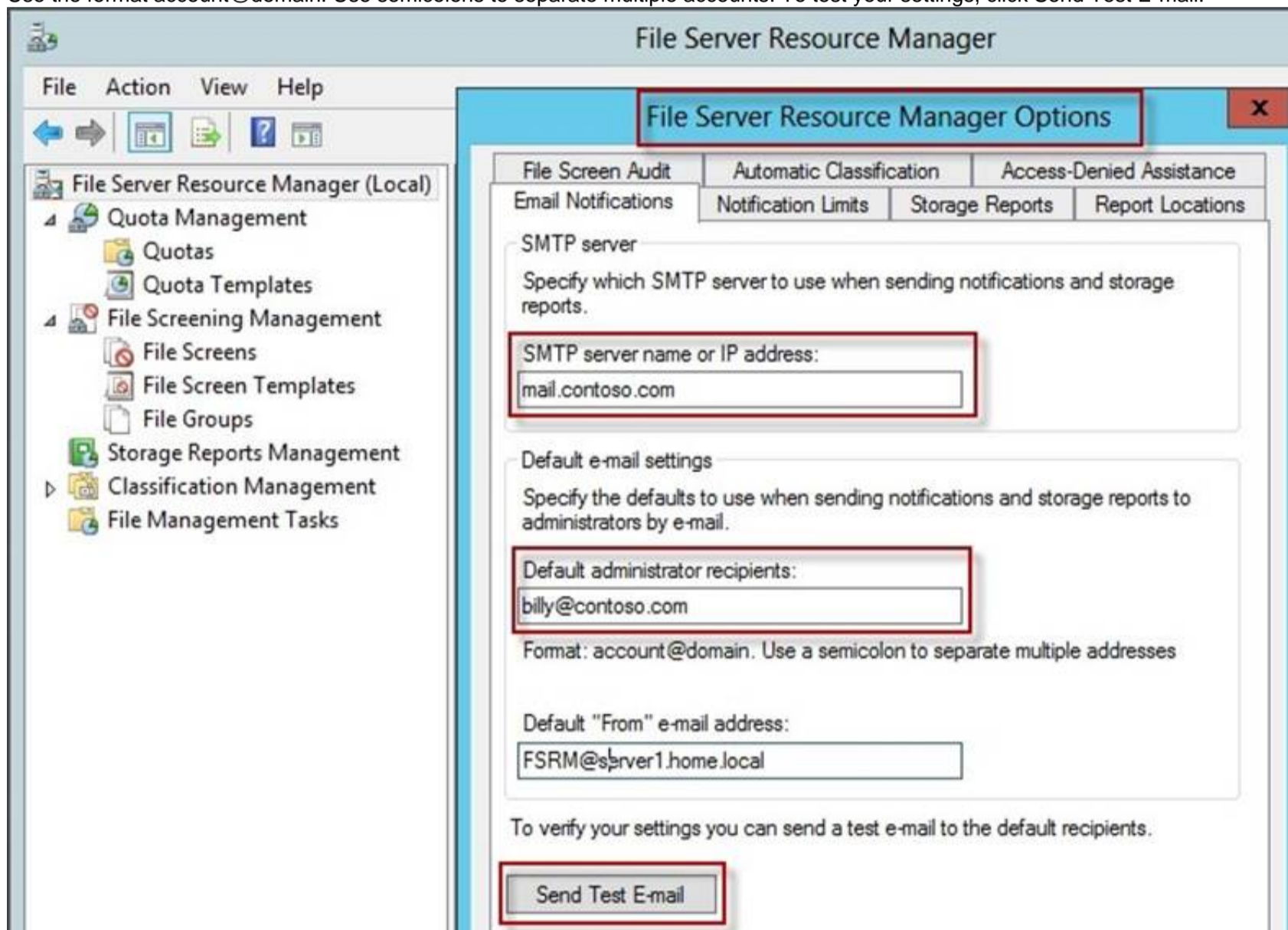
To configure e-mail options

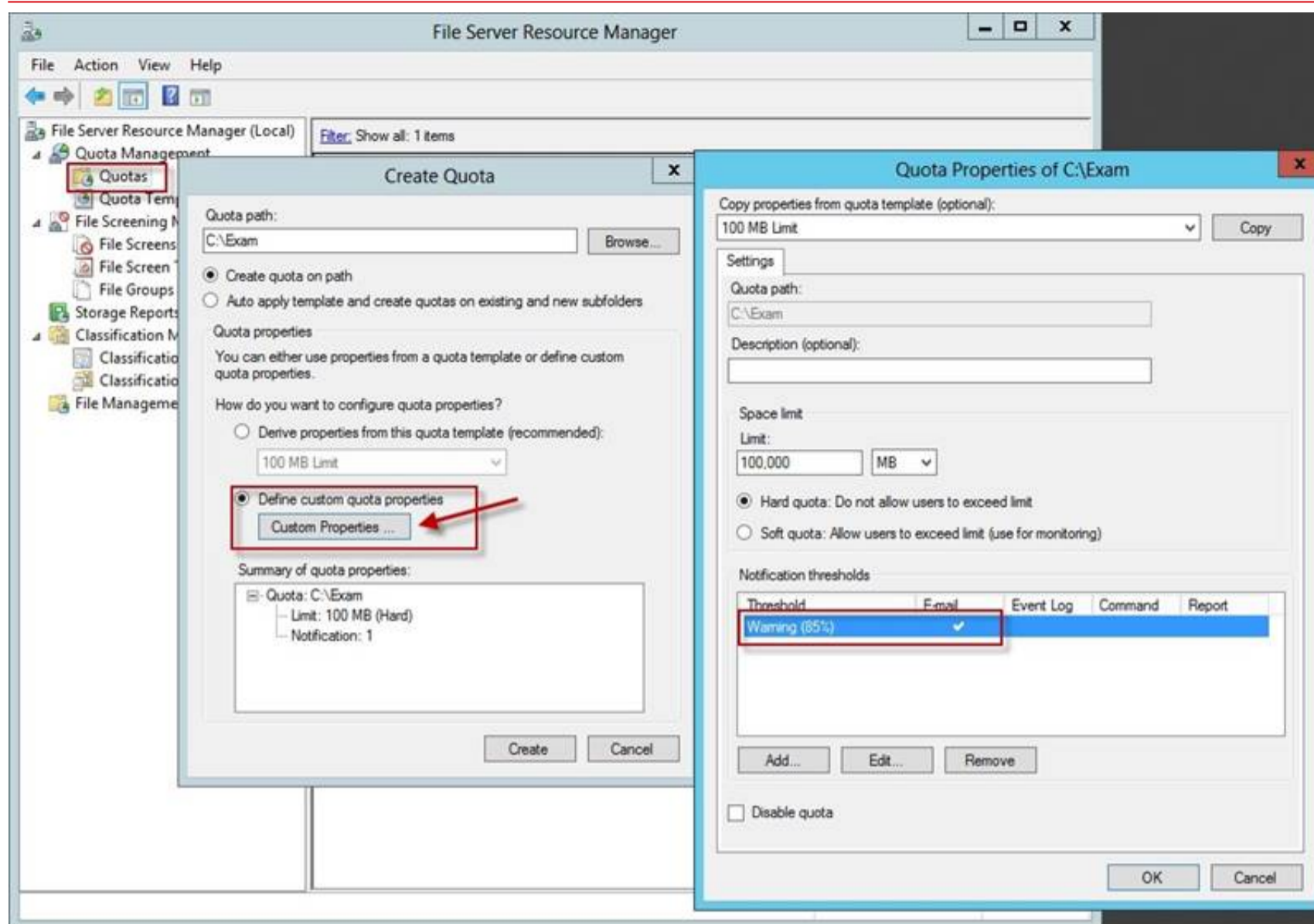
In the console tree, right-click File Server Resource Manager, and then click Configure options. The File Server Resource Manager Options dialog box opens.



On the E-mail Notifications tab, under SMTP server name or IP address, type the host name or the IP address of the SMTP server that will forward e-mail notifications.

If you want to routinely notify certain administrators of quota or file screening events, under Default administrator recipients, type each e-mail address. Use the format account@domain. Use semicolons to separate multiple accounts. To test your settings, click Send Test E-mail.





#### NEW QUESTION 148

- (Topic 3)

Your network contains an Active Directory domain named contoso.com.

All user accounts reside in an organizational unit (OU) named OU1. All of the users in the marketing department are members of a group named Marketing. All of the users in the human resources department are members of a group named HR.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preferences of GPO1 to add two shortcuts named Link1 and Link2 to the desktop of each user.

You need to ensure that Link1 only appears on the desktop of the users in Marketing and that Link2 only appears on the desktop of the users in HR.

What should you configure?

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

**Answer: D**

#### Explanation:

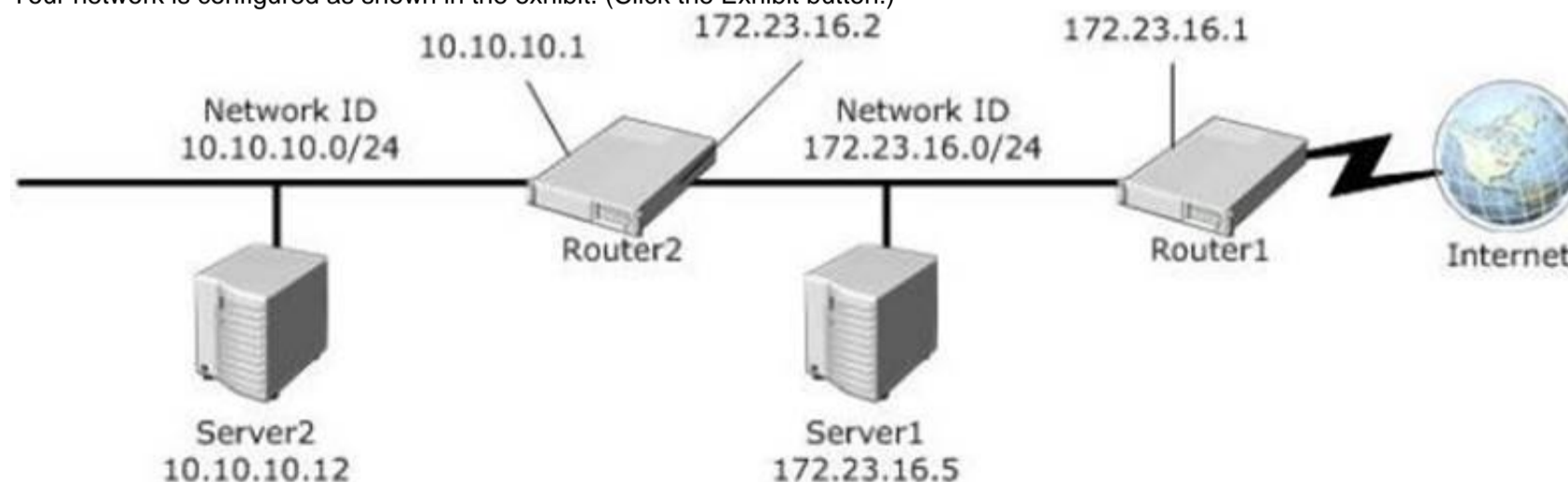
You can use item-level targeting to change the scope of individual preference items, so they apply only to selected users or computers. Within a single Group Policy object (GPO), you can include multiple preference items, each customized for selected users or computers and each targeted to apply settings only to the relevant users or computers.

Reference: <http://technet.microsoft.com/en-us/library/cc733022.aspx>

#### NEW QUESTION 151

- (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 Router1.

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 155

- (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 user accounts were authenticated by RODC01. 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

#### Explanation:

Gets the Active Directory accounts that are authenticated by a read-only domain controller or that are in the revealed list of the domain controller.

Reference: Get-ADDomainControllerPasswordReplicationPolicyUsage <https://technet.microsoft.com/en-us/library/ee617194.aspx>

#### NEW QUESTION 158

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 160

- (Topic 3)

You deploy a Windows Server Update Services (WSUS) server named Server01.

You plan to use a Group Policy object (GPO) to configure all client computers to use Server01 as a Microsoft Update server and to assign the client computers to computer groups.

You need to ensure that the computers are assigned to the correct computer groups automatically when the GPO is deployed. Which two actions should you perform before you deploy the GPO? Each correct answer presents part of the solution.

- A. From Windows PowerShell, run the Approve-WSUSUpdate cmdlet.
- B. From the Update Services console, modify the Computers option.
- C. From Windows PowerShell, run the Add-WSUSComputer cmdlet.
- D. From the Update Services console, manually create the computer groups.
- E. From the Update Services console, modify the Products and Classifications options.

**Answer:** BD

**Explanation:**

References:

[https://technet.microsoft.com/en-us/library/dd939829\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd939829(v=ws.10).aspx)

**NEW QUESTION 161**

- (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 whether the members of the Protected Users group will be prevented from authenticating by using NTLM.

Which cmdlet should you use?

- A. Get-ADGroupMember
- B. Get-ADDomainControllerPasswordReplicationPolicy
- C. Get-ADDomainControllerPasswordReplicationPolicyUsage
- D. Get-ADDomain
- E. Get-ADOptionalFeature
- F. Get-ADAccountAuthorizationGroup
- G. Get-ADAuthenticationPolicySilo
- H. Get-ADAuthenticatonPolicy

**Answer:** D

**Explanation:**

If the domain functional level is Windows Server 2012 R2, members of the (Protected Users) group can no longer authenticate by using NTLM authentication. So we need to check the domain functional level with Get-ADDomain. <https://technet.microsoft.com/en-us/library/Dn518179.aspx>

**NEW QUESTION 165**

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. You create a new user account named Admin5.

You need to ensure that Admin5 can create Group Policy objects (GPOs) and link the GPOs to all of the organizational units (OUs) in the domain. Admin5 must be prevented from modifying GPOs created by other administrators.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. From Active Directory Users and Computers, modify the members of the Network Configuration Operators group.
- B. From Active Directory Users and Computers, modify the Security settings of the Admin5 user account.
- C. From Group Policy Management, click the Group Policy Objects node and modify the Delegation settings.
- D. From Group Policy Management, click the contoso.com node and modify the Delegation settings.
- E. From Active Directory Users and Computers, modify the members of the Group Policy Creator Owners group.

**Answer:** CD

**NEW QUESTION 169**

- (Topic 3)

Your network contains two Active Directory forests named contoso.com and adatum.com. All domain controllers run Windows Server 2012 R2.

The adatum.com domain contains a Group Policy object (GPO) named GPO1. An administrator from adatum.com backs up GPO1 to a USB flash drive.

You have a domain controller named dc1.contoso.com. You insert the USB flash drive in dc1.contoso.com.

You need to identify the domain-specific reference in GPO1. What should you do?

- A. From the Migration Table Editor, click Populate from Backup.
- B. From Group Policy Management, run the Group Policy Modeling Wizard.
- C. From Group Policy Management, run the Group Policy Results Wizard.
- D. From the Migration Table Editor, click Populate from GPO.

**Answer:** A

**NEW QUESTION 170**

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

DirectAccess is deployed to the network.

Remote users connect to the DirectAccess server by using a variety of network speeds.

The remote users report that sometimes their connection is very slow.

You need to minimize Group Policy processing across all wireless wide area network (WWAN) connections.

Which Group Policy setting should you configure?

- A. Configure Group Policy slow link detection.
- B. Configure Direct Access connections as a fast network connection.

- C. Configure wireless policy processing.
- D. Change Group Policy processing to run asynchronously when a slow network connection is detected.

**Answer:** A

#### NEW QUESTION 172

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2008 R2. You plan to test Windows Server 2012 R2 by using native-boot virtual hard disks (VHDs). You have a Windows image file named file1.wim. You need to add an image of a volume to file1.wim. What should you do?

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

**Answer:** D

#### Explanation:

The Deployment Image Servicing and Management (DISM) tool is a command-line tool that enables the creation of Windows image (.wim) files for deployment in a manufacturing or corporate IT environment. The /Append-Image option appends a volume image to an existing .wim file allowing you to store many customized Windows images in a fraction of the space. When you combine two or more Windows image files into a single .wim, any files that are duplicated between the images are only stored once.

Incorrect:

Not A, Not B: Imagex has been retired and replaced by dism.

Reference: Append a Volume Image to an Existing Image Using DISM <https://technet.microsoft.com/en-us/library/hh824916.aspx>

#### NEW QUESTION 173

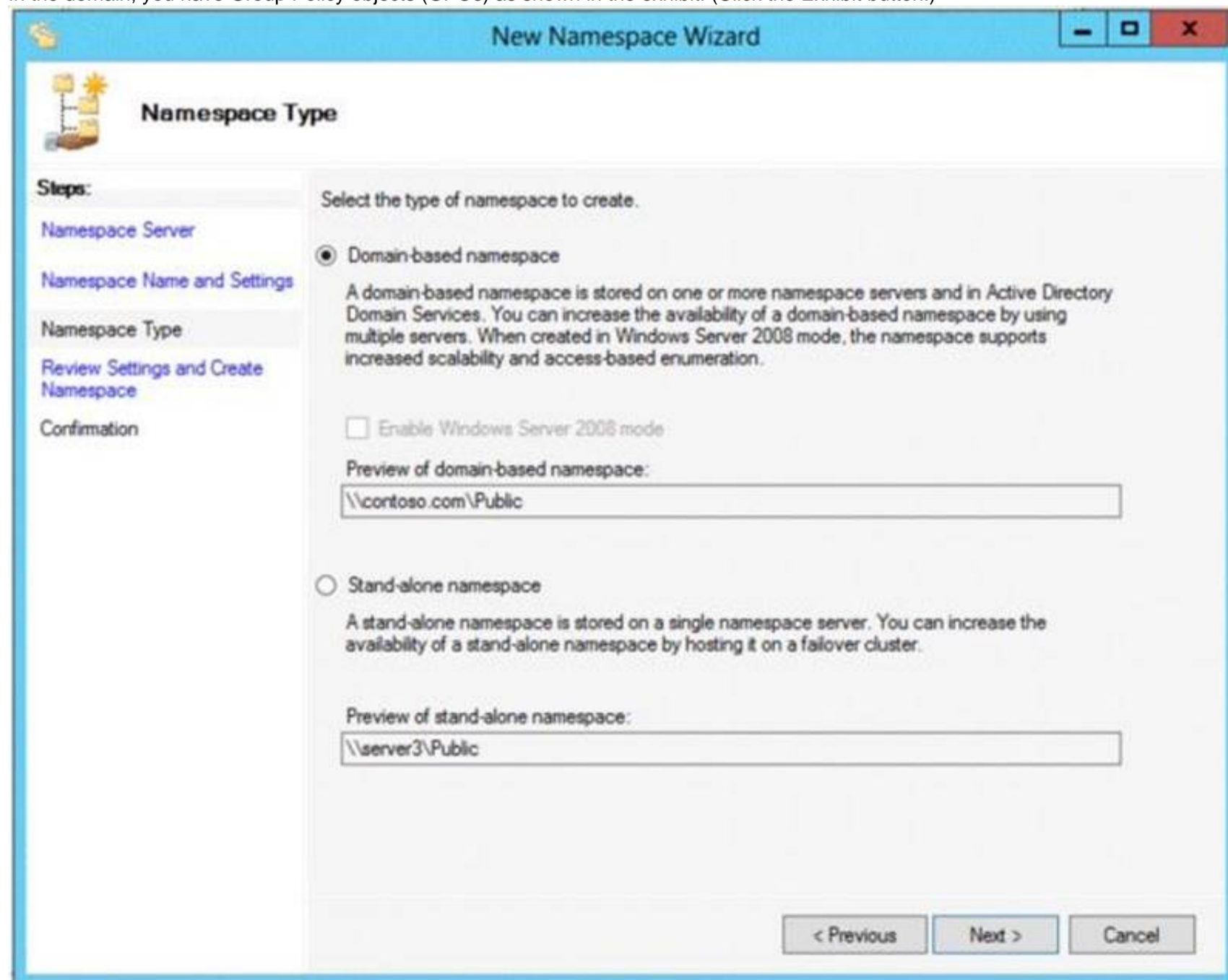
- (Topic 3)

Your network contains an Active Directory domain named contoso.com. The functional level of the forest is Windows Server 2008 R2.

Computer accounts for the marketing department are in an organizational unit (OU) named Departments\Marketing\Computers. User accounts for the marketing department are in an OU named Departments\Marketing\Users.

All of the marketing user accounts are members of a global security group named MarketingUsers. All of the marketing computer accounts are members of a global security group named MarketingComputers.

In the domain, you have Group Policy objects (GPOs) as shown in the exhibit. (Click the Exhibit button.)



You create two Password Settings objects named PSO1 and PSO2. PSO1 is applied to MarketingUsers. PSO2 is applied to MarketingComputers. The minimum password length is defined for each policy as shown in the following table.

Location	Minimum password length
Default Domain Policy	7
GPO1	5
GPO2	6
PSO1	10
PSO2	12

You need to identify the minimum password length required for each marketing user.  
What should you identify?

- A. 5
- B. 6
- C. 7
- D. 10
- E. 12

**Answer:** D

#### NEW QUESTION 175

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. All users have client computers that run Windows 8.1.

All computer accounts reside in an organizational unit (OU) named OU1. All of the computer accounts for the marketing department are members of a group named Marketing. All of the computer accounts for the human resources department are members of a group named HR Computers.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preferences of GPO1 to add two shortcuts named Link1 and Link2 to the desktop.

You need to ensure that Link1 only appears on the desktop of client computers that have more than 80 GB of free disk space and that Link2 only appears on the desktop of client computers that have less than 80 GB of free disk space.

What should you configure?

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

**Answer:** C

#### Explanation:

References: [https://technet.microsoft.com/en-us/library/dn789189\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn789189(v=ws.11).aspx)

#### 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 (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 links them to the domain: "DirectAccess Server Settings" contains Connection Security Settings and Firewall inbound 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](http://www.windowsecurity.com/articles-tutorials/Windows_Server_2012_Security/windows-server-2012-simplified-directaccess-wizard-overview-Part1.html)

#### NEW QUESTION 183

- (Topic 3)

Your network contains an Active Directory domain named adatum.com.

You need to audit changes to the files in the SYSVOL shares on all of the domain controllers. The solution must minimize the amount of SYSVOL replication traffic caused by the audit.

Which two settings should you configure? (Each correct answer presents part of the solution. Choose two.)

- A. Audit Policy\Audit system events
- B. Advanced Audit Policy Configuration\DS Access
- C. Advanced Audit Policy Configuration\Global Object Access Auditing
- D. Audit Policy\Audit object access
- E. Audit Policy\Audit directory service access
- F. Advanced Audit Policy Configuration\Object Access

**Answer:** DF

#### NEW QUESTION 184

.....

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (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 2

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.

The domain contains a server named Server1 that has the Network Policy Server server role and the Remote Access server role installed. The domain contains a server named Server2 that is configured as a RADIUS server.

Server1 provides VPN access to external users.

You need to ensure that all of the VPN connections to Server1 are logged to the RADIUS server on Server2.

What should you run?

- A. Add-RemoteAccessRadius -ServerNameServer1 -AccountingOnOffMsg Enabled - SharedSecret "Secret" -Purpose Accounting
- B. Set-RemoteAccessAccounting -AccountingOnOffMsg Enabled -AccountingOnOffMsg Enabled
- C. Add-RemoteAccessRadius -ServerName Server2 -AccountingOnOffMsg Enabled - SharedSecret "Secret" -Purpose Accounting
- D. Set-RemoteAccessAccounting -EnableAccountingType Inbox -AccountingOnOffMsg Enabled

**Answer: C**

#### Explanation:

Add-RemoteAccessRadius

Adds a new external RADIUS server for VPN authentication, accounting for DirectAccess (DA) and VPN, or one-time password (OTP) authentication for DA.

AccountingOnOffMsg<String>

Indicates the enabled state for sending of accounting on or off messages. The acceptable values for this parameter are:

? Enabled.

? Disabled. This is the default value.

This parameter is applicable only when the RADIUS server is being added for Remote Access accounting.

### NEW QUESTION 3

- (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.

A local account named Admin1 is a member of the Administrators group on Server1.

You need to generate an audit event whenever Admin1 is denied access to a file or folder. What should you run?

- A. auditpol.exe /set /userradmin1 /failure: enable
- B. auditpol.exe /set /user: admin1 /category: "detailed tracking" /failure: enable
- C. auditpol.exe /resourcesacl /set /type: file /user: admin1 /failure
- D. auditpol.exe /resourcesacl /set /type: key /user: admin1 /failure /access: ga

**Answer: C**

#### Explanation:

<http://technet.microsoft.com/en-us/library/ff625687.aspx>

To set a global resource SACL to audit successful and failed attempts by a user to perform generic read and write functions on files or folders:

auditpol /resourceSACL /set /type: File /user: MYDOMAINmyuser /success /failure /access: FRFW

<http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx> Syntax

auditpol /resourceSACL

[/set /type: <resource> [/success] [/failure] /user: <user> [/access: <access flags>]] [/remove /type: <resource> /user: <user> [/type: <resource>]]

[/clear [/type: <resource>]]

[/view [/user: <user>] [/type: <resource>]]

References:

<http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/ff625687.aspx>

<http://technet.microsoft.com/en-us/library/ff625687.aspx>

<http://technet.microsoft.com/en-us/library/ff625687%28v=ws.10%29.aspx>

### NEW QUESTION 4

- (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.

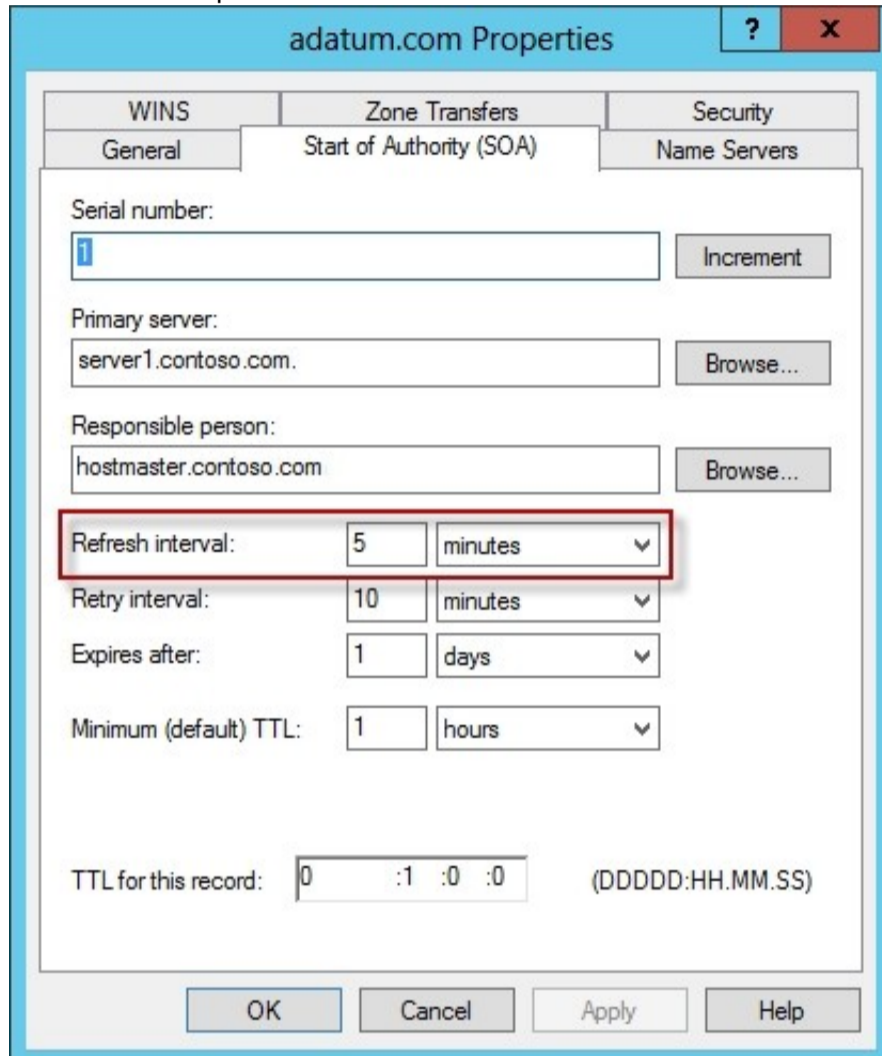
Which setting should you modify in the start of authority (SOA) record?

- 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.



**NEW QUESTION 5**

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 P.2. Server1 has the Network Policy and Access Services server role installed.

You plan to deploy 802.1x authentication to secure the wireless network.

You need to identify which Network Policy Server (NPS) authentication method supports certificate-based mutual authentication for the 802.1x deployment.

Which authentication method should you identify?

- A. MS-CHAP
- B. PEAP-MS-CHAPv2
- C. EAP-TLS
- D. MS-CHAP v2

**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.

**NEW QUESTION 6**

- (Topic 1)

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

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



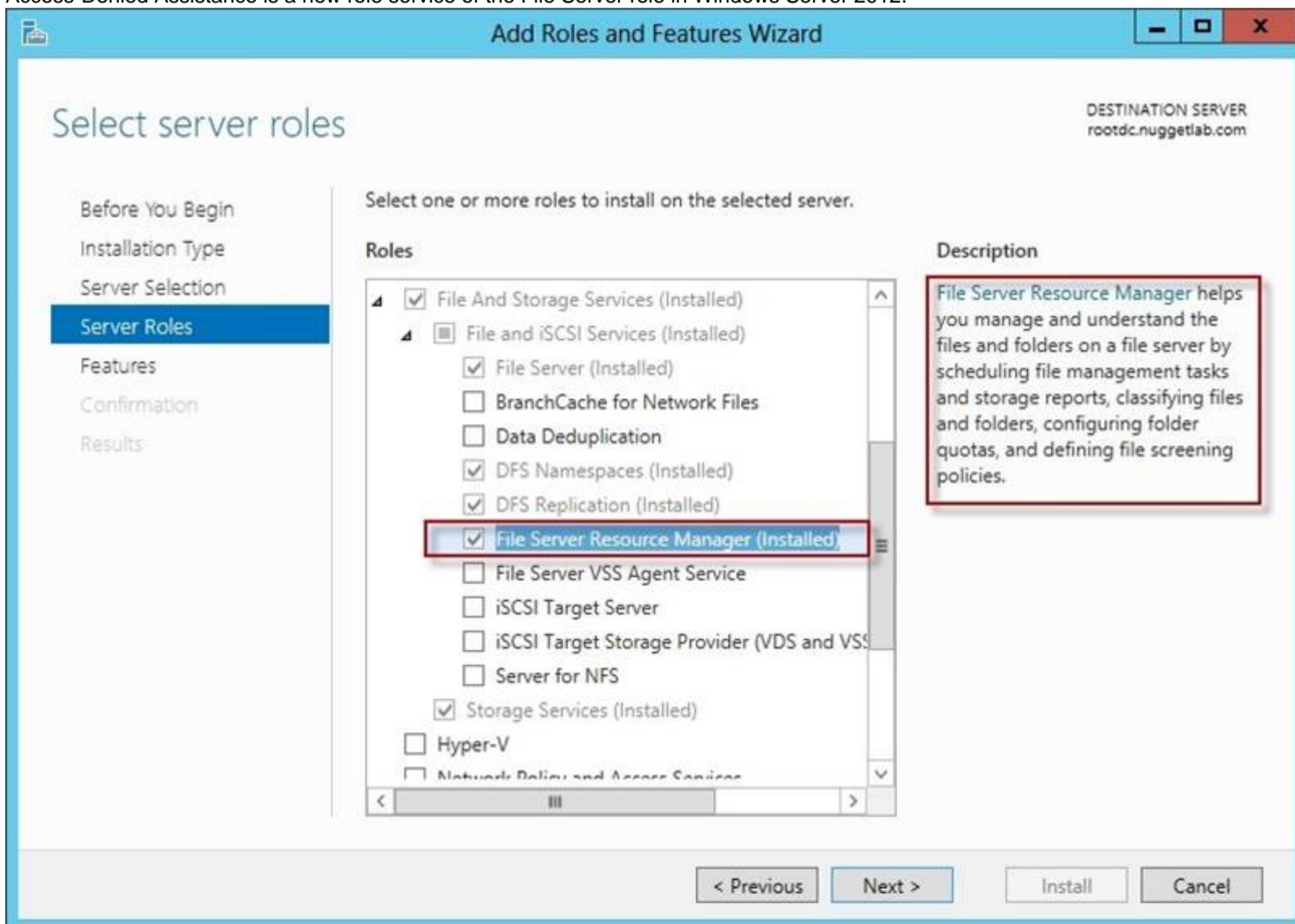
You deploy a new file server named Server2 that runs Windows Server 2012 R2.  
 You need to configure Server2 to display the same custom Access Denied message as Server1.  
 What should you install on Server2?

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

**Answer: C**

**Explanation:**

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



We need to install the prerequisites for Access-Denied Assistance.

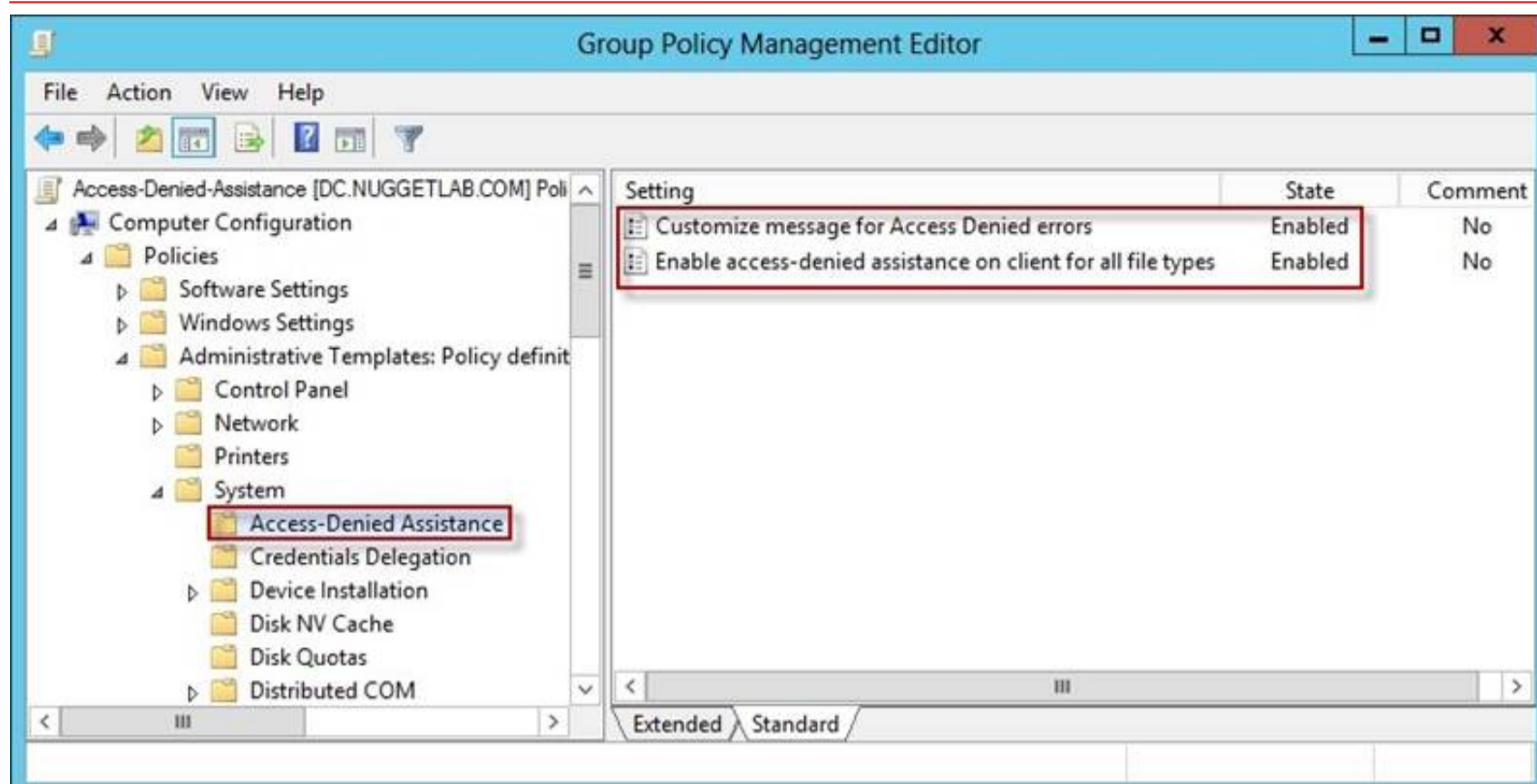
Because Access-Denied Assistance relies up on e-mail notifications, we also need to configure each relevant file server with a Simple Mail Transfer Protocol (SMTP) server address. Let's do that quickly with Windows PowerShell:

```
Set-FSRMSSetting -SMTPServer mailserver.nuggetlab.com -AdminEmailAddress admingroup@nuggetlab.com -FromEmailAddress admingroup@nuggetlab.com
```

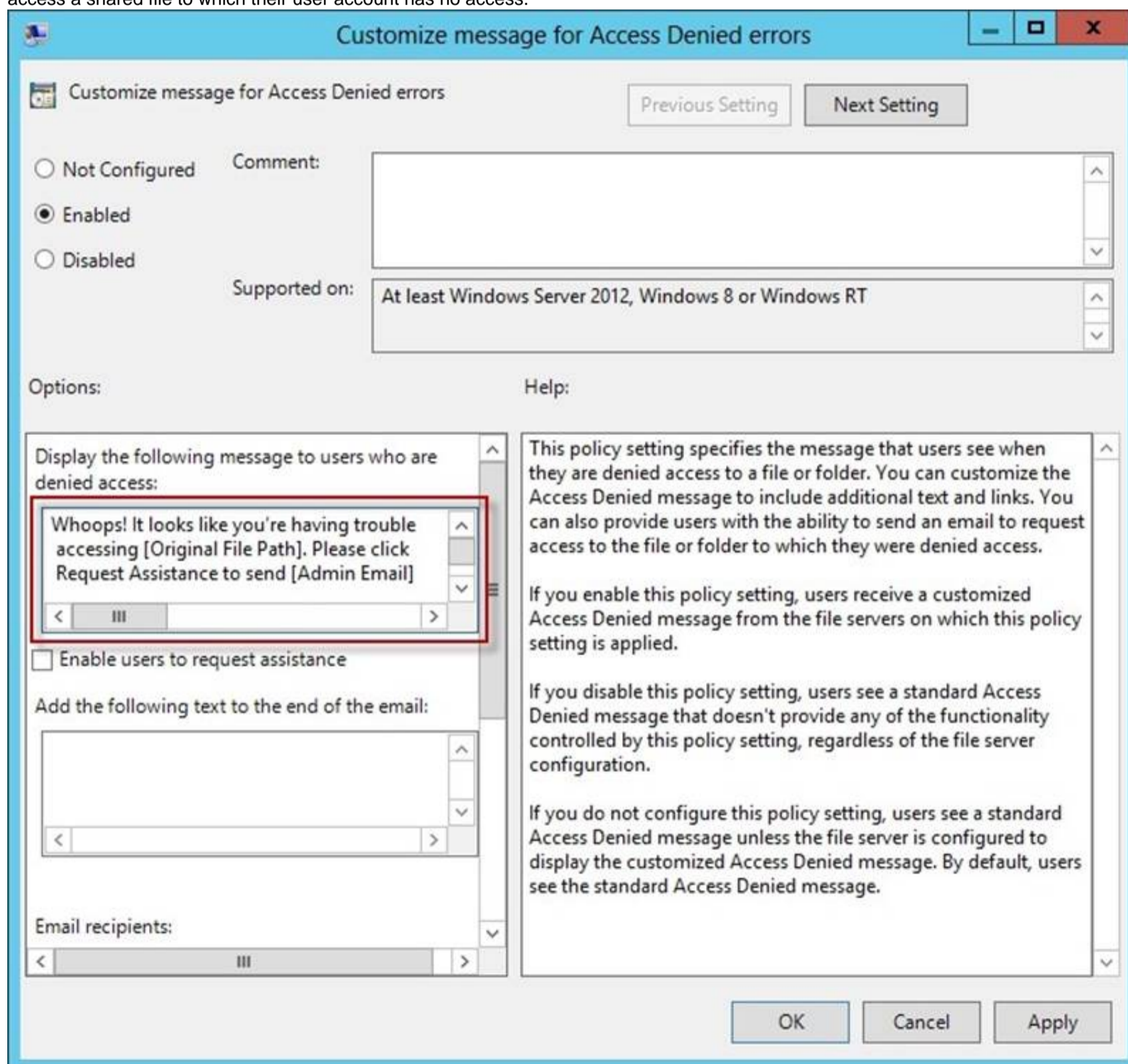
You can enable Access-Denied Assistance either on a per-server basis or centrally via Group Policy. To my mind, the latter approach is infinitely preferable from an administration standpoint.

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

\Computer Configuration\Policies\Administrative Templates\System\Access-Denied Assistance



The Customize message for Access Denied errors policy, shown in the screenshot below, enables us to create the actual message box shown to users when they access a shared file to which their user account has no access.



What's cool about this policy is that we can "personalize" the e-mail notifications to give us administrators (and, optionally, file owners) the details they need to resolve the permissions issue quickly and easily.

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

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

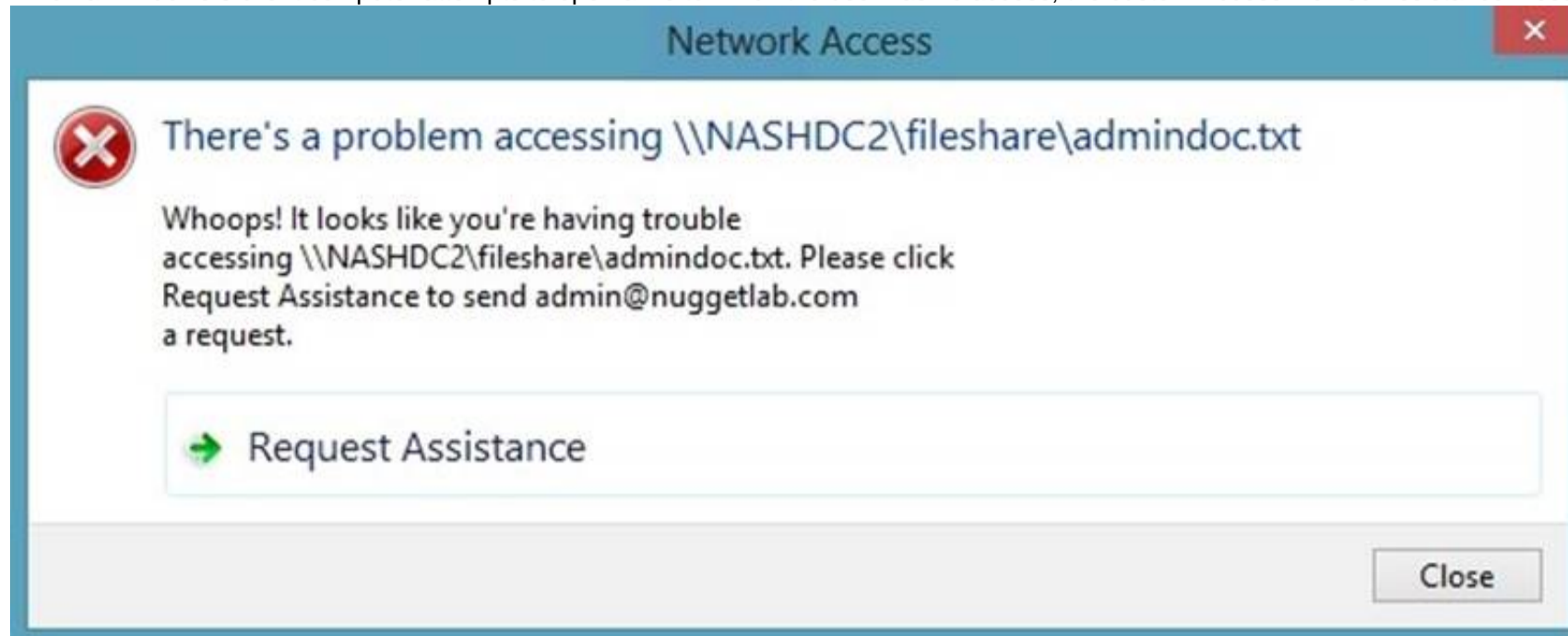
You should find that your users prefer these human-readable, informative error messages to the cryptic, non-descript error dialogs they are accustomed to dealing with.

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

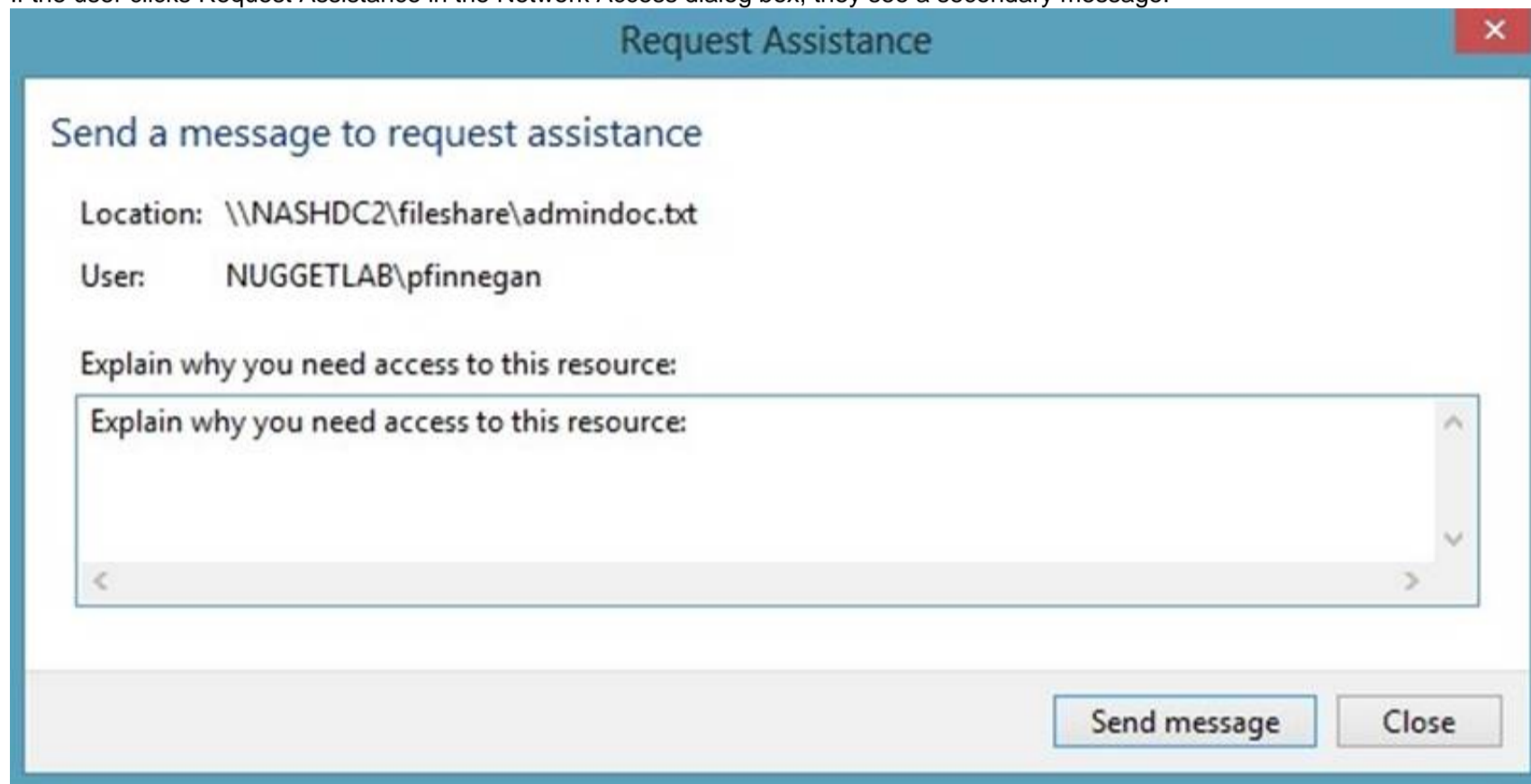
Again, you must make sure to target your GPO scope accordingly to "hit" your domain workstations as well as your Windows Server 2012 file servers.

Testing the configuration

This should come as no surprise to you, but Access-Denied Assistance works only with Windows Server 2012 and Windows 8 computers. More specifically, you must enable the Desktop Experience feature on your servers to see Access-Denied Assistance messages on server computers. When a Windows 8 client computer attempts to open a file to which the user has no access, the custom Access-Denied Assistance message should appear:



If the user clicks Request Assistance in the Network Access dialog box, they see a secondary message:



At the end of this process, the administrator(s) will receive an e-mail message that contains the key information they need in order to resolve the access problem:  
 The user's Active Directory identity  
 The full path to the problematic file  
 A user-generated explanation of the problem  
 So that's it, friends! Access-Denied Assistance presents Windows systems administrators with an easy-to-manage method for more efficiently resolving user access problems on shared file system resources. Of course, the key caveat is that your file servers must run Windows Server 2012 and your client devices must run Windows 8, but other than that, this is a great technology that should save admins extra work and end-users extra headaches.  
 Reference: <http://4sysops.com/archives/access-denied-assistance-in-windows-server-2012/>

## NEW QUESTION 7

- (Topic 1)

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

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

**Answer: B**

### Explanation:

RADIUS client properties

Following are the RADIUS client conditions that you can configure in network policy.

? Calling Station ID: Specifies the network access server telephone number that was dialed by the dial-up access client.

? Client Friendly Name: Specifies the name of the RADIUS client that forwarded the connection request to the NPS server.

? Client IPv4 Address: Specifies the Internet Protocol (IP) version 4 address of the RADIUS client that forwarded the connection request to the NPS server.

? Client IPv6 Address: Specifies the Internet Protocol (IP) version 6 address of the RADIUS client that forwarded the connection request to the NPS server.

? Client Vendor: Specifies the name of the vendor or manufacturer of the RADIUS client that sends connection requests to the NPS server.

? MS RAS Vendor: Specifies the vendor identification number of the network access server that is requesting authentication.

#### NEW QUESTION 8

- (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 following role services installed:

? DirectAccess and VPN (RRAS)

? Network Policy Server

Remote users have client computers that run either Windows XP, Windows 7, or Windows 8.

You need to ensure that only the client computers that run Windows 7 or Windows 8 can establish VPN connections to Server1.

What should you configure on Server1?

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

**Answer:** A

#### Explanation:

If you want to configure the Operating System condition, click Operating System, and then click Add. In Operating System Properties, click Add, and then specify the operating system settings that are required to match the policy.

The Operating System condition specifies the operating system (operating system version or service pack number), role (client or server), and architecture (x86, x64, or ia64) required for the computer configuration to match the policy.

#### NEW QUESTION 9

- (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 /Domain:contoso.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/cc785343(v=WS.10).aspx) <http://technet.microsoft.com/en-us/library/cc733107.aspx>

#### NEW QUESTION 10

HOTSPOT - (Topic 1)

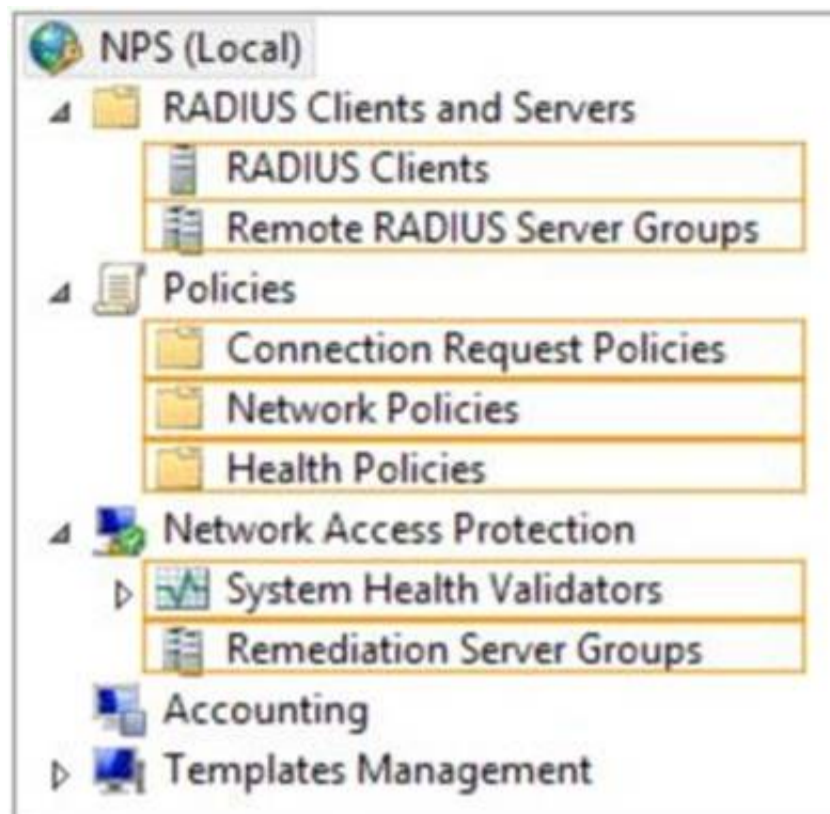
Your network contains a RADIUS server named Server1.

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.

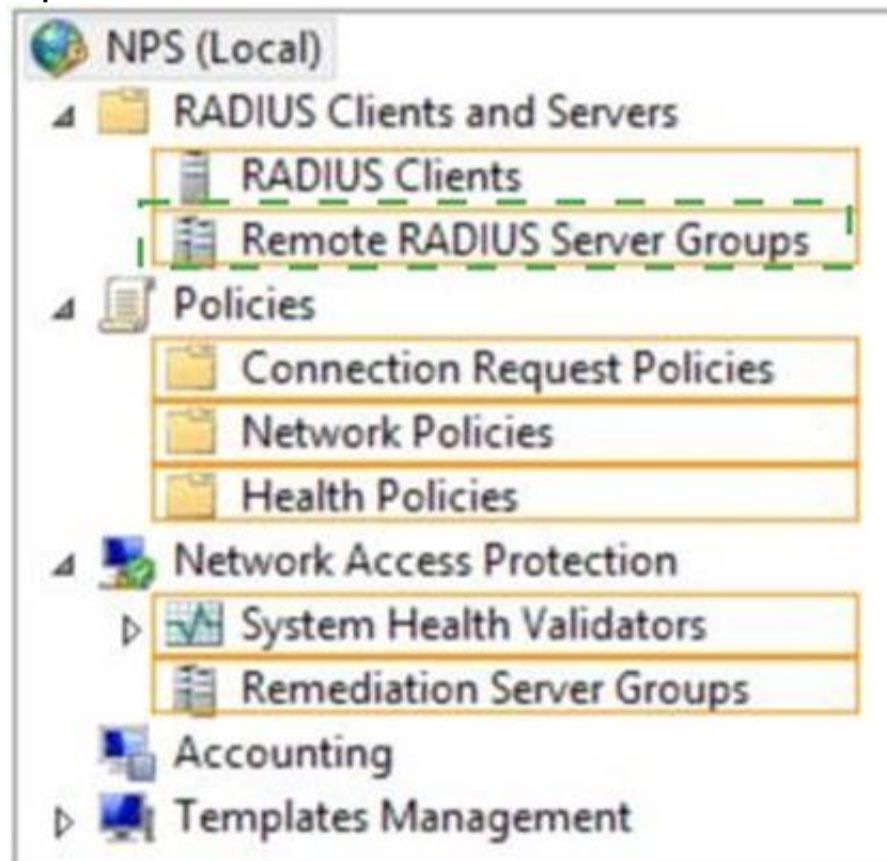
What else should you configure on Server2? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 10

- (Topic 1)

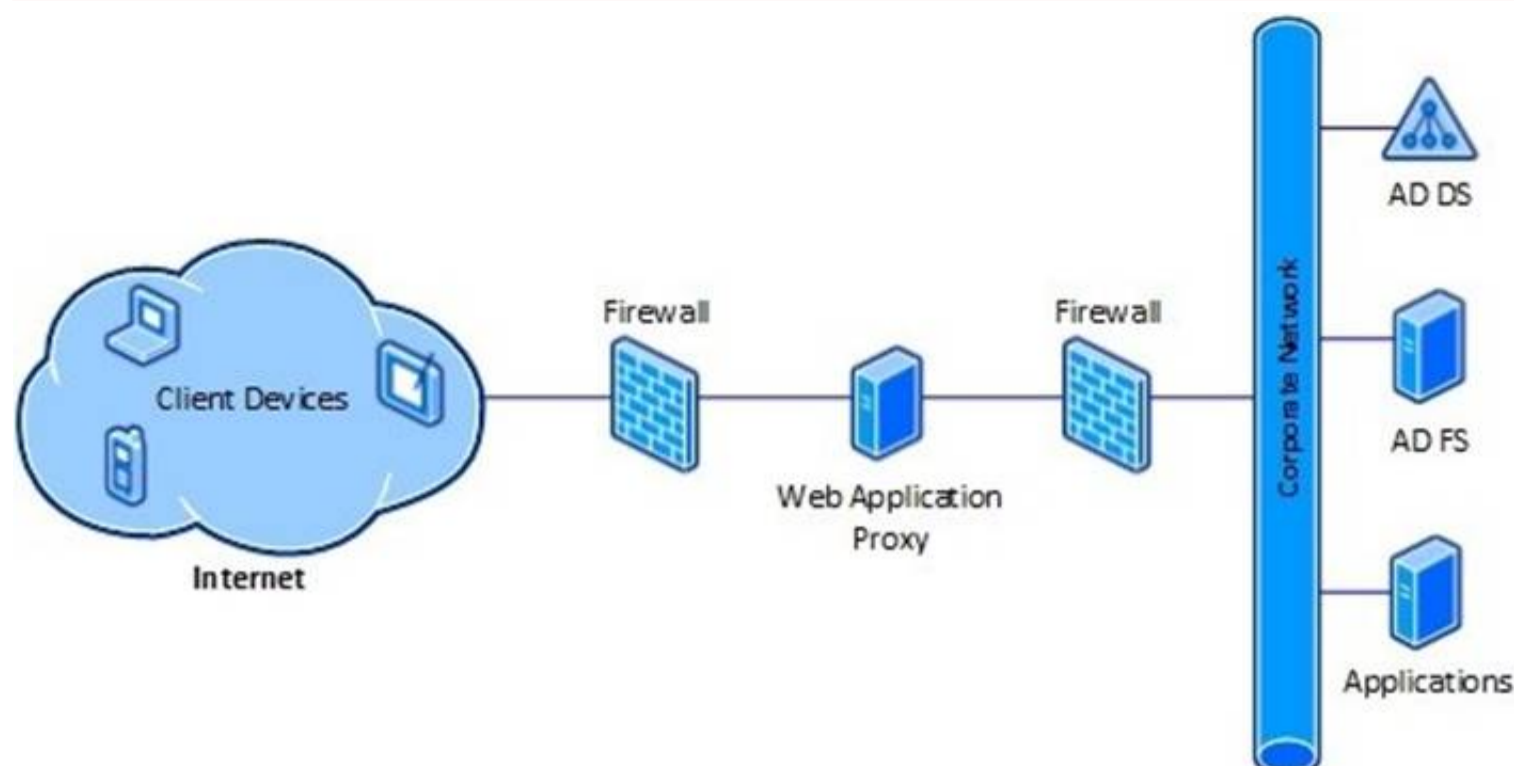
Your network contains an Active Directory domain named contoso.com. You need to install and configure the Web Application Proxy role service. What should you do?

- A. Install the Active Directory Federation Services server role and the Remote Access server role on different servers.
- B. Install the Active Directory Federation Services server role and the Remote Access server role on the same server.
- C. Install the Web Server (IIS) server role and the Application Server server role on the same server.
- D. Install the Web Server (IIS) server role and the Application Server server role on different servers.

**Answer:** A

**Explanation:**

Web Application Proxy is a new Remote Access role service in Windows Server® 2012 R2.



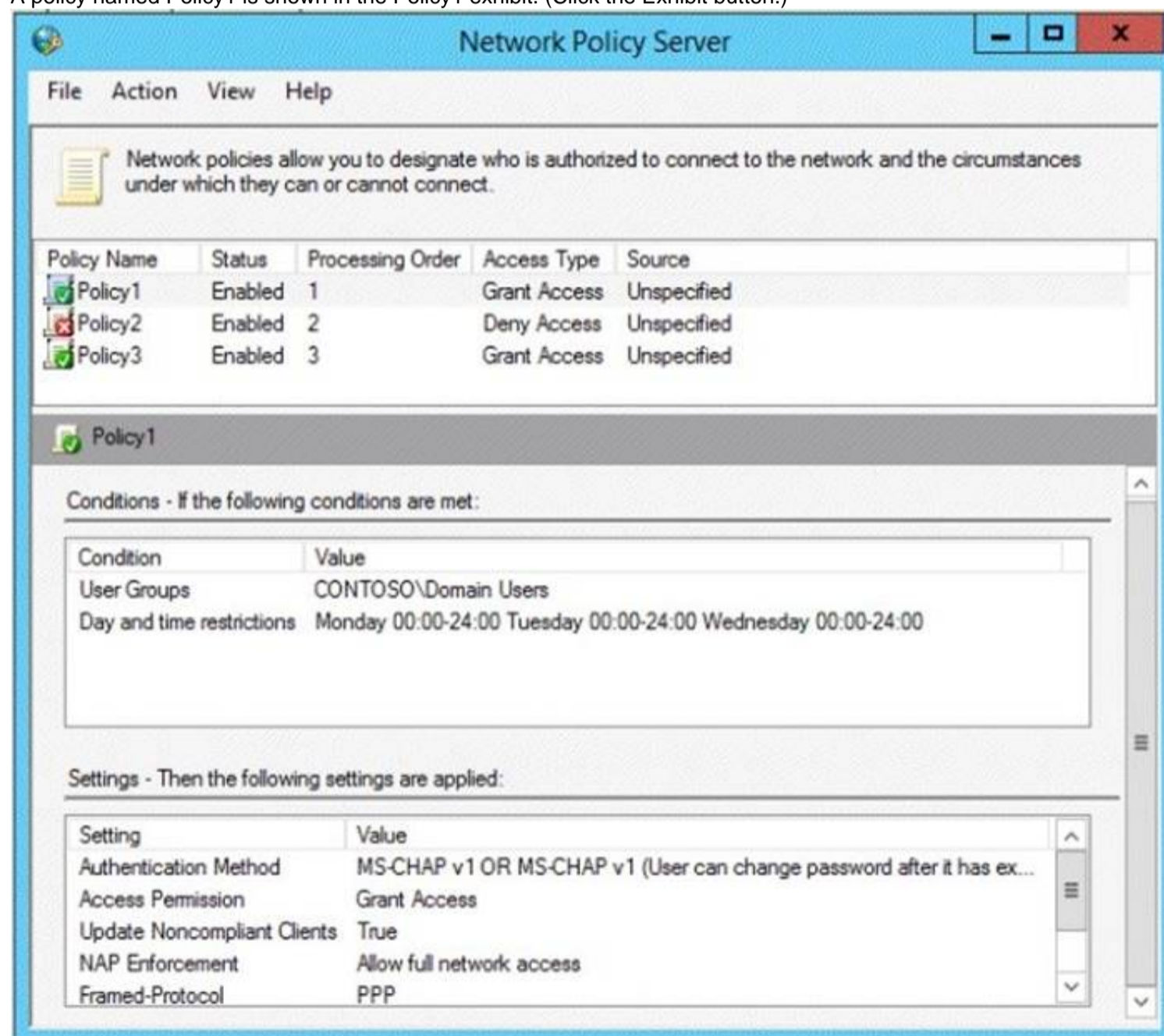
# NEW QUESTION 11

HOTSPOT - (Topic 1)

Your network contains an Active Directory named contoso.com. You have users named User1 and user2.

The Network Access Permission for User1 is set to Control access through NPS Network Policy. The Network Access Permission for User2 is set to Allow access.

A policy named Policy1 is shown in the Policy1 exhibit. (Click the Exhibit button.)



**Network Policy Server**

File Action View Help

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

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

**Policy1**

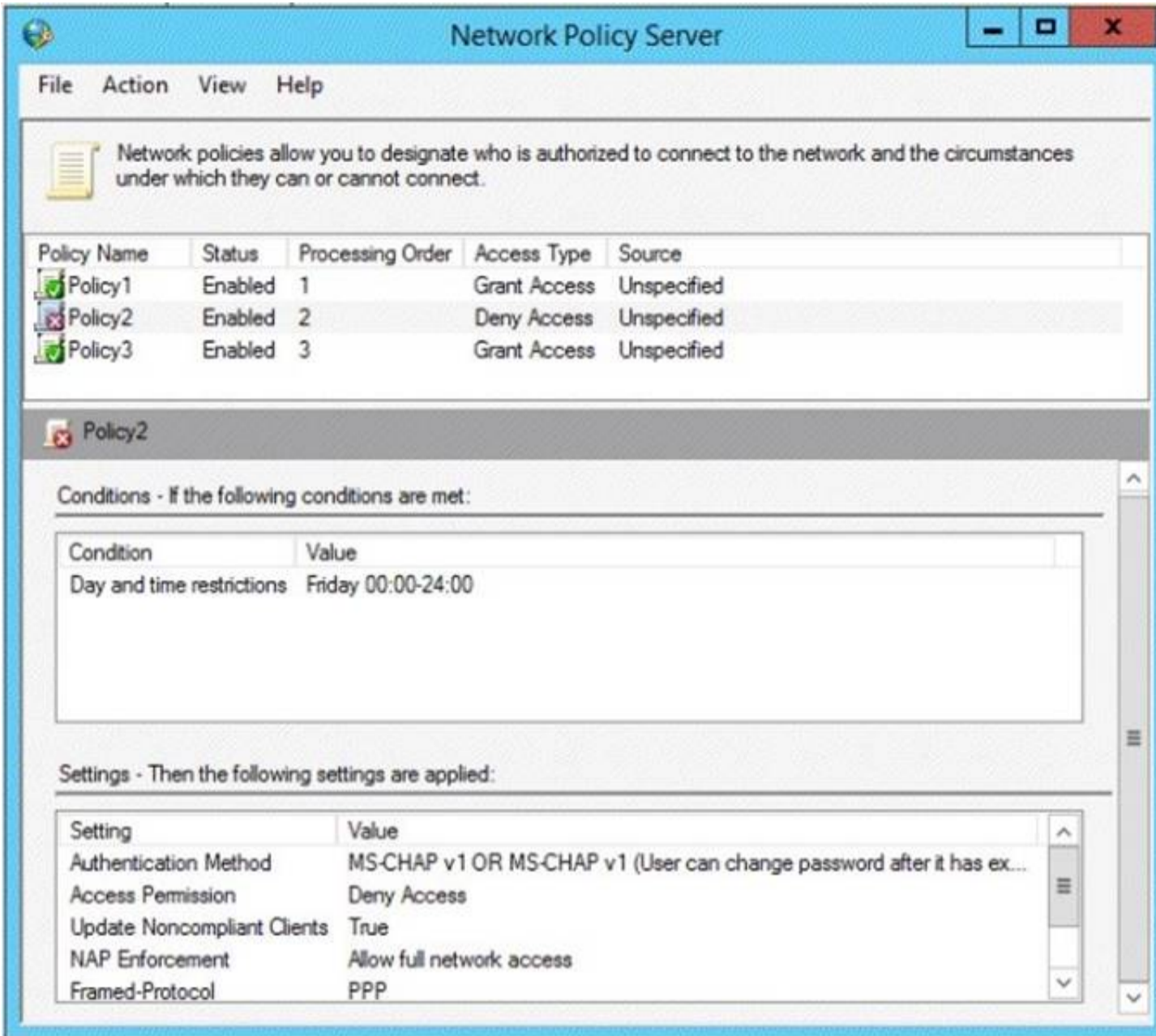
Conditions - If the following conditions are met:

Condition	Value
User Groups	CONTOSO\Domain Users
Day and time restrictions	Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00

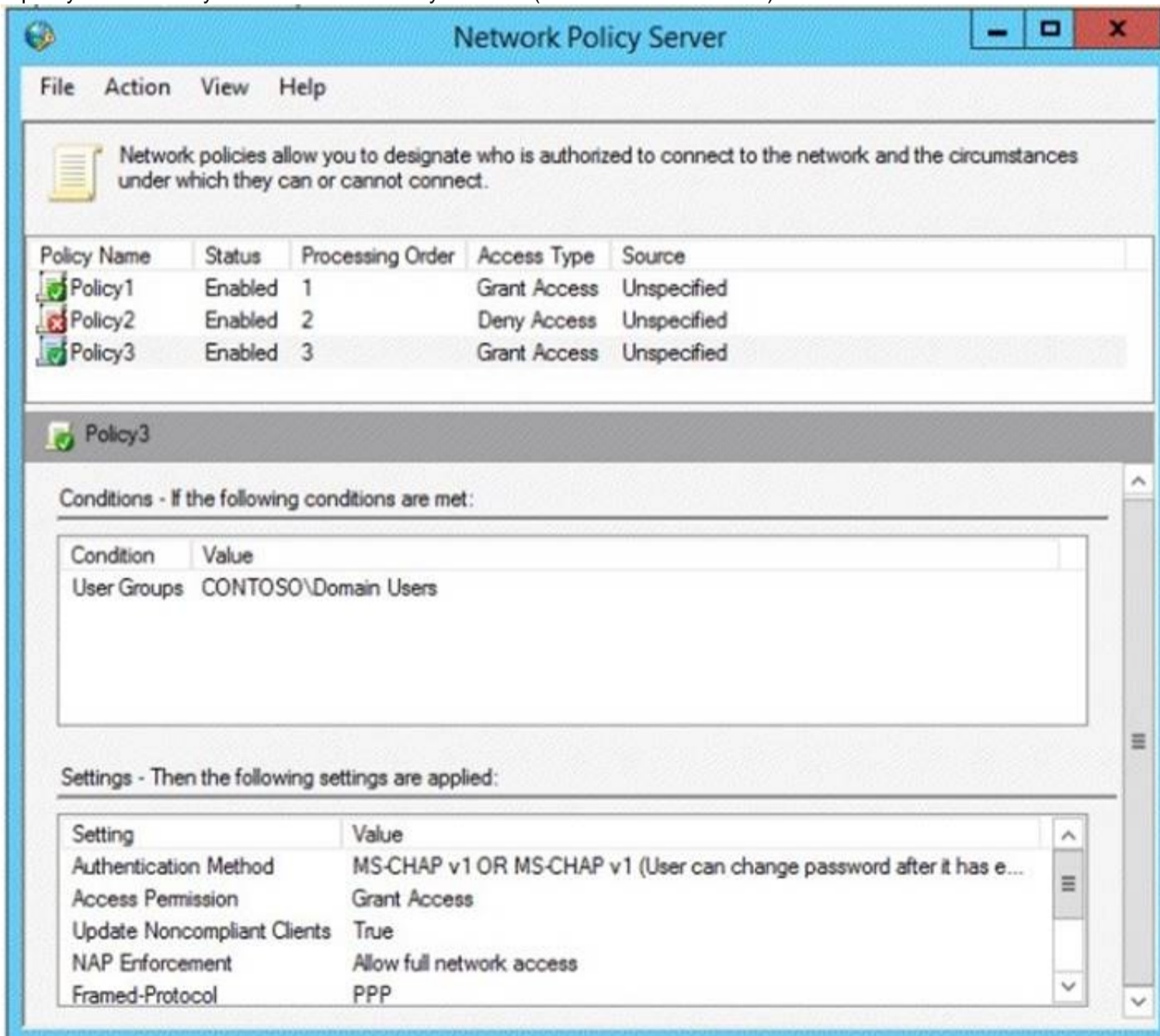
Settings - Then the following settings are applied:

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

A policy named Policy2 is shown in the Policy2 exhibit. (Click the Exhibit button.)



A policy named Policy3 is shown in the Policy3 exhibit. (Click the Exhibit button.)



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

	Yes	No
User1 will be able to establish a VPN connection on Thursday.	<input type="radio"/>	<input type="radio"/>
User1 will be able to establish a VPN connection on Friday.	<input type="radio"/>	<input type="radio"/>
User2 will be able to establish a VPN connection on Friday.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

	Yes	No
User1 will be able to establish a VPN connection on Thursday.	<input checked="" type="radio"/>	<input type="radio"/>
User1 will be able to establish a VPN connection on Friday.	<input type="radio"/>	<input checked="" type="radio"/>
User2 will be able to establish a VPN connection on Friday.	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 16

HOTSPOT - (Topic 1)

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

User name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

To answer, select the appropriate policy for each user in the answer area.

Answer Area

User1:

User2:

User3:

#### Answer Area

User1:

User2:

User3:

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

When you configure multiple network policies in NPS, the policies are an ordered list of rules. NPS evaluates the policies in listed order from first to last. If there is a network policy that matches the connection request, NPS uses the policy to determine whether to grant or deny access to the user or computer connection. Network policies are evaluated according to the processing order. Once a match is found, no further network policy is processed.

Policies are processed in this order:

-Policy2 (applies only to members of Group1)

-Policy1 (applies to all users during specified time slot)

-Policy3 (applies only to members of Group2)

Since policy1 will always apply (sunday 0:00 to saturday 24:00 = always), policy3 will never be evaluated.

Correct answer is : User1: Policy2 User2: Policy1 User3: Policy1

[https://technet.microsoft.com/en-us/library/cc732724\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732724(v=ws.10).aspx)

#### NEW QUESTION 20

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All domain controllers run either Windows Server 2008 or Windows Server 2008 R2. You deploy a new domain controller named DC1 that runs Windows Server 2012 R2. You log on to DC1 by using an account that is a member of the Domain Admins group. 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. Modify the membership of the Group Policy Creator Owners group.
- B. Transfer the PDC emulator operations master role to DC1.
- C. Upgrade all of the domain controllers that run Windows Server 2008.
- D. Raise the functional level of the domain.

**Answer:** D

#### Explanation:

Fine-grained password policies allow you to specify multiple password policies within a single domain so that you can apply different restrictions for password and account lockout policies to different sets of users in a domain. To use a fine-grained password policy, your domain functional level must be at least Windows Server 2008. To enable fine-grained password policies, you first create a Password Settings Object (PSO). You then configure the same settings that you configure for the password and account lockout policies. You can create and apply PSOs in the Windows Server 2012 environment by using the Active Directory Administrative Center (ADAC) or Windows PowerShell.

Step 1: Create a PSO

Applies To: Windows Server 2008, Windows Server 2008 R2

ce:

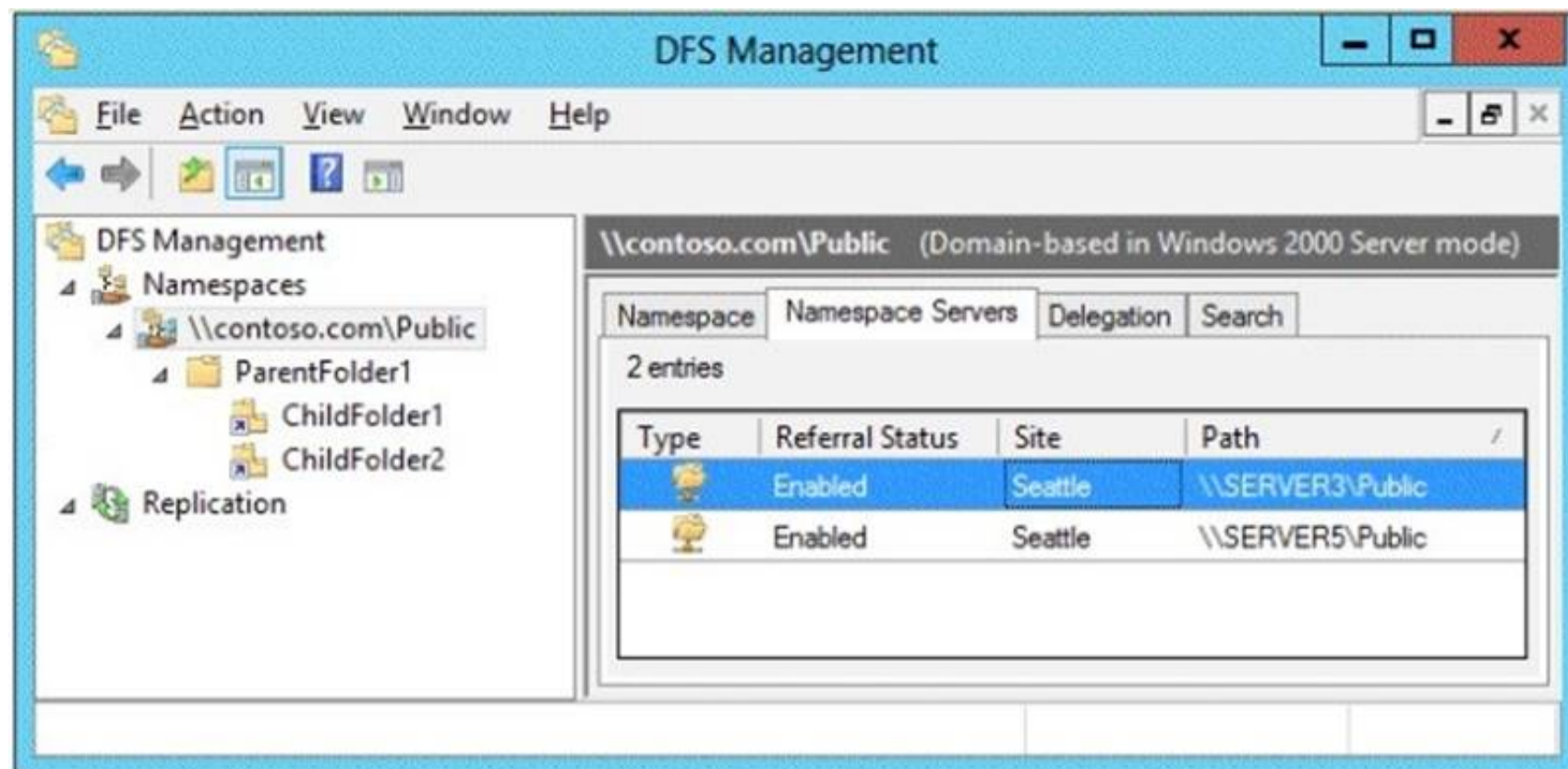
<http://technet.microsoft.com/en-us/library/cc754461%28v=ws.10%29.aspx>

#### NEW QUESTION 21

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The functional level of both the domain and the forest is Windows Server 2008 R2.

The domain contains a domain-based Distributed File System (DFS) namespace that is configured as shown in the exhibit. (Click the Exhibit button.)



You need to enable access-based enumeration on the DFS namespace. What should you do first?

- A. Raise the domain functional level.
- B. Raise the forest functional level.
- C. Install the File Server Resource Manager role service on Server3 and Server5.
- D. Delete and recreate the namespace.

**Answer:** D

**Explanation:**

Access-based enumeration is only supported on a Domain-based Namespace in Windows Server 2008 Mode. This type of Namespace requires a minimum Windows Server 2003 forest functional level and a minimum Windows Server 2008 domain functional level.

The exhibit indicates that the current namespace is a Domain-based Namespace in Windows Server 2000 Mode. To migrate a domain-based namespace from Windows 2000 Server mode to Windows Server 2008 mode, you must export the namespace to a file, delete the namespace, recreate it in Windows Server 2008 mode, and then import the namespace settings.

Reference:

<http://msdn.microsoft.com/en-us/library/cc770287.aspx> <http://msdn.microsoft.com/en-us/library/cc753875.aspx>

**NEW QUESTION 24**

DRAG DROP - (Topic 1)

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 is configured as a Network Policy Server (NPS) server and as a DHCP server.

You need to log all DHCP clients that have windows Firewall disabled.

Which three actions should you perform in sequence? To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a connection request policy.	
Create a network policy.	
Create a remediation server group.	
Create a Windows Security Health Validator (WSHV) configuration.	
Create a health policy.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

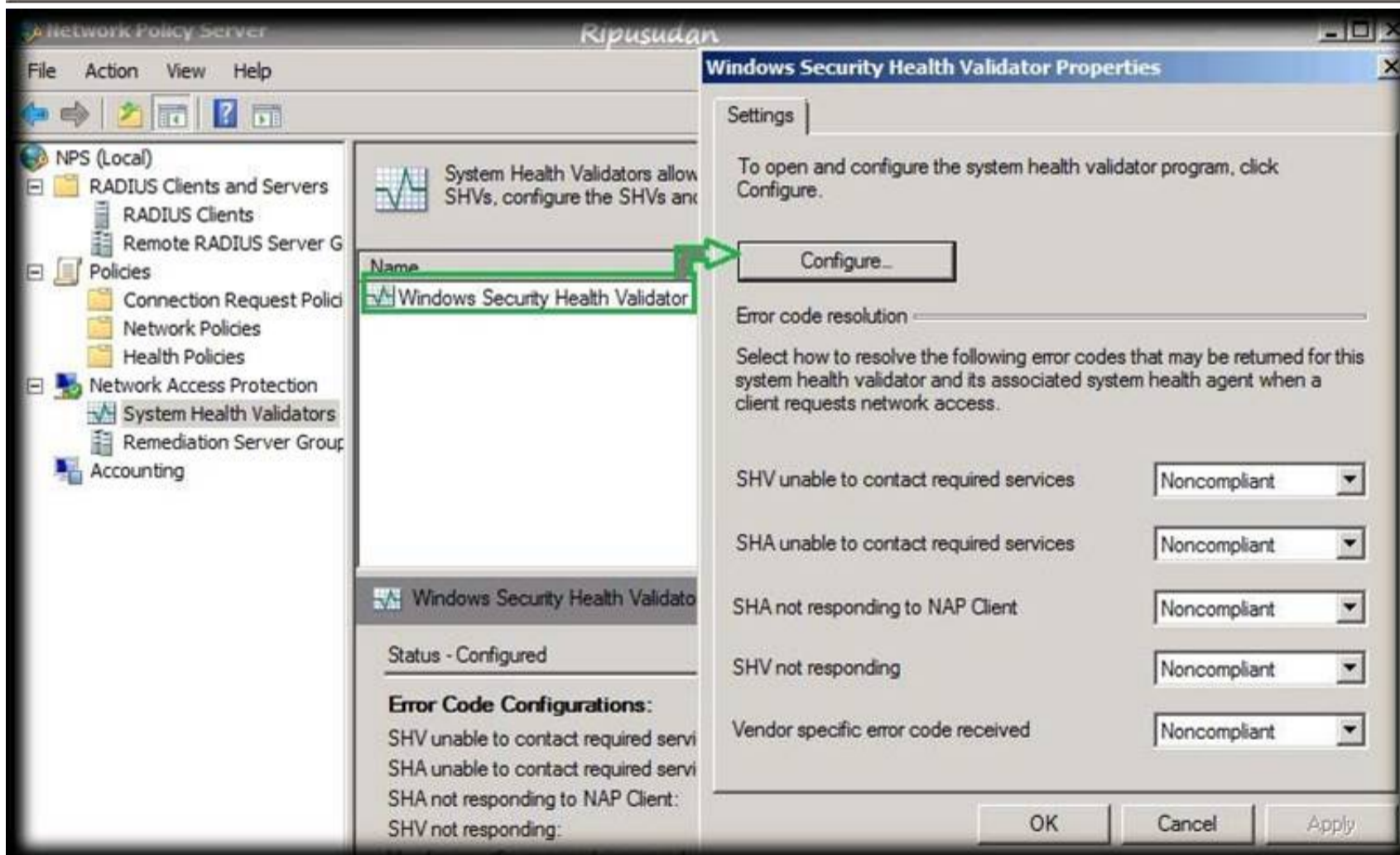
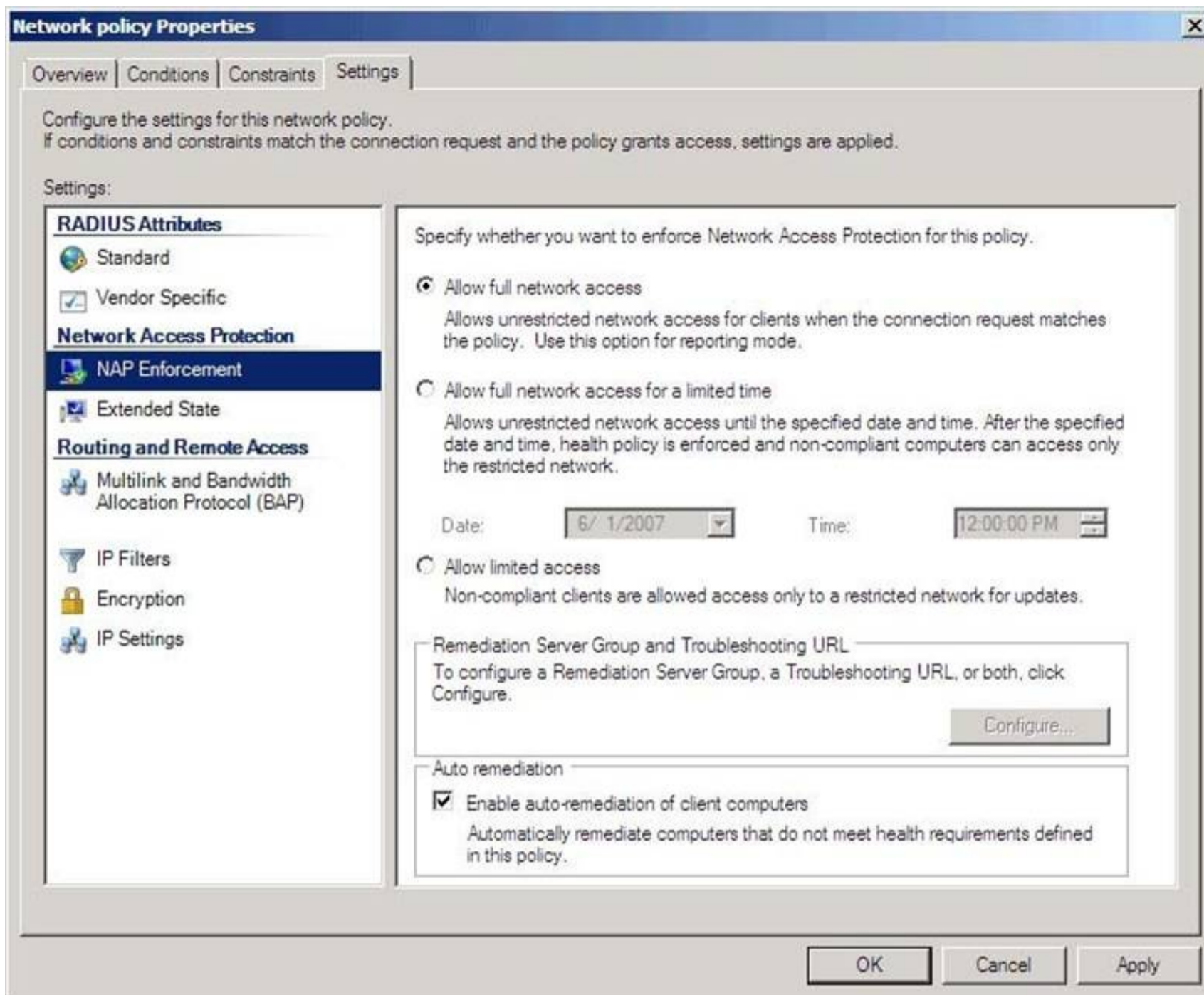
<http://technet.microsoft.com/es-es/library/dd314198%28v=ws.10%29.aspx>

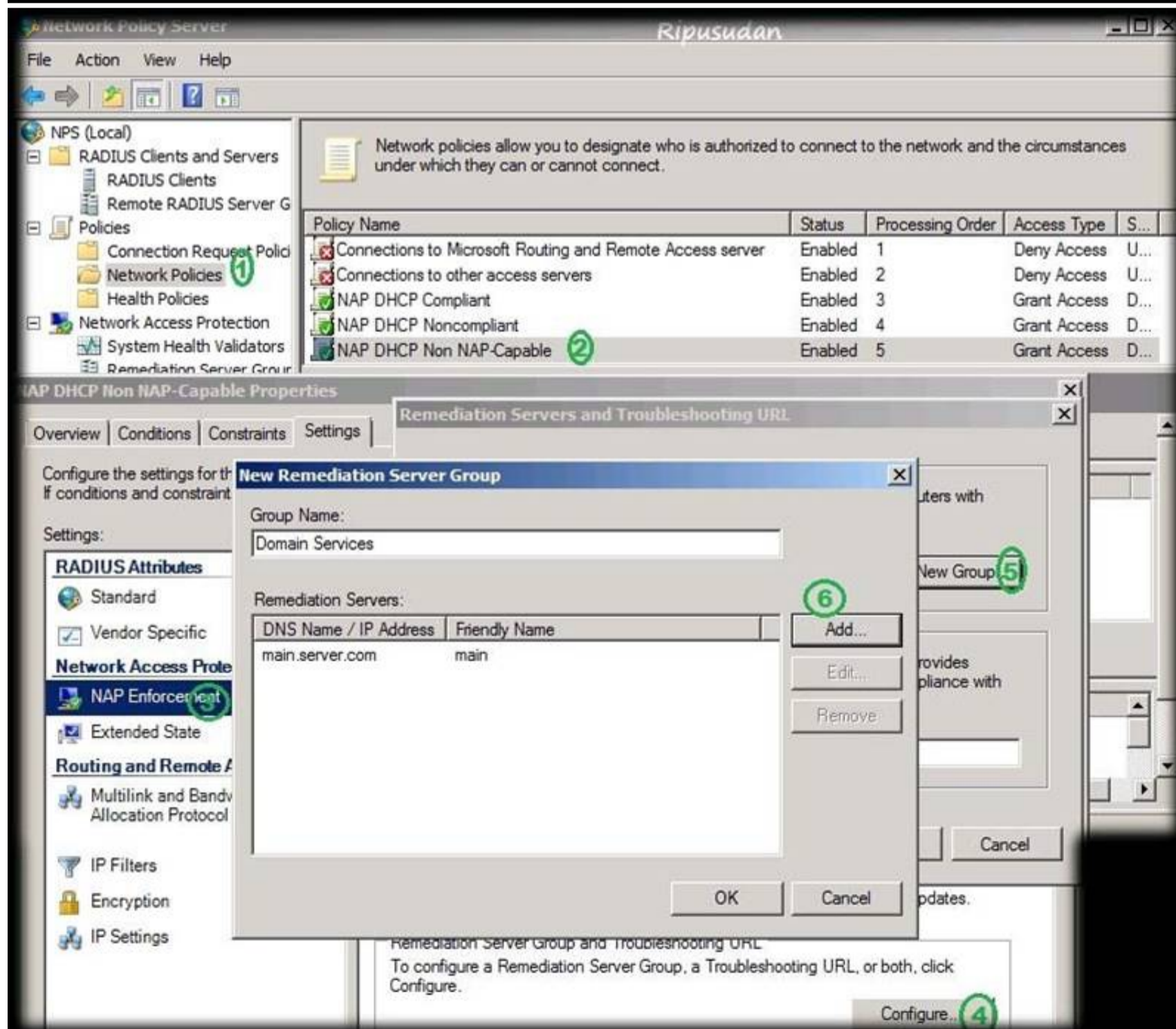
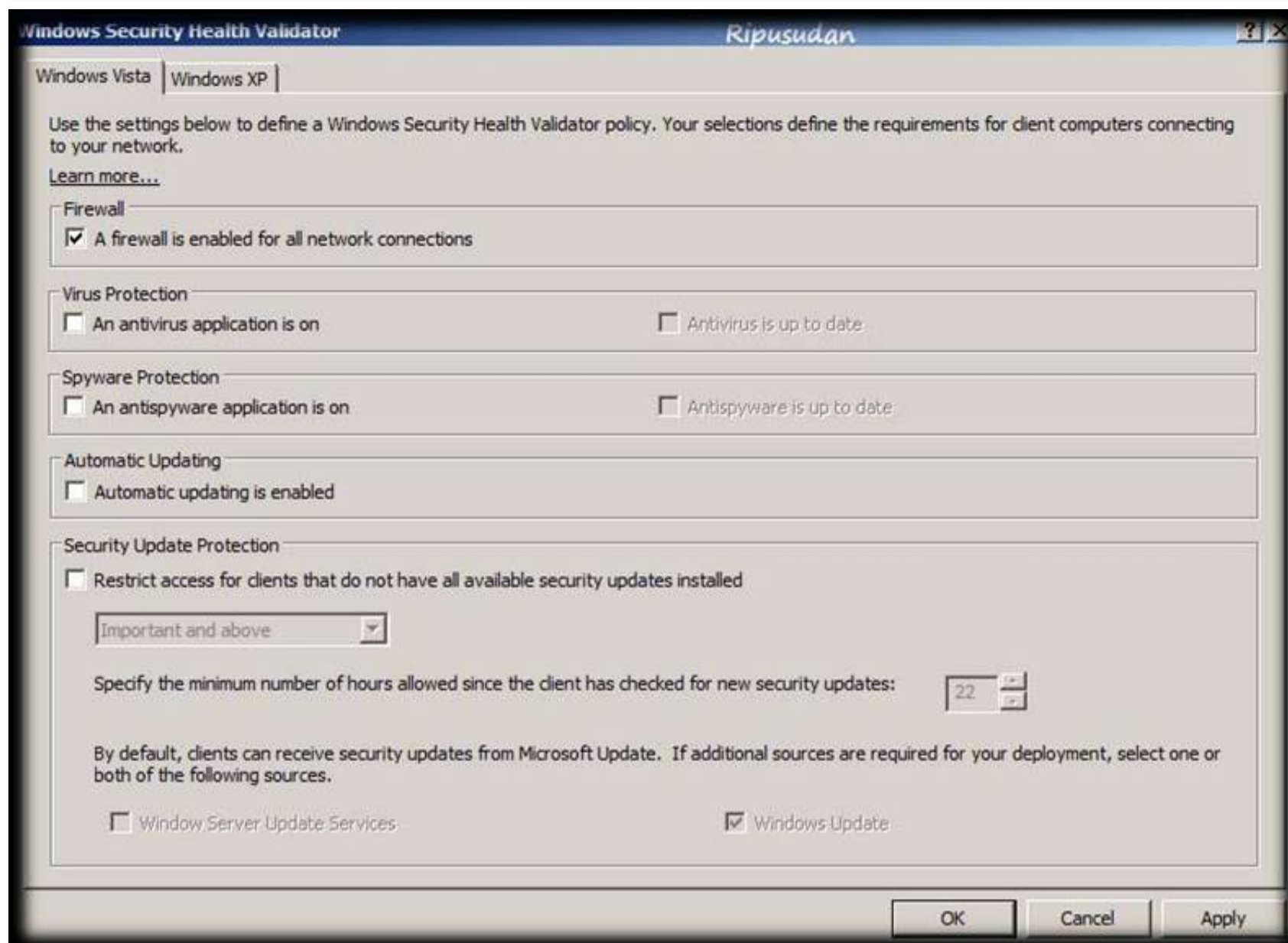
<http://technet.microsoft.com/es-es/magazine/2009.05.goat.aspx>

<http://technet.microsoft.com/es-es/library/dd314173%28v=ws.10%29.aspx>

<http://ripusudan.wordpress.com/2013/03/19/how-to-configure-nap-enforcement-for-dhcp/> <http://technet.microsoft.com/es-es/magazine/2009.05.goat.aspx>

<http://technet.microsoft.com/en-us/library/dd125379%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/cc772356%28v=ws.10%29.aspx>





\* With NPS, you can create client health policies using SHVs that allow NAP to detect, enforce, and remediate client computer configurations. WSHA and WSHV provide the following functionality for NAP-capable computers: The client computer has firewall software installed and enabled.

\* Example measurements of health include:  
 The operational status of Windows Firewall. Is the firewall enabled or disabled?

In NAP terminology, verifying that a computer meets your defined health requirements is called health policy validation. NPS performs health policy validation for NAP.

#### NEW QUESTION 25

- (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2.

On Server1, you configure a custom Data Collector Set (DCS) named DCS1. DCS1 is configured to store performance log data in C:\Logs.

You need to ensure that the contents of C:\Logs are deleted automatically when the folder reaches 100 MB in size.

What should you configure?

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

**Answer: B**

#### Explanation:

To configure data management for a Data Collector Set

1. In Windows Performance Monitor, expand Data Collector Sets and click User Defined.

2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click Data Manager.

3. On the Data Manager tab, you can accept the default values or make changes according to your data retention policy. See the table below for details on each option.

When Minimum free disk or Maximum folders is selected, previous data will be deleted according to the Resource policy you choose (Delete largest or Delete oldest) when the limit is reached. When Apply policy before the data collector set starts is selected, previous data will be deleted according to your selections before the data collector set creates its next log file.

When Maximum root path size is selected, previous data will be deleted according to your selections when the root log folder size limit is reached.

4. Click the Actions tab. You can accept the default values or make changes. See the table below for details on each option.

5. When you have finished making your changes, click OK.

#### NEW QUESTION 29

DRAG DROP - (Topic 1)

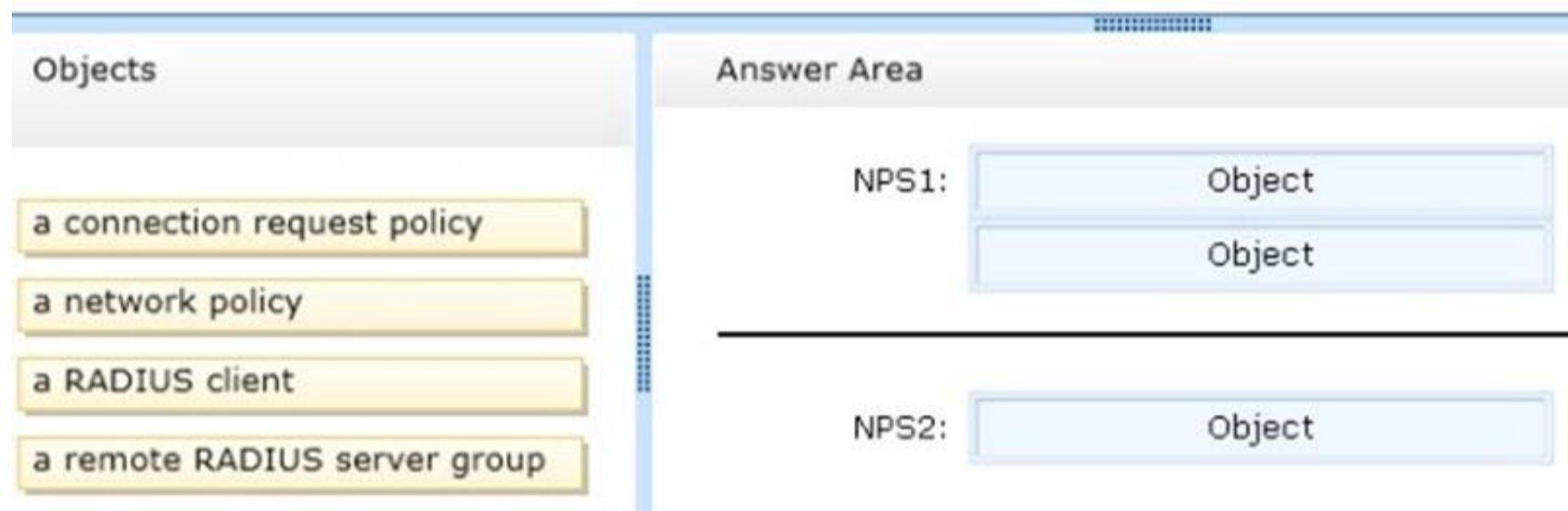
Your network contains an Active Directory forest named contoso.com. The forest contains a Network Policy Server (NPS) server named NPS1 and a VPN server named VPN1. VPN1 forwards all authentication requests to NPS1.

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?

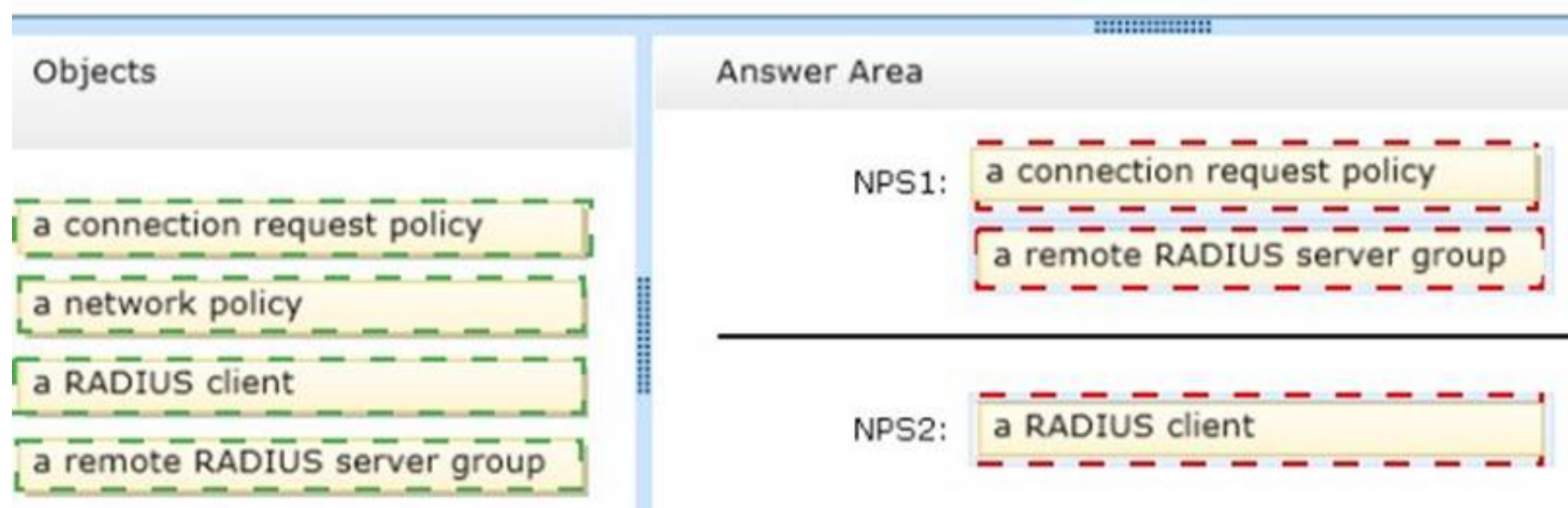
To answer, drag the appropriate objects to the correct NPS servers. Each object may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:



### NEW QUESTION 32

- (Topic 1)

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. Recover the items by using Active Directory Recycle Bin.
- B. Modify the Recycled attribute of Group1.
- C. Perform tombstone reanimation.
- D. Perform an authoritative restore.
- E. Perform a non- authoritative restore.

**Answer:** A

#### Explanation:

Active Directory Recycle Bin helps minimize directory service downtime by enhancing your ability to preserve and restore accidentally deleted Active Directory objects without restoring Active Directory data from backups, restarting Active Directory Domain Services (AD DS), or rebooting domain controllers.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion. For example, restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains.

### NEW QUESTION 33

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All user accounts reside in an organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preference of GPO1 to add a shortcut named Link1 to the desktop of each user.

You discover that when a user deletes Link1, the shortcut is removed permanently from the desktop.

You need to ensure that if a user deletes Link1, the shortcut is added to the desktop again. What should you do?

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

**Answer:** B

#### Explanation:

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

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

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

References:

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

### NEW QUESTION 35

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. All servers run Windows Server 2012 R2.

You need to collect the error events from all of the servers on Server1. The solution must ensure that when new servers are added to the domain, their error events are collected automatically on Server1.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Answer:** BC

**Explanation:**

To set up a Source-Initiated Subscription with Windows Server 2003/2008 so that events of interest from the Security event log of several domain controllers can be forwarded to an administrative workstation.

\* Group Policy

The forwarding computer needs to be configured with the address of the server to which the events are forwarded. This can be done with the following group policy setting:

Computer configuration-Administrative templates-Windows components-Event forwarding- Configure the server address, refresh interval, and issue certificate authority of a target subscription manager.

\* Edit the GPO and browse to Computer Configuration | Policies | Administrative Templates

| Windows Components | Event Forwarding - Configure the server address, refresh interval, and issuer certificate authority of a target Subscription Manager.

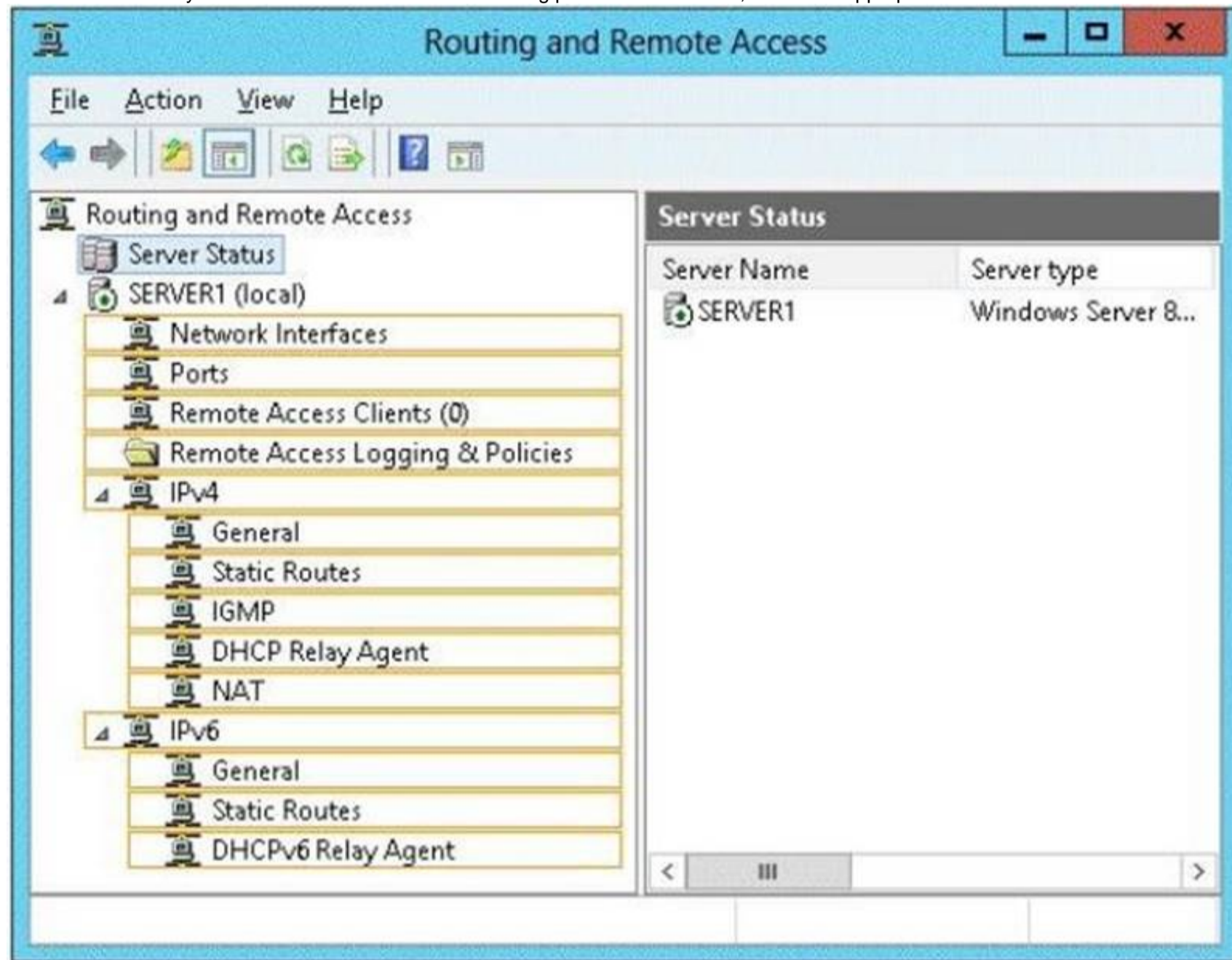
**NEW QUESTION 38**

HOTSPOT - (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has two network adapters and is located in a perimeter network.

You need to install the RIP version 2 routing protocol on Server1.

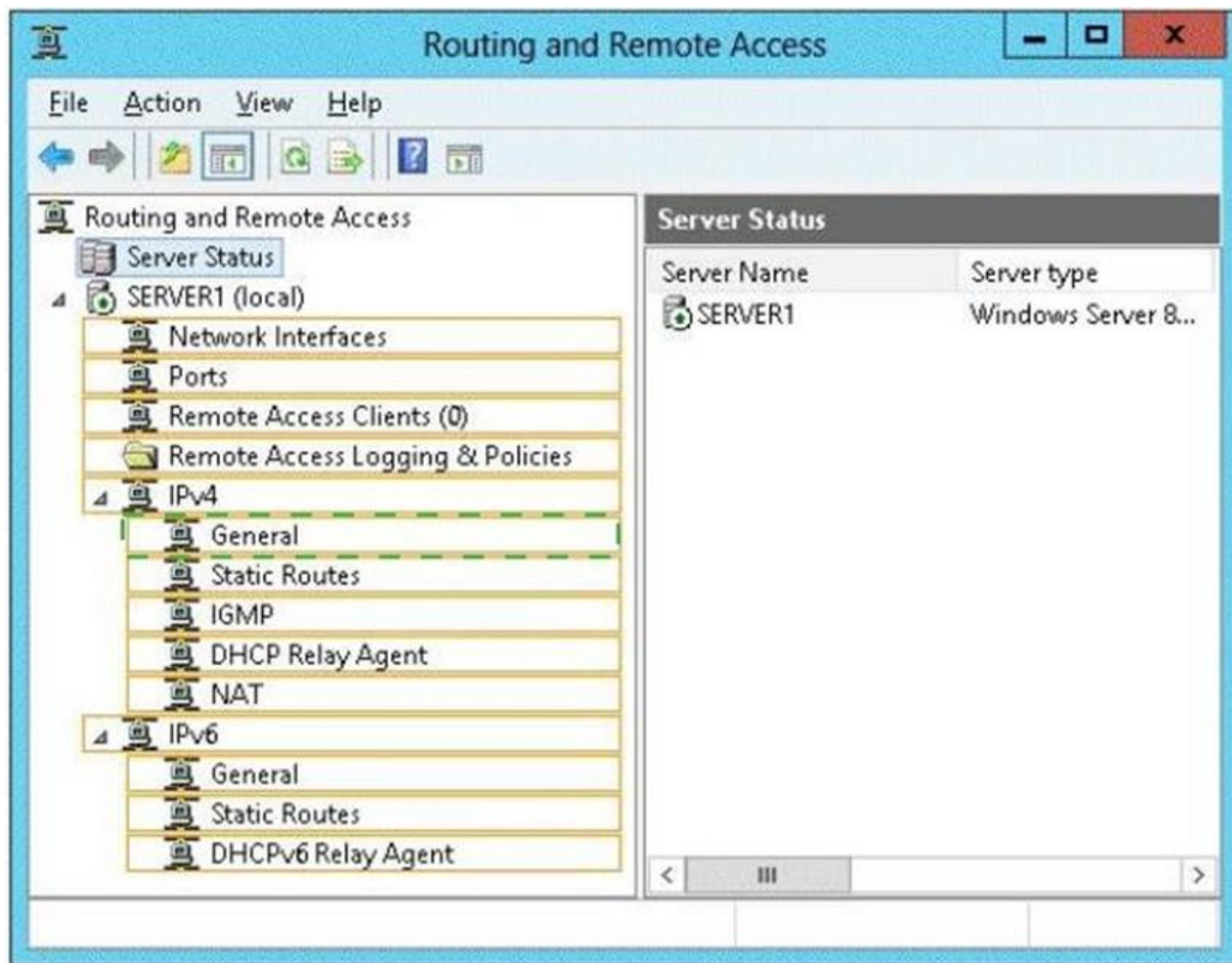
Which node should you use to add the RIP version 2 routing protocol? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 40

- (Topic 1)

Your network contains two Active Directory domains named contoso.com and adatum.com.

The network contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the DNS Server server role installed. Server1 has a copy of the contoso.com DNS zone.

You need to configure Server1 to resolve names in the adatum.com domain. The solution must meet the following requirements:

Prevent the need to change the configuration of the current name servers that host zones for adatum.com. Minimize administrative effort.

Which type of zone should you create?

- A. Secondary
- B. Stub
- C. Reverse lookup
- D. Primary

**Answer: B**

#### Explanation:

When a zone that this DNS server hosts is a stub zone, this DNS server is a source only for information about the authoritative name servers for this zone. The zone at this server must be obtained from another DNS server that hosts the zone. This DNS server must have network access to the remote DNS server to copy the authoritative name server information about the zone.

A stub zone is a copy of a zone that contains only necessary resource records (Start of Authority (SOA), Name Server (NS), and Address/Host (A) record) in the master zone and acts as a pointer to the authoritative name server. The stub zone allows the server to forward queries to the name server that is authoritative for the master zone without going up to the root name servers and working its way down to the server. While a stub zone can improve performance, it does not provide redundancy or load sharing.



You can use stub zones to:

Keep delegated zone information current. By updating a stub zone for one of its child zones regularly, the DNS server that hosts both the parent zone and the stub zone will maintain a current list of authoritative DNS servers for the child zone.

Improve name resolution. Stub zones enable a DNS server to perform recursion using the stub zone's list of name servers, without having to query the Internet or an internal root server for the DNS namespace.

Simplify DNS administration. By using stub zones throughout your DNS infrastructure, you can distribute a list of the authoritative DNS servers for a zone without using secondary zones. However, stub zones do not serve the same purpose as secondary zones, and they are not an alternative for enhancing redundancy and load sharing.

There are two lists of DNS servers involved in the loading and maintenance of a stub zone: The list of master servers from which the DNS server loads and updates a stub zone. A master server may be a primary or secondary DNS server for the zone. In both cases, it will have a complete list of the DNS servers for the zone.

The list of the authoritative DNS servers for a zone. This list is contained in the stub zone using name server (NS) resource records.

When a DNS server loads a stub zone, such as widgets. tailspintoys.com, it queries the master servers, which can be in different locations, for the necessary resource records of the authoritative servers for the zone widgets. tailspintoys.com. The list of master servers may contain a single server or multiple servers, and it can be changed anytime.

References:

<http://technet.microsoft.com/en-us/library/cc771898.aspx> <http://technet.microsoft.com/en-us/library/cc754190.aspx> <http://technet.microsoft.com/en-us/library/cc730980.aspx>

#### NEW QUESTION 45

- (Topic 1)

You have a server named Server 1.

You enable BitLocker Drive Encryption (BitLocker) on Server 1.

You need to change the password for the Trusted Platform Module (TPM) chip. What should you run on Server1?

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

**Answer: B**

#### Explanation:

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

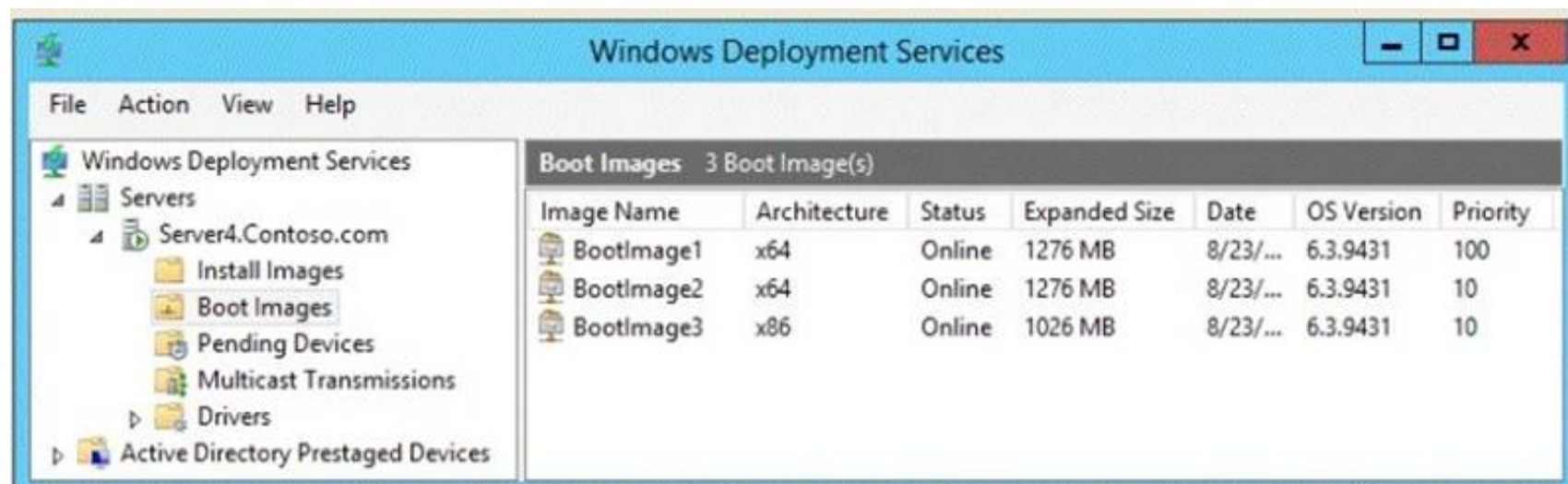
Use the ConvertTo-TpmOwnerAuthcmdlet to create an owner authorization value. You can specify a new owner authorization value or specify a file that contains the new value.

#### NEW QUESTION 48

HOTSPOT - (Topic 1)

You have a server named Server4 that runs Windows Server 2012 R2. Server4 has the Windows Deployment Services server role installed.

Server4 is configured as shown in the exhibit. (Click the Exhibit button.)



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

#### Answer Area

When you connect to Windows Deployment Services (WDS) from an x64 client computer, you can select ...

When you connect to Windows Deployment Services (WDS) from an x64 client computer, the default image will be ...

#### Answer Area

When you connect to Windows Deployment Services (WDS) from an x64 client computer, you can select ...

- BootImage3 only.
- BootImage1 and BootImage2 only.
- BootImage2 and BootImage3 only.
- BootImage1, BootImage2, and BootImage3

When you connect to Windows Deployment Services (WDS) from an x64 client computer, the default image will be ...

- BootImage1.
- BootImage2.
- BootImage3.

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

#### Answer Area

When you connect to Windows Deployment Services (WDS) from an x64 client computer, you can select ...

- BootImage3 only.
- BootImage1 and BootImage2 only.
- BootImage2 and BootImage3 only.
- BootImage1, BootImage2, and BootImage3

When you connect to Windows Deployment Services (WDS) from an x64 client computer, the default image will be ...

- BootImage1.
- BootImage2.
- BootImage3.

#### NEW QUESTION 52

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a read-only domain controller (RODC) named RODC1.

You create a global group named RODC\_Admins.

You need to provide the members of RODC\_Admins with the ability to manage the hardware and the software on RODC1. The solution must not provide RODC\_Admins with the ability to manage Active Directory objects.

What should you do?

- A. From Active Directory Site and Services, configure the Security settings of the RODC1 server object.
- B. From Windows PowerShell, run the Set-ADAccountControlcmdlet.
- C. From a command prompt, run the dsmgmt local roles command.
- D. From Active Directory Users and Computers, configure the Member Of settings of the RODC1 account.

**Answer: C**

#### Explanation:

RODC: using the dsmgmt.exe utility to manage local administrators

One of the benefits of RODC is that you can add local administrators who do not have full access to the domain administration. This gives them the ability to manage the server but not add or change active directory objects unless those roles are delegated. Adding this type of user is done using the dsmdmt.exe utility at the command prompt.

#### NEW QUESTION 57

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.

Client computers run either Windows 7 or Windows 8. All of the client computers have an application named App1 installed.

The domain contains a Group Policy object (GPO) named GPO1 that is applied to all of the client computers.

You need to add a system variable named App1Data to all of the client computers. Which Group Policy preference should you configure?

- A. Environment
- B. Ini Files
- C. Data Sources
- D. Services

**Answer:** A

#### Explanation:

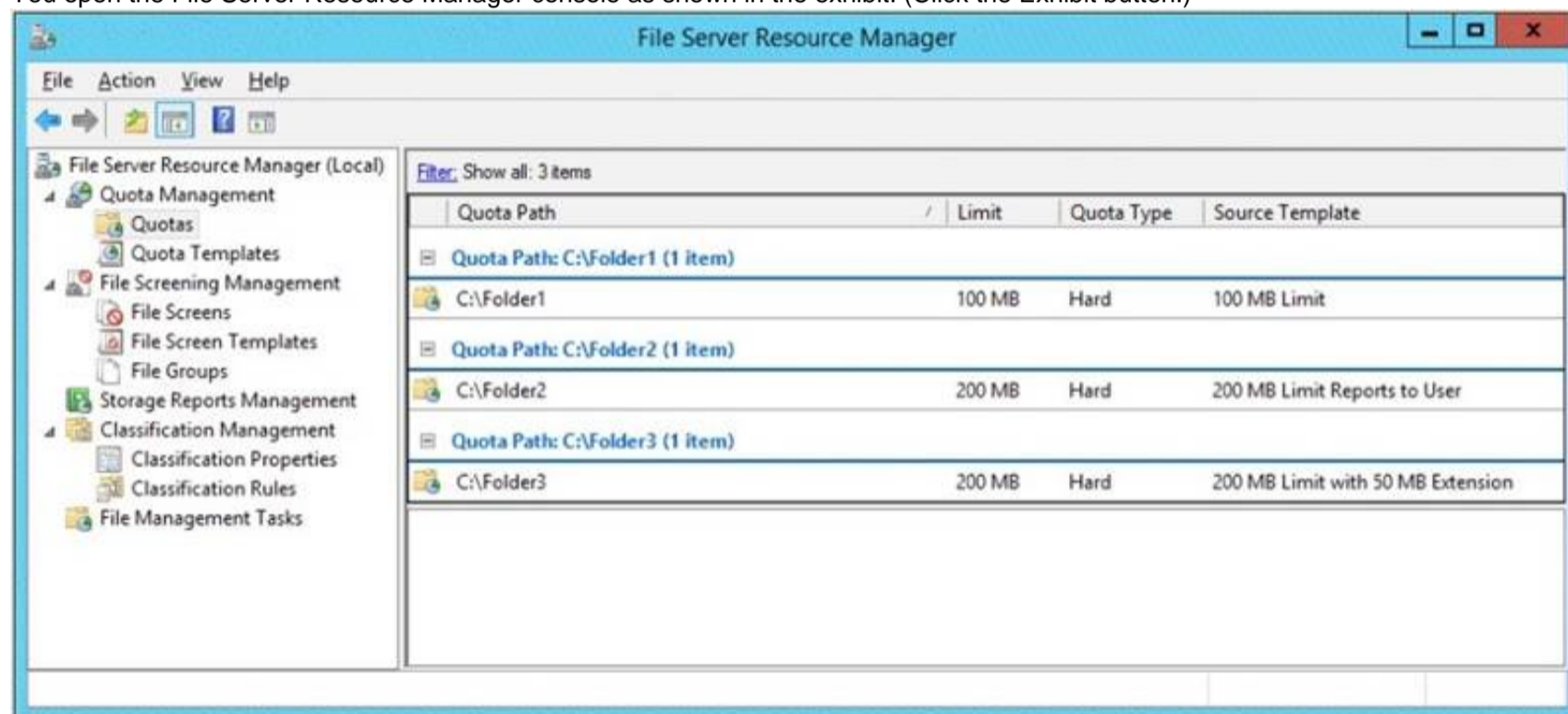
Environment Variable preference items allow you to create, update, replace, and delete user and system environment variables or semicolon-delimited segments of the PATH variable. Before you create an Environment Variable preference item, you should review the behavior of each type of action possible with this extension.

#### NEW QUESTION 60

- (Topic 1)

You have a file server that has the File Server Resource Manager role service installed.

You open the File Server Resource Manager console as shown in the exhibit. (Click the Exhibit button.)



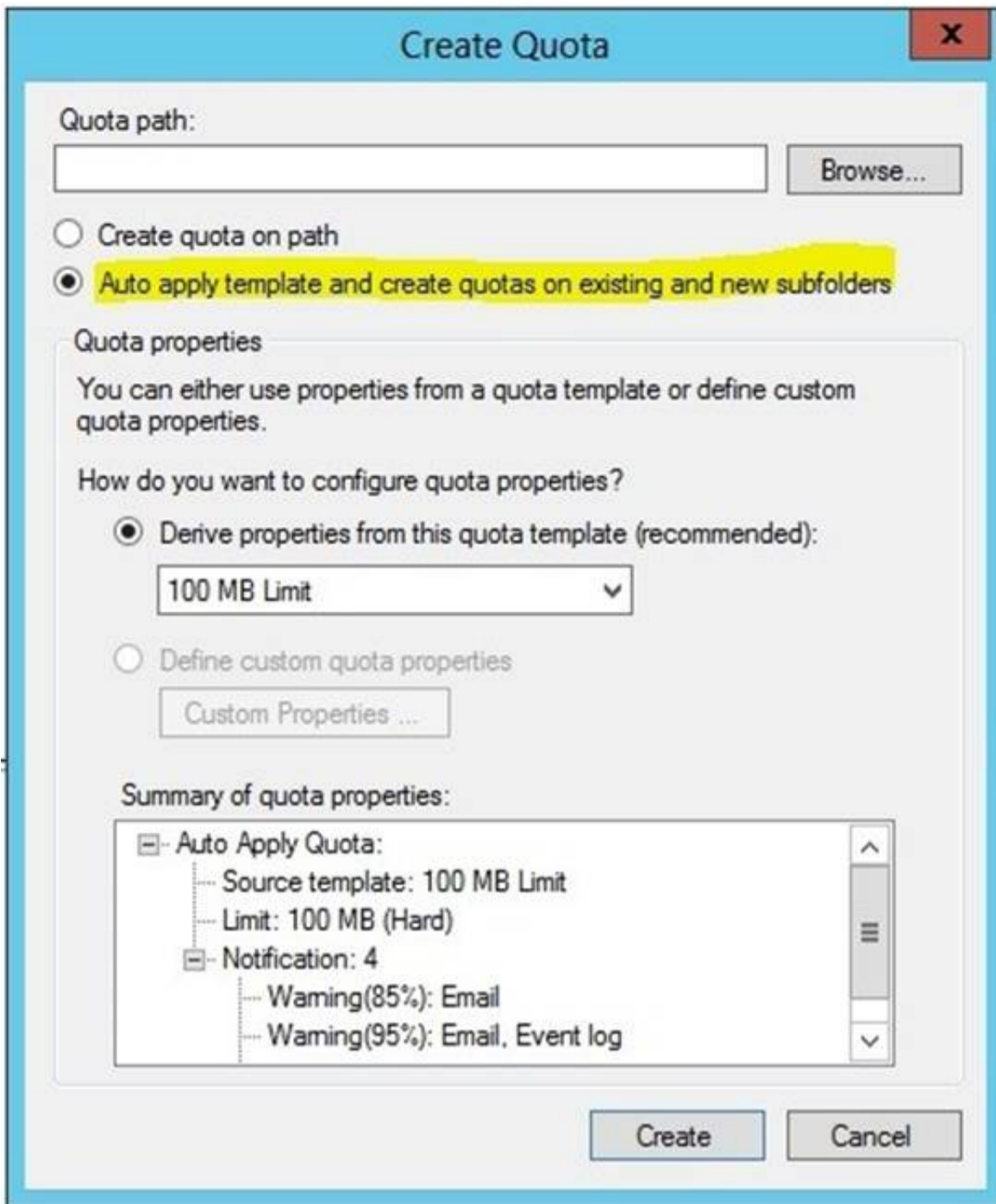
You need to ensure that all of the folders in Folder1 have a 100-MB quota limit. What should you do?

- A. Run the Update FsrmQuotacmdlet.
- B. Run the Update-FsrmAutoQuotacmdlet.
- C. Create a new quota for Folder1.
- D. Modify the quota properties of Folder1.

**Answer:** C

#### Explanation:

By using auto apply quotas, you can assign a quota template to a parent volume or folder. Then File Server Resource Manager automatically generates quotas that are based on that template. Quotas are generated for each of the existing subfolders and for subfolders that you create in the future.



Ref: <http://technet.microsoft.com/en-us/library/cc731577.aspx>

#### NEW QUESTION 64

- (Topic 1)

Your network contains two servers named Server1 and Server2 that run windows Server 2012 R2. Server1 and Server2 have the Windows Server Update Services server role installed.

Server1 synchronizes from Microsoft Update. Server2 is a Windows Server Update Services (WSUS) replica of Server1.

You need to configure replica downstream servers to send Server1 summary information about the computer update status.

What should you do?

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

**Answer:** A

#### Explanation:

WSUS Reporting Rollup Sample Tool

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

Reference: <http://technet.microsoft.com/en-us/windowsserver/bb466192.aspx>

#### NEW QUESTION 65

DRAG DROP - (Topic 1)

Your network contains an Active Directory forest named contoso.com. All domain controllers run Windows Server 2008 R2.

The schema is upgraded to Windows Server 2012 R2.

Contoso.com contains two servers. The servers are configured as shown in the following table.

Server name	Operating system	Role
Server1	Windows Server 2012 R2	Web Server (IIS) server role Network Load Balancing (NLB) feature
Server2	Windows Server 2012 R2	Web Server (IIS) server role Network Load Balancing (NLB) feature

Server1 and Server2 host a load-balanced application pool named AppPool1.

You need to ensure that AppPool1 uses a group Managed Service Account as its identity. Which three actions should you perform?

To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Run the <b>Install-ADServiceAccount</b> cmdlet.	
Modify the settings of AppPool1.	
Run the <b>New-ADServiceAccount</b> cmdlet.	
Install a domain controller that runs Windows Server 2012 R2.	
Run the <b>Set-ADServiceAccount</b> cmdlet.	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Note: Box 1:

Group Managed Service Accounts Requirements:

At least one Windows Server 2012 Domain Controller

A Windows Server 2012 or Windows 8 machine with the ActiveDirectory PowerShell module, to create/manage the gMSA.

A Windows Server 2012 or Windows 8 domain member to run/use the gMSA. Box 2:

To create a new managed service account

? On the domain controller, click Start, and then click Run. In the Open box, type dsa. msc, and then click OK to open the Active Directory Users and Computers snap-in. Confirm that the Managed Service Account container exists.

? Click Start, click All Programs, click Windows PowerShell 2.0, and then click the Windows PowerShell icon.

? Run the following command: New-ADServiceAccount [- SAMAccountName<String>] [-Path <String>].

Box 3:

Configure a service account for Internet Information Services

Organizations that want to enhance the isolation of IIS applications can configure IIS application pools to run managed service accounts.

To use the Internet Information Services (IIS) Manager snap-in to configure a service to use a managed service account

? Click Start, point to Administrative Tools, and then click Internet Information

Services (IIS) Manager.

? Double-click <Computer name>, double-click Application Pools, right-click <Pool

Name>, and click Advanced Settings.

? In the Identity box, click ..., click Custom Account, and then click Set.

? Type the name of the managed service account in the format domainname\accountname.

**NEW QUESTION 67**

- (Topic 1)

You manage a server that runs Windows Server 2012 R2. The server has the Windows Deployment Services server role installed.

You have a desktop computer that has the following configuration:

? Computer name: Computer1

? Operating system: Windows 8

? MAC address: 20-CF-30-65-D0-87

? GUID: 979708BF-C04B-4525-9FE0-C4150BB6C618

You need to configure a pre-staged device for Computer1 in the Windows Deployment Services console.

Which two values should you assign to the device ID? (Each correct answer presents a complete solution. Choose two.)

- A. 20CF3065D08700000000000000000000  
B. 979708BFC04B45259FE0C4150BB6C618  
C. 979708BF-C04B-452S-9FE0-C4150BB6C618  
D. 00000000000000000000000020CF306SD087  
E. 00000000-0000-0000-0000-C41S0BB6C618

**Answer:** CD

**Explanation:**

In the text box, type the client computer's MAC address preceded with twenty zeros or the globally unique identifier (GUID) in the format: {XXXXXXXX-XXXX-XXXX-XXX- XXXXXXXXXXXXX}.

\* To add or remove pre-staged client to/from AD DS, specify the name of the computer or the device ID, which is a GUID, media access control (MAC) address, or Dynamic Host Configuration Protocol (DHCP) identifier associated with the computer.

\* Example: Remove a device by using its ID from a specified domain

This command removes the pre-staged device that has the specified ID. The cmdlet searches the domain named TSQA.contoso.com for the device.

Windows PowerShell

PS C:\> Remove-WdsClient -DeviceID "5a7a1def-2e1f-4a7b-a792-ae5275b6ef92" -Domain

-DomainName "TSQA.contoso.com"

**NEW QUESTION 70**

- (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

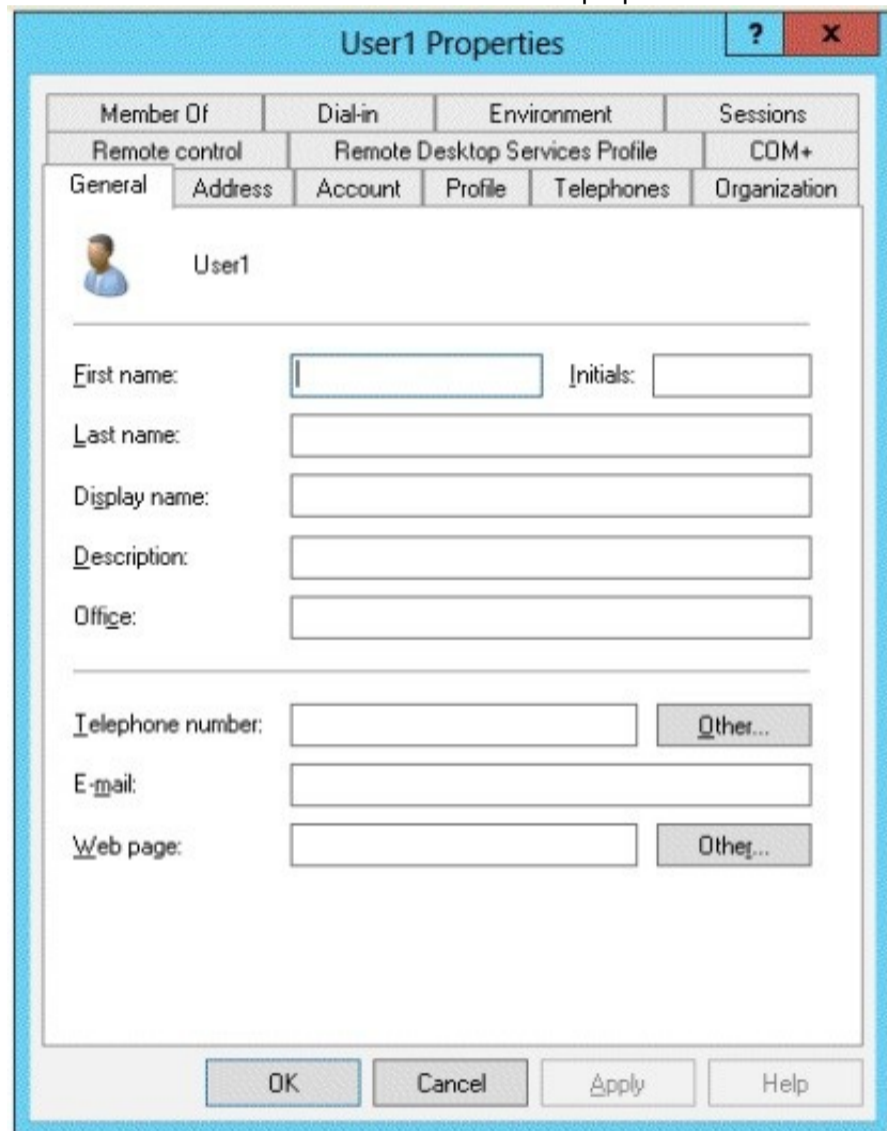
**Explanation:**

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 75**

- (Topic 2)

Your network contains an Active Directory domain named contoso.com.  
 You create a user account named User1. The properties of User1 are shown in the exhibit. (Click the Exhibit button.)



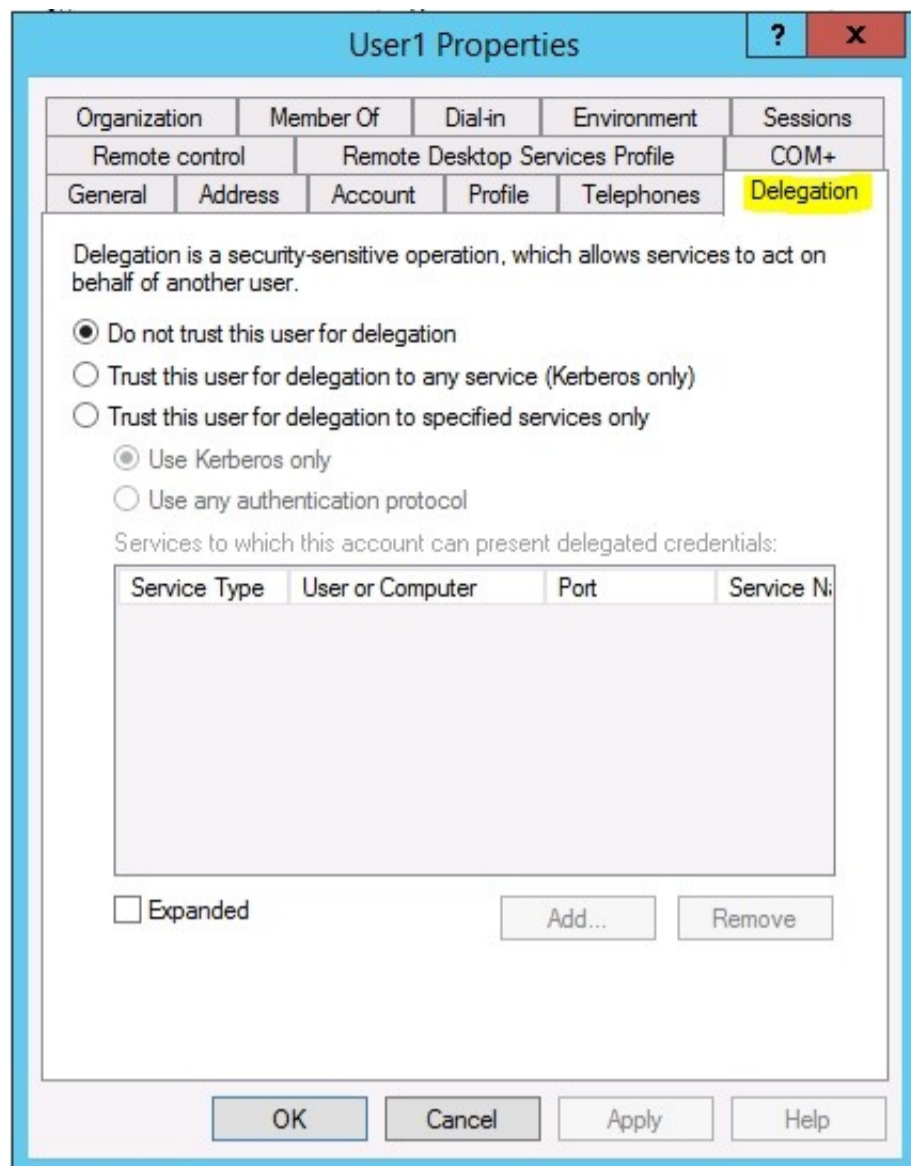
You plan to use the User1 account as a service account. The service will forward authentication requests to other servers.  
 You need to ensure that you can view the Delegation tab from the properties of the User1 account.  
 What should you do first?

- A. Configure the Name Mappings of User1.
- B. Modify the user principal name (UPN) of User1.
- C. Configure a Service Principal Name (SPN) for User1.
- D. Modify the Security settings of User1.

**Answer:** C

**Explanation:**

If you cannot see the Delegation tab, do one or both of the following:  
 Register a Service Principal Name (SPN) for the user account with the Setspn utility in the support tools on your CD. Delegation is only intended to be used by service accounts, which should have registered SPNs, as opposed to a regular user account which typically does not have SPNs.  
 Raise the functional level of your domain to Windows Server 2003. For more information, see Related Topics.



References:

<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>  
<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>  
[http://technet.microsoft.com/en-us/library/cc739474\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc739474(v=ws.10).aspx)  
<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>

#### NEW QUESTION 77

- (Topic 2)

You have a DNS server named Server1.

Server1 has a primary zone named contoso.com.

Zone Aging/Scavenging is configured for the contoso.com zone.

One month ago, an administrator removed a server named Server2 from the network.

You discover that a static resource record for Server2 is present in contoso.com. Resource records for decommissioned client computers are removed automatically from contoso.com.

You need to ensure that the static resource records for all of the servers are removed automatically from contoso.com.

What should you modify?

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

**Answer: B**

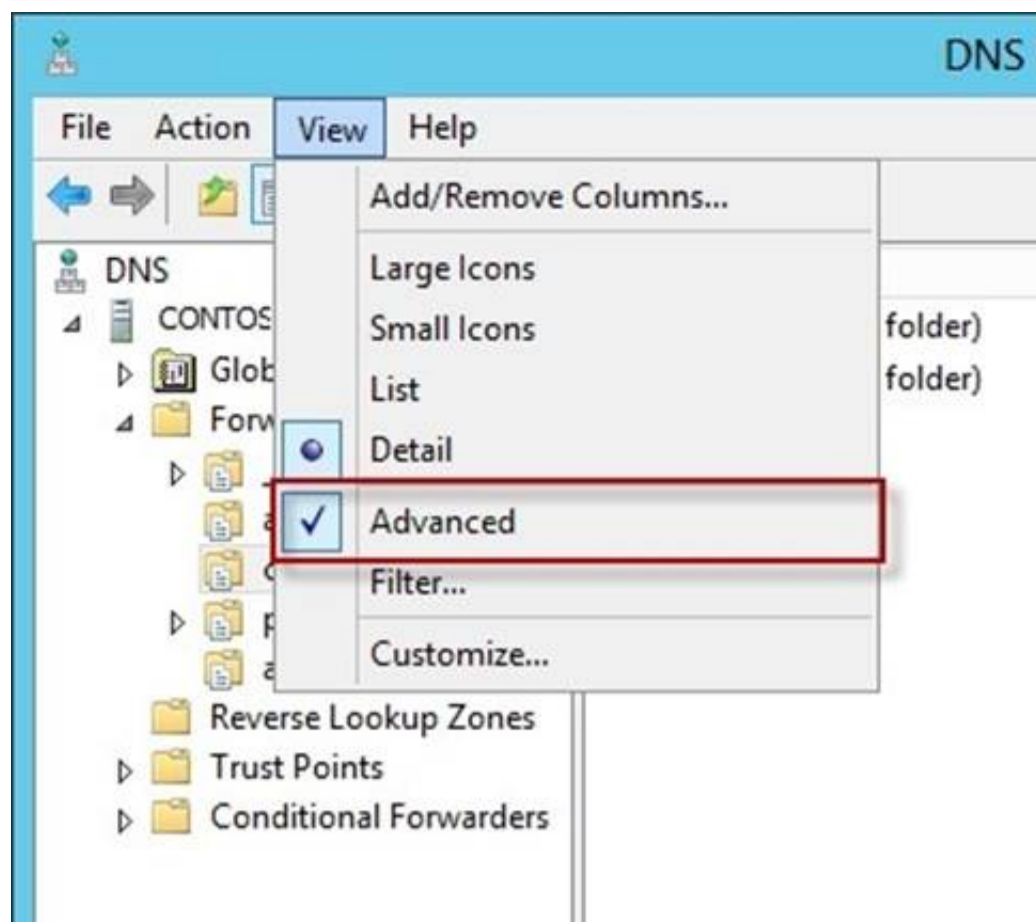
#### Explanation:

Reset and permit them to use a current (non-zero) time stamp value. This enables these records to become aged and scavenged.

You can use this procedure to change how a specific resource record is scavenged.

A stale record is a record where both the No-Refresh Interval and Refresh Interval have passed without the time stamp updating.

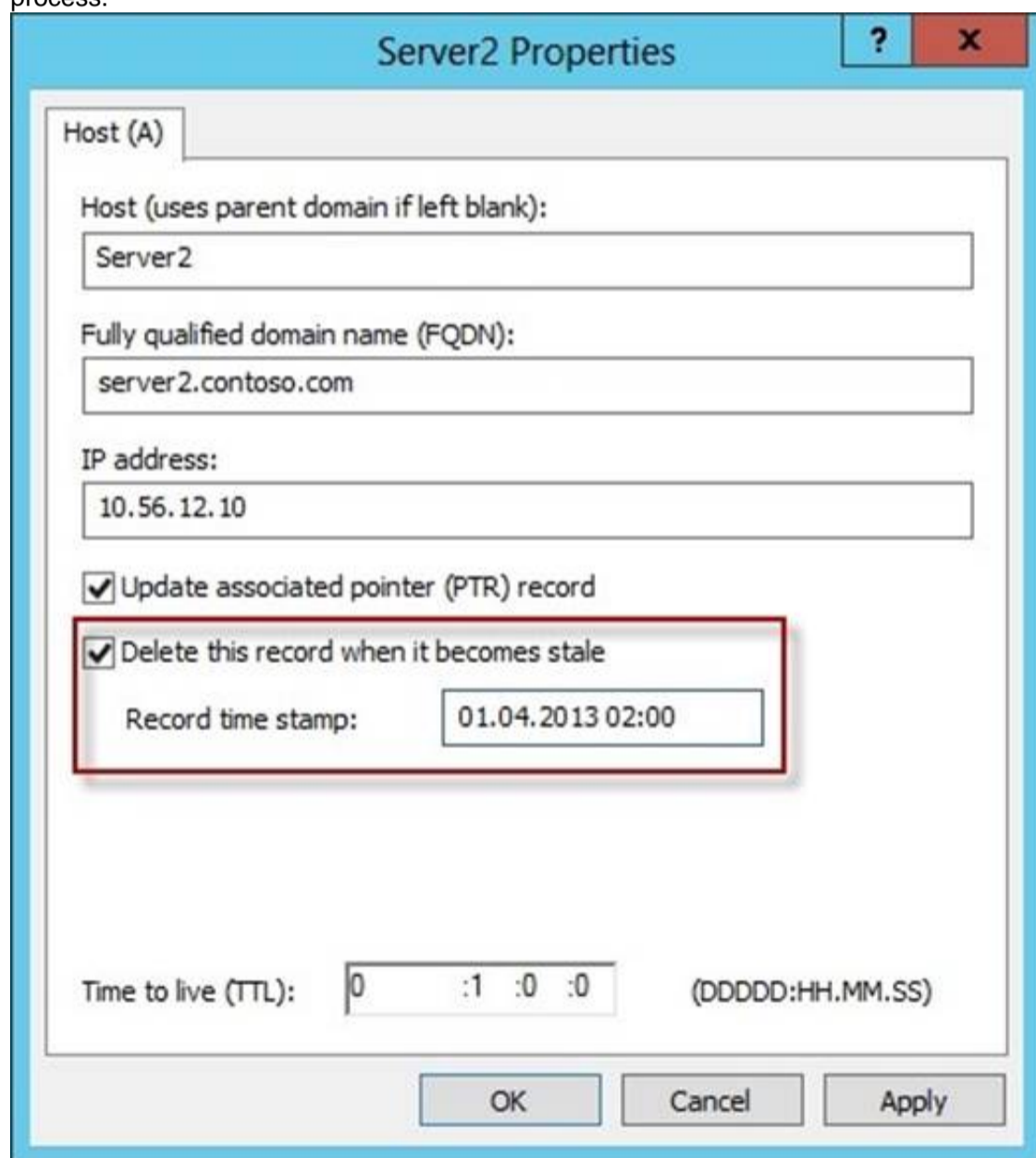
DNS->View->Advanced



Depending on the how the resource record was originally added to the zone, do one of the following:

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

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



References:

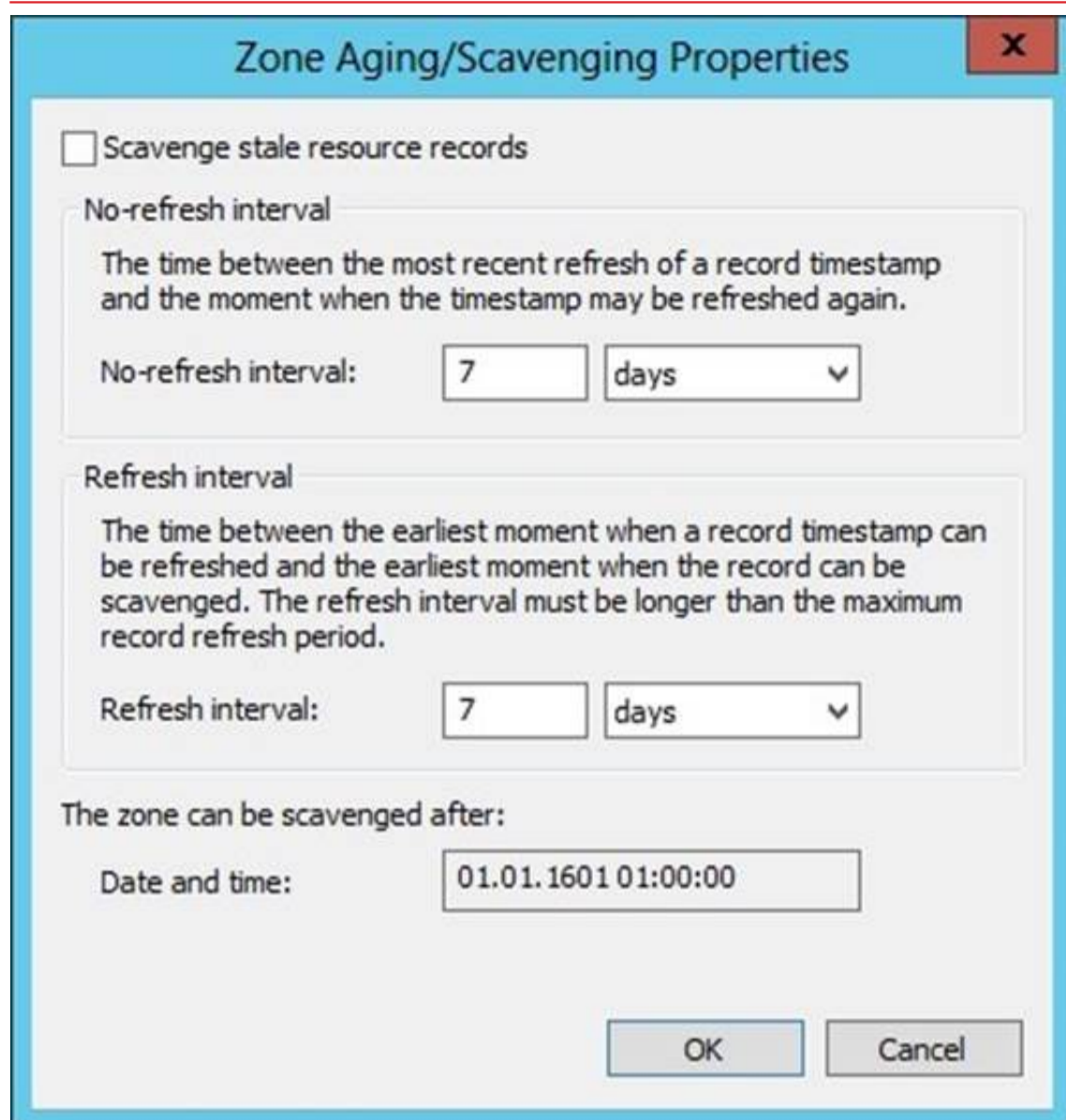
<http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx>

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

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

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

Scavenging and aging must be enabled both at the DNS server and on the zone. Scavenging is disabled by default.



**Zone Aging/Scavenging Properties**

☐ Scavenge stale resource records

**No-refresh interval**  
 The time between the most recent refresh of a record timestamp and the moment when the timestamp may be refreshed again.

No-refresh interval:

**Refresh interval**  
 The time between the earliest moment when a record timestamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period.

Refresh interval:

**The zone can be scavenged after:**

Date and time:

DNS scavenging depends on the following two settings:

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

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

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

References:

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

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

<http://technet.microsoft.com/en-us/library/cc771570.aspx>

<http://technet.microsoft.com/en-us/library/cc771677.aspx>

[http://technet.microsoft.com/en-us/library/cc758321\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc758321(v=ws.10).aspx)

## NEW QUESTION 82

- (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Server Update Services server role installed.

Server1 stores update files locally in C:\Updates.

You need to change the location in which the update files are stored to D:\Updates. What should you do?

- A. From the Update Services console, run the Windows Server Update Services Configuration Wizard.
- B. From a command prompt, run wsusutil.exe and specify the movecontent parameter.
- C. From the Update Services console, configure the Update Files and Languages option.
- D. From a command prompt, run wsusutil.exe and specify the export parameter.

**Answer: B**

### Explanation:

You might need to change the location where WSUS stores updates locally. This might be required if the disk becomes full and there is no longer any room for new updates. You might also have to do this if the disk where updates are stored fails and the replacement disk uses a new drive letter.

You accomplish this move with the movecontent command of WSUSutil.exe, a command-line tool that is copied to the file system of the WSUS server during WSUS Setup. By default, Setup copies WSUSutil.exe to the following location: WSUSInstallationDrive:\Program Files\Microsoft Windows Server Update Services\Tools\

## 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.

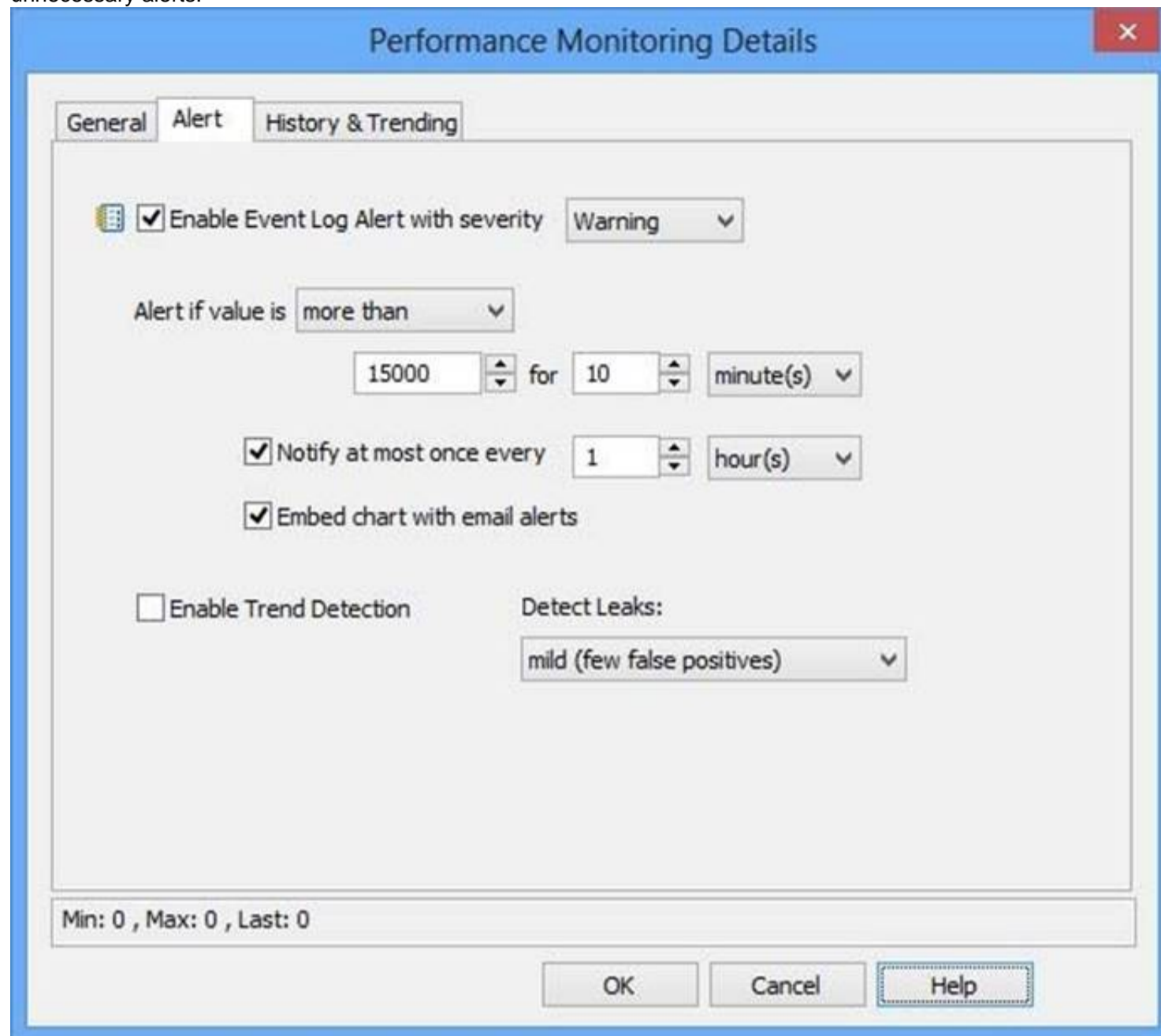
Which type of data collector should you create?

- 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.



The image shows the 'Performance Monitoring Details' dialog box with the 'Alert' tab selected. The 'General' tab is also visible. The 'Alert' tab contains the following settings:

- ☒ 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)

At the bottom, there are buttons for 'OK', 'Cancel', and 'Help'. A status bar at the bottom left shows 'Min: 0 , Max: 0 , Last: 0'.

#### NEW QUESTION 87

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

A domain controller named DC1 runs Windows Server 2012 R2. DC1 is backed up daily. During routine maintenance, you delete a group named Group1.

You need to recover Group1 and 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. Perform an authoritative restore of Group1.
- B. Mount the most recent Active Directory backup.
- C. Use the Recycle Bin to restore Group1.
- D. Reactivate the tombstone of 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.

There is another approach you should be aware of. Tombstone reanimation (which has nothing to do with zombies) provides the only way to recover deleted objects without taking a DC offline, and it's the only way to recover a deleted object's identity information, such as its objectGUID and objectSid attributes. It neatly solves the problem of recreating a deleted user or group and having to fix up all the old access control list (ACL) references, which contain the objectSid of the deleted object.

Restores domain controllers to a specific point in time, and marks objects in Active Directory as being authoritative with respect to their replication partners.

#### NEW QUESTION 89

- (Topic 2)

Your network contains a Network Policy Server (NPS) server named Server1. The network contains a server named SQL1 that has Microsoft SQL Server 2008 R2 installed. All servers run Windows Server 2012 R2.

You configure NPS on Server1 to log accounting data to a database on SQL1.

You need to ensure that the accounting data is captured if SQL1 fails. The solution must minimize cost.

What should you do?

- A. Implement Failover Clustering.
- B. Implement database mirroring.
- C. Run the Accounting Configuration Wizard.

D. Modify the SQL Server Logging properties.

**Answer: C**

**Explanation:**

In Windows Server 2008 R2, an accounting configuration wizard is added to the Accounting node in the NPS console. By using the Accounting Configuration wizard, you can configure the following four accounting settings:

- ? SQL logging only. By using this setting, you can configure a data link to a SQL Server that allows NPS to connect to and send accounting data to the SQL server. In addition, the wizard can configure the database on the SQL Server to ensure that the database is compatible with NPS SQL server logging.
- ? Text logging only. By using this setting, you can configure NPS to log accounting data to a text file.
- ? Parallel logging. By using this setting, you can configure the SQL Server data link and database. You can also configure text file logging so that NPS logs simultaneously to the text file and the SQL Server database.
- ? SQL logging with backup. By using this setting, you can configure the SQL Server data link and database. In addition, you can configure text file logging that NPS uses if SQL Server logging fails.

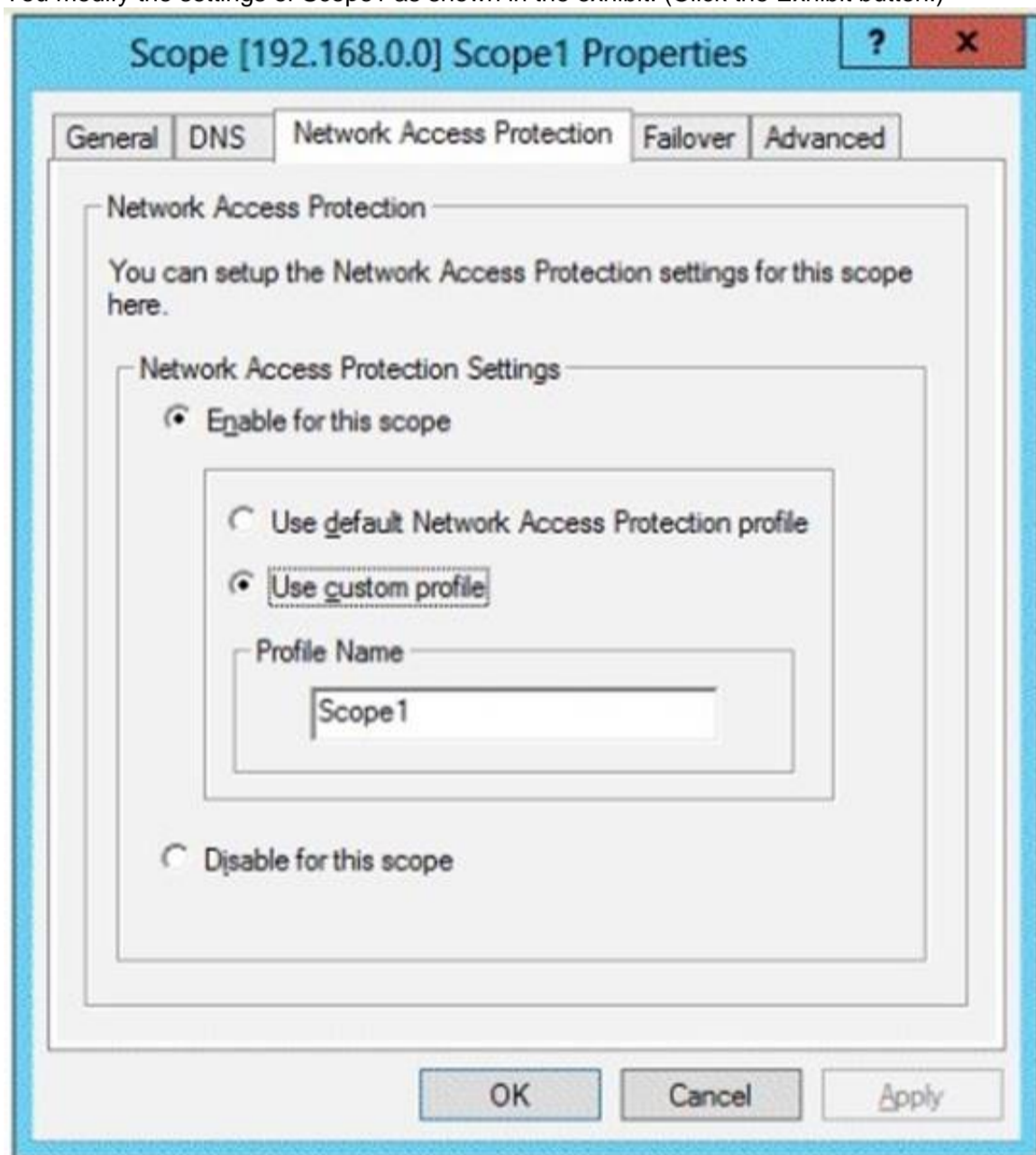
**NEW QUESTION 93**

- (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.)



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.

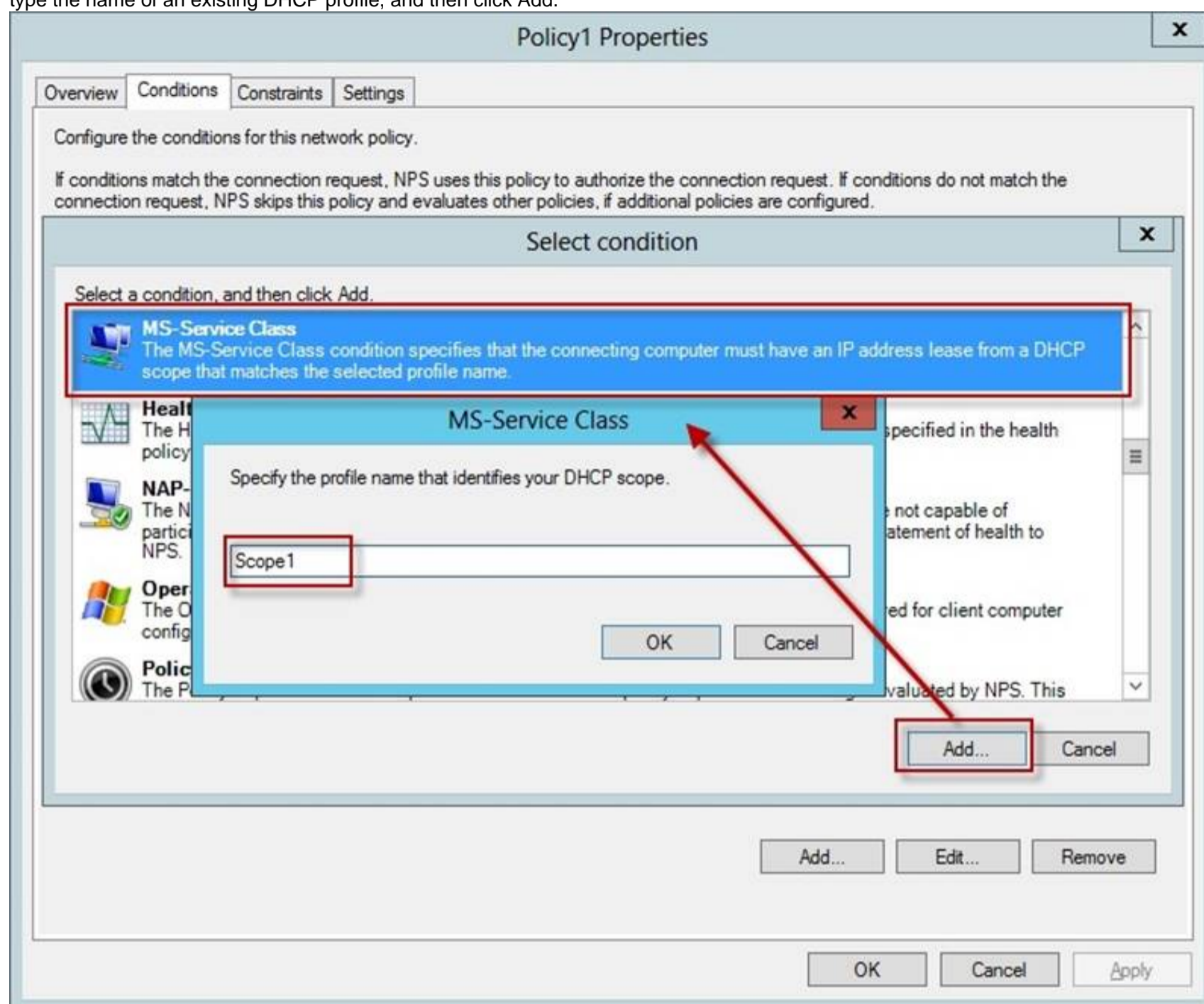
Open the NPS console, double-click Policies, click Network Policies, and then double-click the policy you want to configure.

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.



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/cc731560(v=ws.10).aspx)  
[http://technet.microsoft.com/en-us/library/cc731220\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731220(v=ws.10).aspx)

#### NEW QUESTION 94

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2. All client computers run Windows 7.

You need to ensure that user settings are saved to \\Server1\Users\. What should you do?

- A. From the properties of each user account, configure the Home folder settings.
- B. From a Group Policy object (GPO), configure the Folder Redirection settings.
- C. From the properties of each user account, configure the User profile settings.
- D. From a Group Policy object (GPO), configure the Drive Maps preference.

**Answer: C**

**Explanation:**

If a computer is running Windows 2000 Server or later on a network, users can store their profiles on the server. These profiles are called roaming user profiles.

#### NEW QUESTION 96

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. You have a standard primary zone named adatum.com.

You need to provide a user named User1 the ability to modify records in the zone. Other users must be prevented from modifying records in the zone. What should you do first?

- A. Run the Zone Signing Wizard for the zone.
- B. From the properties of the zone, modify the start of authority (SOA) record.
- C. From the properties of the zone, change the zone type.
- D. Run the New Delegation Wizard for the zone.

**Answer: C**

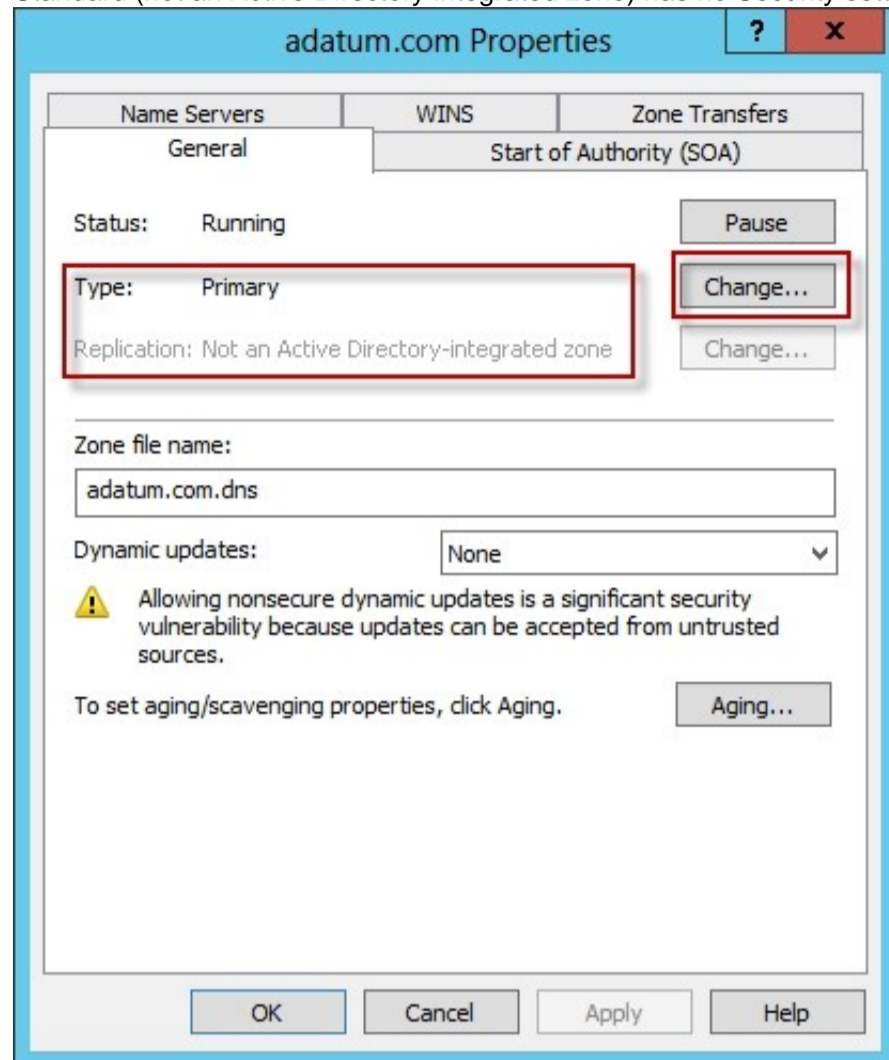
**Explanation:**

The Zone would need to be changed to a AD integrated zone When you use directory- integrated zones, you can use access control list (ACL) editing to secure a dnsZone object container in the directory tree. This feature provides detailed access to either the zone or a specified resource record in the zone. For example, an

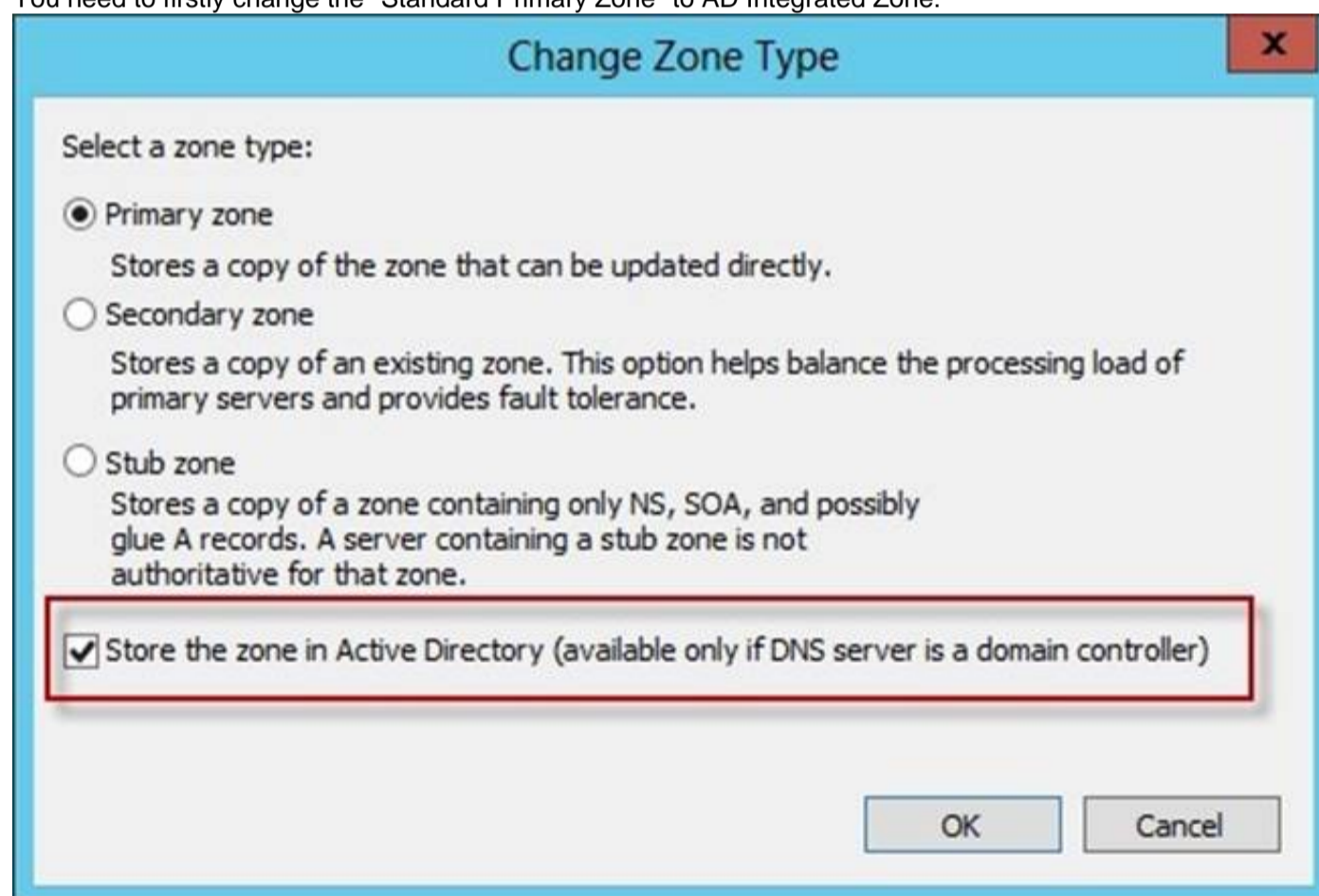
ACL for a zone resource record can be restricted so that dynamic updates are allowed only for a specified client computer or a secure group, such as a domain administrators group. This security feature is not available with standard primary zones.

DNS update security is available only for zones that are integrated into Active Directory. After you integrate a zone, you can use the access control list (ACL) editing features that are available in the DNS snap-in to add or to remove users or groups from the ACL for a specific zone or for a resource record.

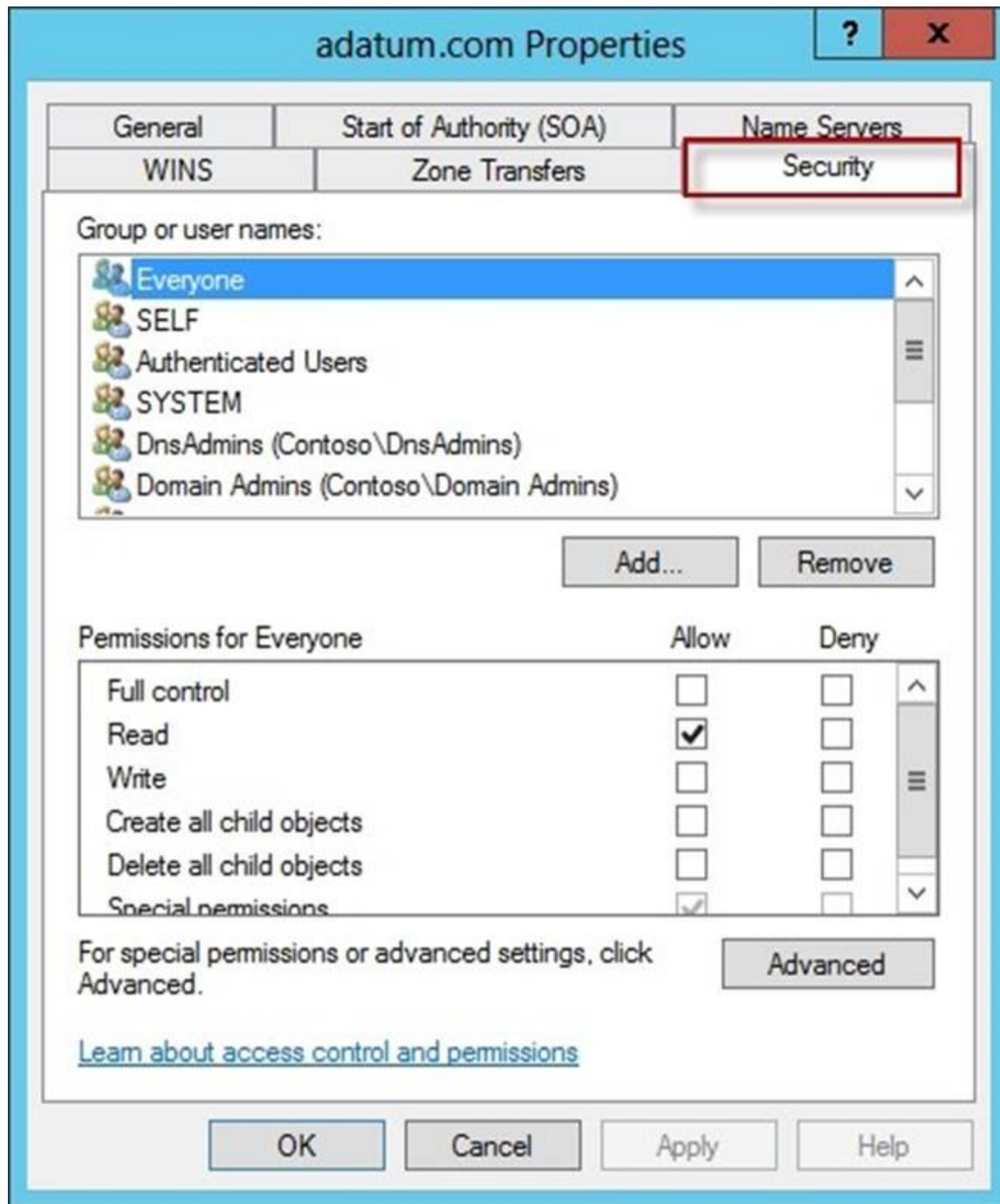
Standard (not an Active Directory integrated zone) has no Security settings:



You need to firstly change the "Standard Primary Zone" to AD Integrated Zone:



Now there's Security tab:



References:

<http://technet.microsoft.com/en-us/library/cc753014.aspx> <http://technet.microsoft.com/en-us/library/cc726034.aspx> <http://support.microsoft.com/kb/816101>

#### NEW QUESTION 99

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. The domain contains 10 domain controllers that run Windows Server 2012 R2.

You plan to create a new Active Directory-integrated zone named contoso.com. You need to ensure that the new zone will be replicated to only four of the domain controllers.

What should you do first?

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

**Answer: A**

#### Explanation:

Application directory partitions

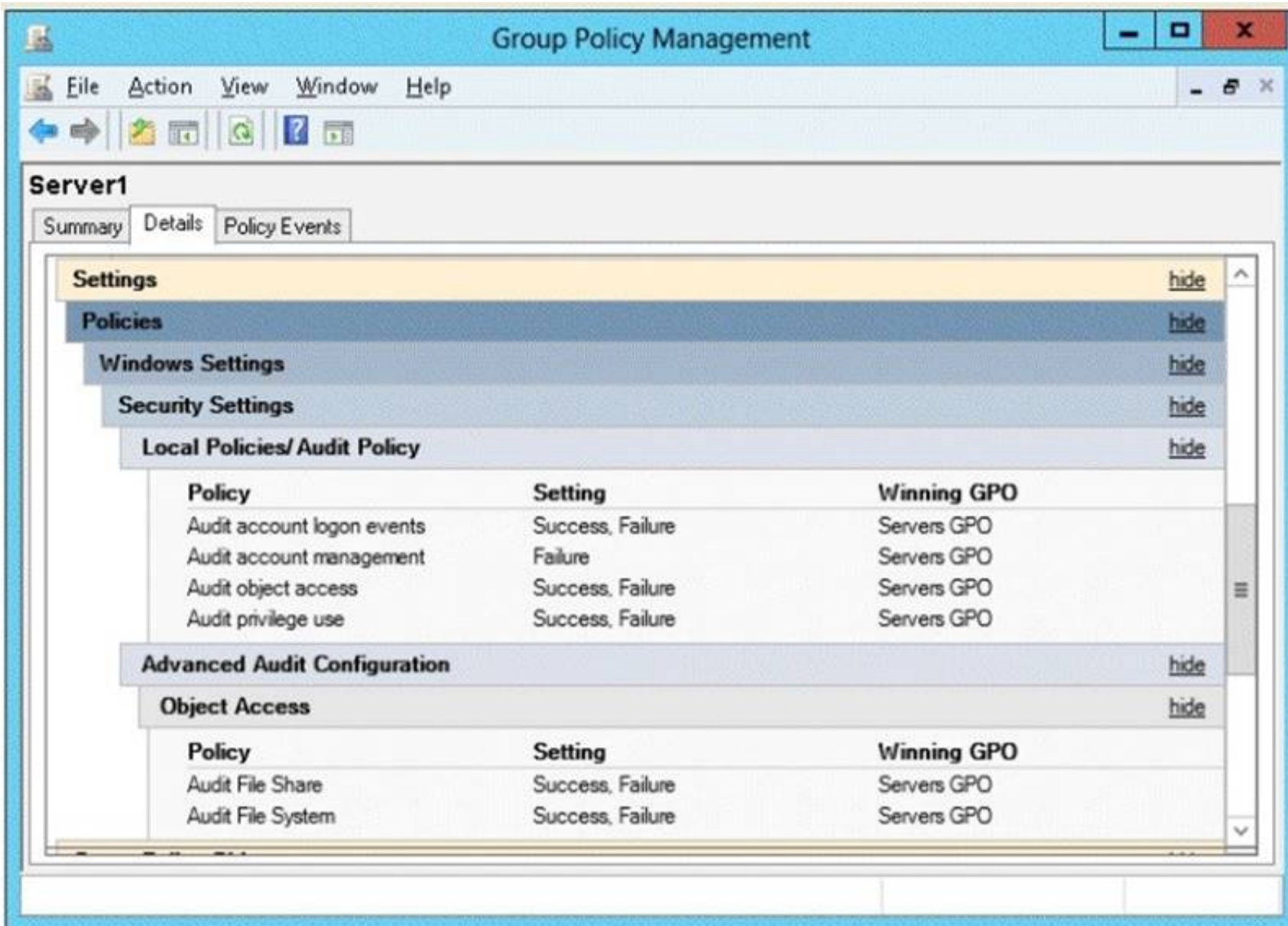
An application directory partition is a directory partition that is replicated only to specific domain controllers. A domain controller that participates in the replication of a particular application directory partition hosts a replica of that partition. Only domain controllers running Windows Server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

#### NEW QUESTION 104

- (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.)



You need to ensure that an entry is added to the event log whenever a local user account is created or deleted on Server1. What should you do?

- A. In Servers GPO, modify the Advanced Audit Configuration settings.
- B. On Server1, attach a task to the security log.
- C. In Servers GPO, modify the Audit Policy settings.
- D. On Server1, attach a task to the system log.

**Answer: A**

**Explanation:**

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. The following procedure shows how to prevent conflicts by blocking the application of any basic audit policy settings.

**Enabling Advanced Audit Policy Configuration**

Basic and advanced audit policy configurations should not be mixed. As such, it's best practice to enable Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings in Group Policy to make sure that basic auditing is disabled. The setting can be found under Computer Configuration\Policies\Security Settings\Local Policies\Security Options, and sets the SCENoApplyLegacyAuditPolicy registry key to prevent basic auditing being applied using Group Policy and the Local Security Policy MMC snap-in.

In Windows 7 and Windows Server 2008 R2, the number of audit settings for which success and failure can be tracked has increased to 53. Previously, there were nine basic auditing settings under Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy. These 53 new settings allow you to select only the behaviors that you want to monitor and exclude audit results for behaviors that are of little or no concern to you, or behaviors that create an excessive number of log entries. In addition, because Windows 7 and Windows Server 2008 R2 security audit policy can be applied by using domain Group Policy, audit policy settings can be modified, tested, and deployed to selected users and groups with relative simplicity.

**Audit Policy settings**

Any changes to user account and resource permissions. Any failed attempts for user logon.

Any failed attempts for resource access. Any modification to the system files.

**Advanced Audit Configuration Settings**

Audit compliance with important business-related and security-related rules by tracking precisely defined activities, such as:

? A group administrator has modified settings or data on servers that contain finance information.

? An employee within a defined group has accessed an important file.

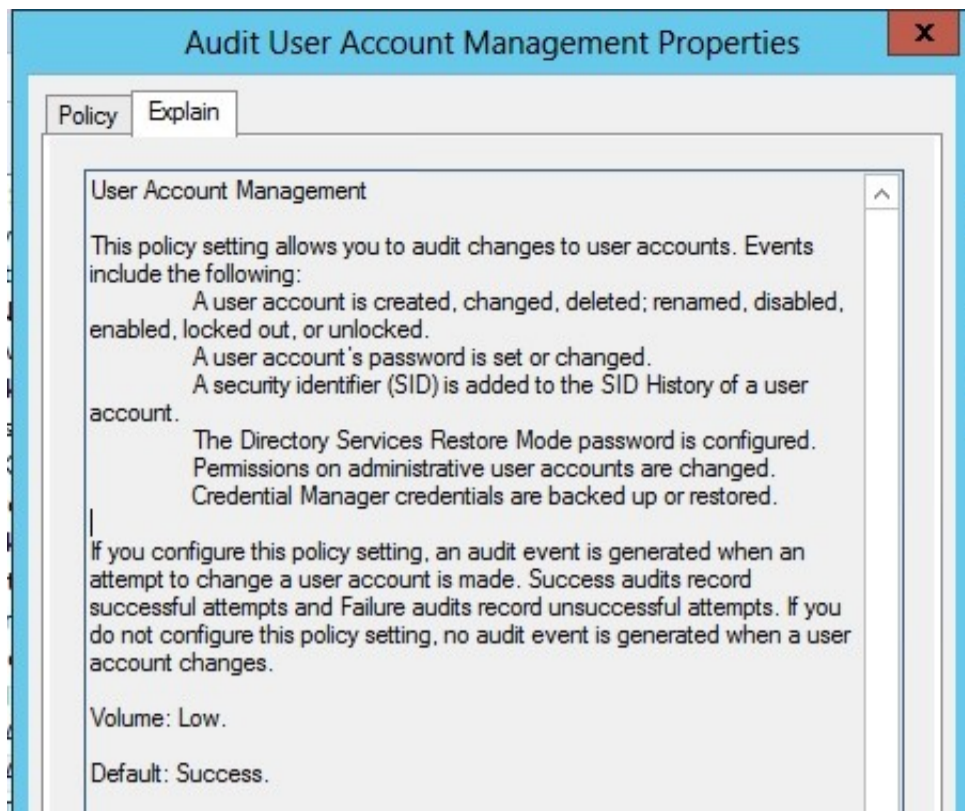
? The correct system access control list (SACL) is applied to every file and folder or registry key on a computer or file share as a verifiable safeguard against undetected access.

In Servers GPO, modify the Audit Policy settings - enabling audit account management setting will generate events about account creation, deletion and so on.

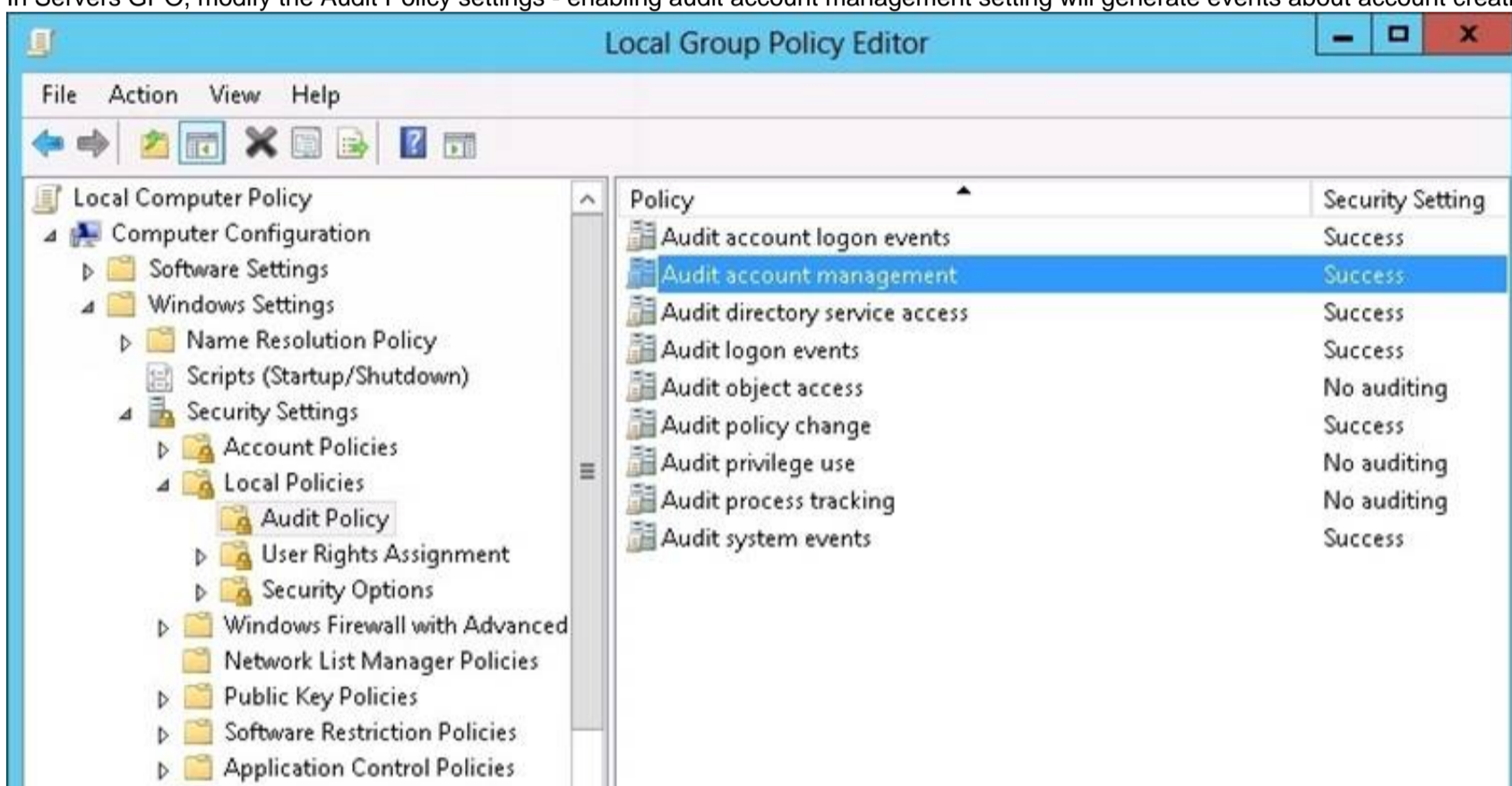
**Advanced Audit Configuration Settings**

Advanced Audit Configuration Settings -> Audit Policy

-> Account Management -> Audit User Account Management



In Servers GPO, modify the Audit Policy settings - enabling audit account management setting will generate events about account creation, deletion and so on.



ence:

<http://blogs.technet.com/b/abizerh/archive/2010/05/27/tracing-down-user-and-computer-account-deletion-in-active-directory.aspx>

<http://technet.microsoft.com/en-us/library/dd772623%28v=ws.10%29.aspx>

[http://technet.microsoft.com/en-us/library/jj852202\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/jj852202(v=ws.10).aspx)

<http://www.petri.co.il/enable-advanced-audit-policy-configuration-windows-server.htm>

<http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx>

[http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx#BKMK\\_step2](http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx#BKMK_step2)

## NEW QUESTION 108

### HOTSPOT - (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains 30 user accounts that are used for network administration. The user accounts are members of a domain global group named Group1.

You identify the security requirements for the 30 user accounts as shown in the following table.

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

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

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

## Answer Area

Security setting	Configured by using
Minimum password length	<input type="text"/>
Account is sensitive and cannot be delegated	<input type="text"/>
User cannot change password	<input type="text"/>
Password never expires	<input type="text"/>

Security setting	Configured by using
Minimum password length	<input type="text"/> <div> PSO  User account properties </div>
Account is sensitive and cannot be delegated	<input type="text"/> <div> PSO  User account properties </div>
User cannot change password	<input type="text"/> <div> PSO  User account properties </div>
Enforce password history	<input type="text"/> <div> PSO  User account properties </div>

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

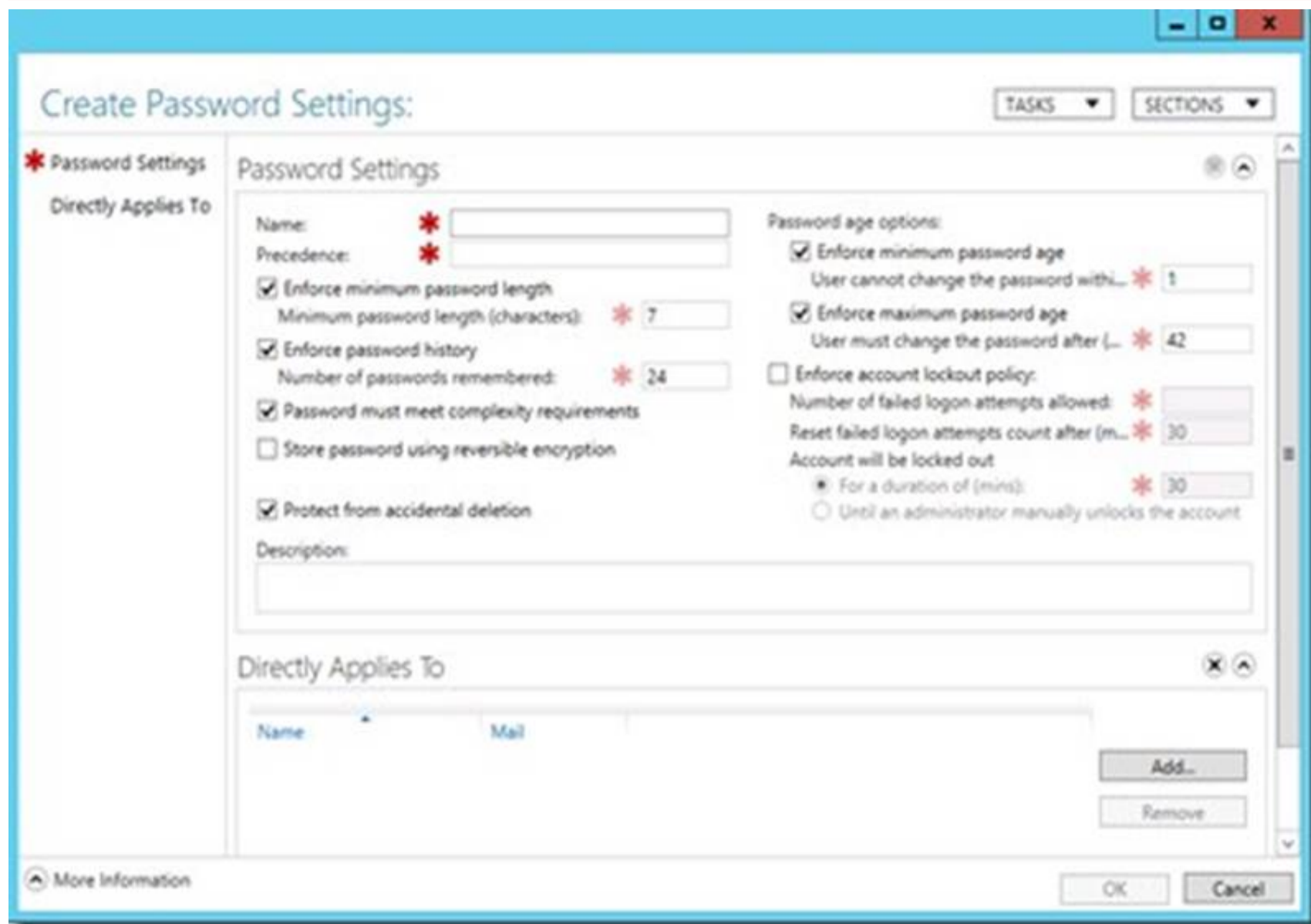
Box 1: PSO

Box 2: User Account Properties Box 3: User Account Properties Box 4: PSO

Note:

\* Password Setting Object (PSO) is another name for Fine Grain Password Policies.

\* Here you can see all the settings that go into a PSO.



#### NEW QUESTION 109

- (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. You discover that the performance of Server1 is poor. The results of a performance report generated on Server1 are shown in the following table.

Counter	Value
Processor(_Total)\% DPC Time	35
Processor(_Total)\% Interrupt Time	51
Processor(_Total)\% User Time	12
Processor(_Total)\% Privileged Time	2
Processor Information(_Total)\% Processor Time	100
Memory\Available Bytes	7,341,024,329
Memory\Pages/sec	125

You need to identify the cause of the performance issue. What should you identify?

- A. Driver malfunction
- B. Insufficient RAM
- C. Excessive paging
- D. NUMA fragmentation

**Answer: A**

#### Explanation:

Processor: %DPC Time. Much like the other values, this counter shows the amount of time that the processor spends servicing DPC requests. DPC requests are more often than not associated with the network interface.

Processor: % Interrupt Time. This is the percentage of time that the processor is spending on handling Interrupts. Generally, if this value exceeds 50% of the processor time you may have a hardware issue. Some components on the computer can force this issue and not really be a problem. For example a programmable I/O card like an old disk controller card, can take up to 40% of the CPU time. A NIC on a busy IIS server can likewise generate a large percentage of processor activity.

Processor: % User Time. The value of this counter helps to determine the kind of processing that is affecting the system. Of course the resulting value is the total amount of non-idle time that was spent on User mode operations. This generally means application code.

Processor: %Privilege Time. This is the amount of time the processor was busy with Kernel mode operations. If the processor is very busy and this mode is high, it is usually an indication of some type of NT service having difficulty, although user mode programs can make calls to the Kernel mode NT components to occasionally cause this type of performance issue.

Memory: Pages/sec. This value is often confused with Page Faults/sec. The Pages/sec counter is a combination of Pages Input/sec and Pages Output/sec counters. Recall that Page Faults/sec is a combination of hard page faults and soft page faults. This counter, however, is a general indicator of how often the system is using the hard drive to store or retrieve memory associated data.

References:  
<http://technet.microsoft.com/en-us/library/cc768048.aspx>

### NEW QUESTION 111

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

An organizational unit (OU) named OU1 contains 200 client computers that run Windows 8 Enterprise. A Group Policy object (GPO) named GPO1 is linked to OU1.

You make a change to GPO1.

You need to force all of the computers in OU1 to refresh their Group Policy settings immediately. The solution must minimize administrative effort.

Which tool should you use?

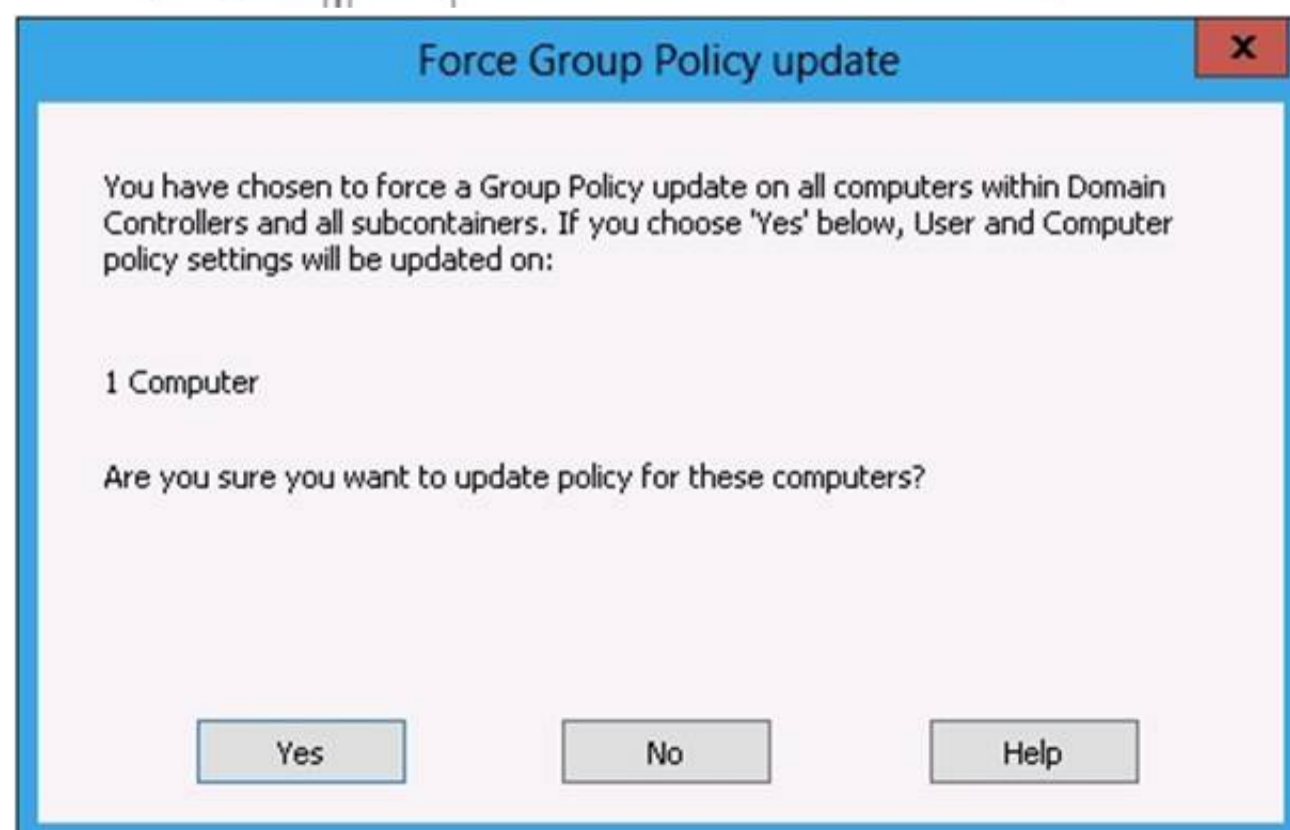
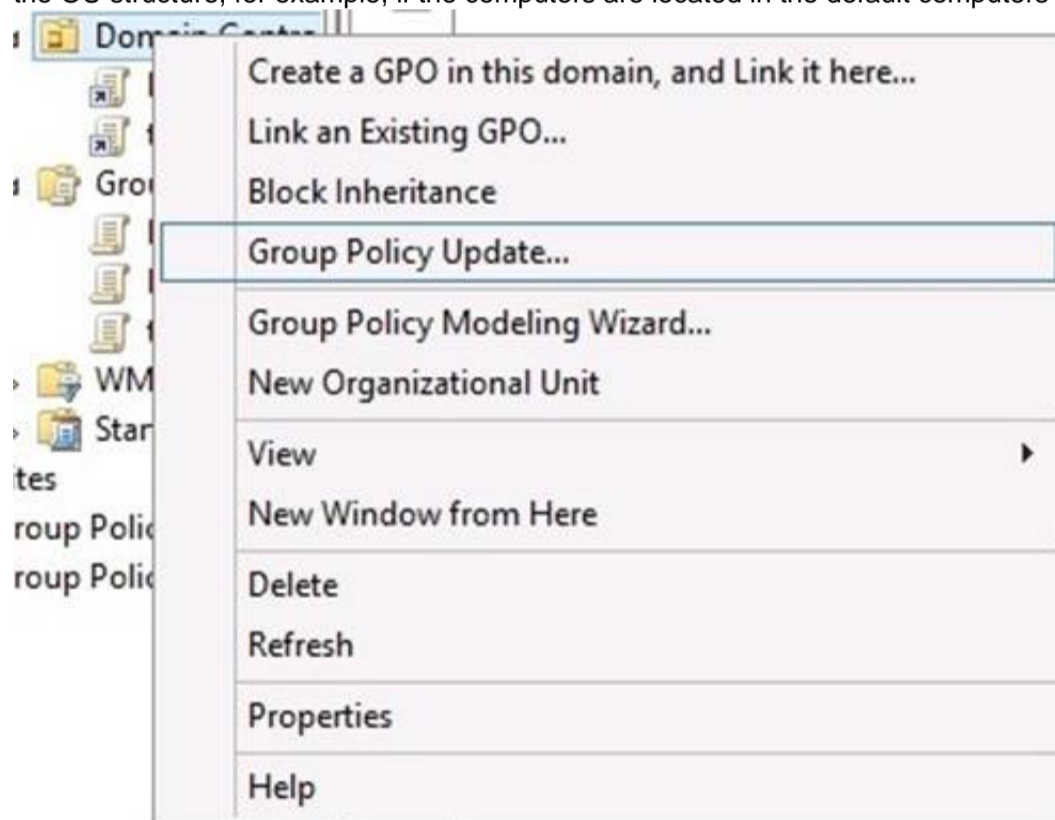
- A. The Secedit command
- B. Group Policy Management Console (GPMC)
- C. Server Manager
- D. The Gpupdate command

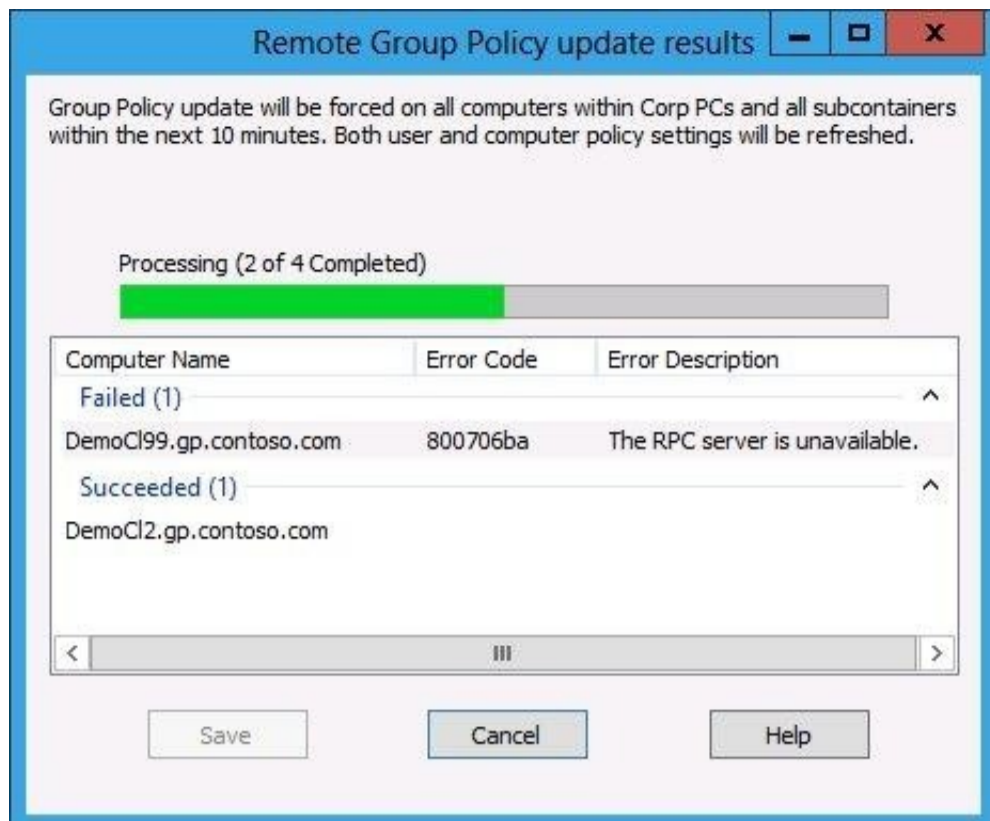
**Answer: B**

### Explanation:

In the previous versions of Windows, this was accomplished by having the user run GpUpdate.exe on their computer.

Starting with Windows Server® 2012 and Windows® 8, you can now remotely refresh Group Policy settings for all computers in an OU from one central location through the Group Policy Management Console (GPMC). Or you can use the Invoke-GPUdatecmdlet to refresh Group Policy for a set of computers, not limited to the OU structure, for example, if the computers are located in the default computers container.





<http://technet.microsoft.com/en-us/library/jj134201.aspx>

<http://blogs.technet.com/b/grouppolicy/archive/2012/11/27/group-policy-in-windows-server-2012-using-remote-gpupdate.aspx>

### NEW QUESTION 112

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named IT and an OU named Sales. All of the help desk user accounts are located in the IT OU. All of the sales user accounts are located in the Sales OU. The Sales OU contains a global security group named G\_Sales. The IT OU contains a global security group named G\_HelpDesk.

You need to ensure that members of G\_HelpDesk can perform the following tasks:

? Reset the passwords of the sales users.

? Force the sales users to change their password at their next logon.

What should you do?

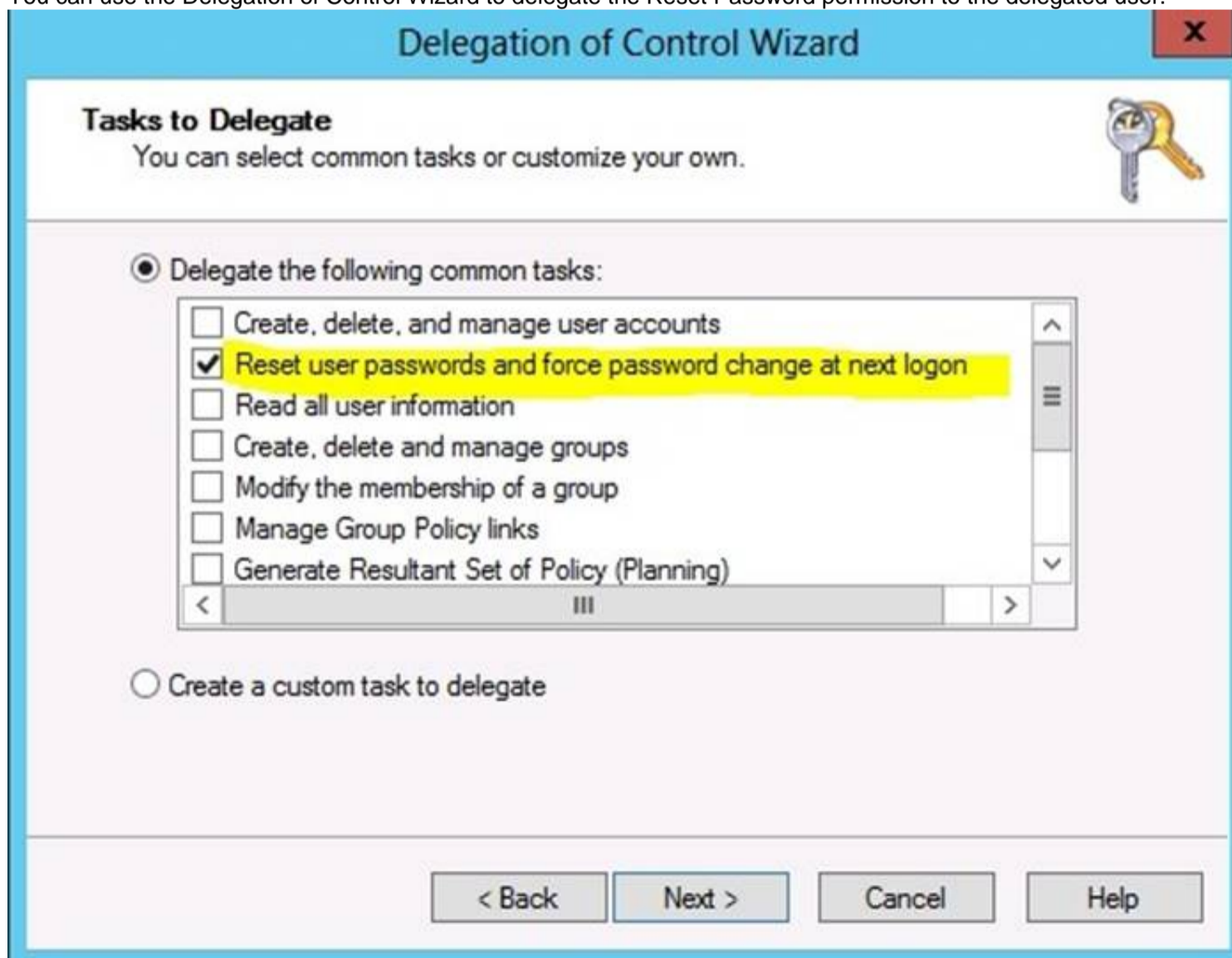
- A. Run the Set-ADAccountPasswordcmdlet and specify the -identity parameter.
- B. Right-click the Sales OU and select Delegate Control.
- C. Right-click the IT OU and select Delegate Control.
- D. Run the Set-ADFineGrainedPasswordPolicycmdlet and specify the -identity parameter.

**Answer: B**

### Explanation:

G\_HelpDesk members need to be allowed to delegate control on the Sales OU as it contains the sales users (G\_Sales)

You can use the Delegation of Control Wizard to delegate the Reset Password permission to the delegated user.



References:

<http://support.microsoft.com/kb/296999/en-us>

<http://support.microsoft.com/kb/296999/en-us>  
<http://technet.microsoft.com/en-us/library/cc732524.aspx>

#### NEW QUESTION 114

DRAG DROP - (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed.

All of the VPN servers on your network use Server1 for RADIUS authentication. You create a security group named Group1.

You need to configure Network Policy and Access Services (NPAS) to meet the following requirements:

? Ensure that only the members of Group1 can establish a VPN connection to the VPN servers.

? Allow only the members of Group1 to establish a VPN connection to the VPN

servers if the members are using client computers that run Windows 8 or later. Which type of policy should you create for each requirement?

To answer, drag the appropriate policy types to the correct requirements. Each policy type 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.

Policy Types	Answer Area
Connection Request Policies	Ensure that only the members of Group1 can establish a VPN connection to the VPN servers. <span>Policy type</span>
Health Policies	
Network Policies	Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later. <span>Policy type</span>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Policy Types	Answer Area
Connection Request Policies	Ensure that only the members of Group1 can establish a VPN connection to the VPN servers. <span>Network Policies</span>
Health Policies	
Network Policies	Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later. <span>Network Policies</span>

#### NEW QUESTION 117

- (Topic 2)

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	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. What should you do?

- A. Transfer the schema master to DC6.
- B. Transfer the PDC emulator to DC5.
- C. Transfer the schema master to DC4.
- D. Transfer the PDC emulator to DC2.

**Answer: D**

**Explanation:**

A deployed Windows Server 2012 domain controller (virtualized or physical) that hosts the PDC emulator role (DC1). To verify whether the PDC emulator role is hosted on a Windows Server 2012 domain controller, run the following Windows PowerShell command:  
Get-ADComputer (Get-ADDomainController –Discover –Service "PrimaryDC").name  
–Propertyoperatingsystemversion|fl  
Reference: [http://technet.microsoft.com/en-us/library/hh831734.aspx#steps\\_deploy\\_vdc](http://technet.microsoft.com/en-us/library/hh831734.aspx#steps_deploy_vdc)

**NEW QUESTION 119**

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 120**

- (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 122

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.

Server1 and Server2 are nodes in a Hyper-V cluster named Cluster1. Cluster1 hosts 10 virtual machines. All of the virtual machines run Windows Server 2012 R2 and are members of the domain.

You need to ensure that the first time a service named Service1 fails on a virtual machine, the virtual machine is moved to a different node.

You configure Service1 to be monitored from Failover Cluster Manager. What should you configure on the virtual machine?

- A. From the General settings, modify the Startup type.
- B. From the General settings, modify the Service status.
- C. From the Recovery settings of Service1, set the First failure recovery action to Take No Action.
- D. From the Recovery settings of Service1, set the First failure recovery action to Restart the Service.

**Answer: C**

### Explanation:

Configure the virtual machine to take no action through Hyper-V if the physical computer shuts down by modifying the Automatic Stop Action setting to None.

Virtual machine state must be managed through the Failover Clustering feature.

Virtual machine application monitoring and management

In clusters running Windows Server 2012, administrators can monitor services on clustered virtual machines that are also running Windows Server 2012. This functionality extends the high-level monitoring of virtual machines that is implemented in Windows Server 2008 R2 failover clusters. If a monitored service in a virtual machine fails, the service can be restarted, or the clustered virtual machine can be restarted or moved to another node (depending on service restart settings and cluster failover settings).

This feature increases the uptime of high availability services that are running on virtual machines within a failover cluster.

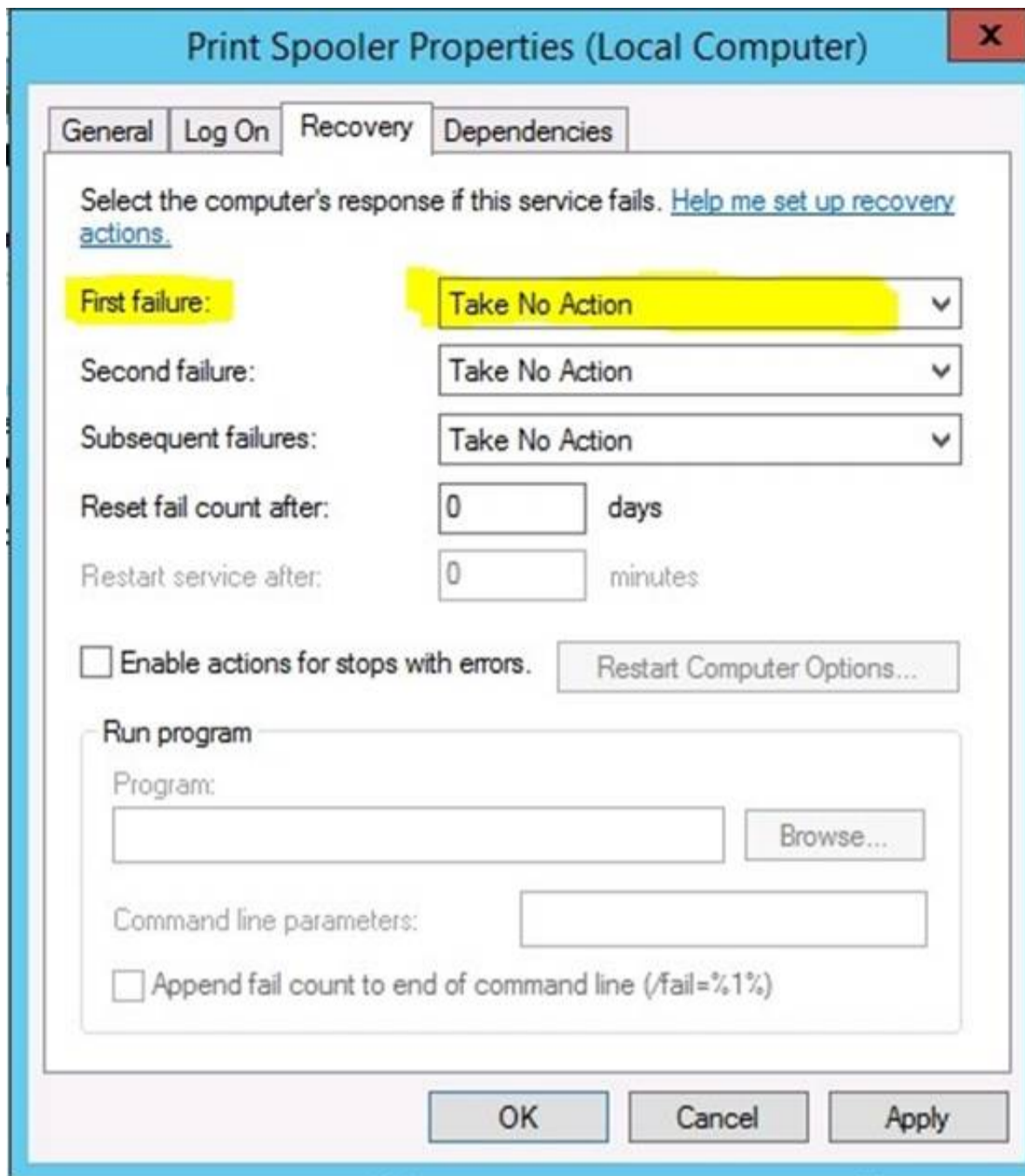
Windows Server 2012 Failover Cluster introduces a new capability for Hyper-V virtual machines (VMs), which is a basic monitoring of a service within the VM which causes the VM to be rebooted should the monitored service fail three times. For this feature to work the following must be configured:

? Both the Hyper-V servers must be Windows Server 2012 and the guest OS running in the VM must be Windows Server 2012.

? The host and guest OSs are in the same or at least trusting domains.

? The Failover Cluster administrator must be a member of the local administrator's group inside the VM.

Ensure the service being monitored is set to Take No Action (see screen shot below) within the guest VM for Subsequent failures (which is used after the first and second failures) and is set via the Recovery tab of the service properties within the Services application (services.msc).



**Print Spooler Properties (Local Computer)**

General Log On **Recovery** Dependencies

Select the computer's response if this service fails. [Help me set up recovery actions.](#)

First failure: Take No Action

Second failure: Take No Action

Subsequent failures: Take No Action

Reset fail count after: 0 days

Restart service after: 0 minutes

☐ Enable actions for stops with errors. Restart Computer Options...

Run program

Program:  Browse...

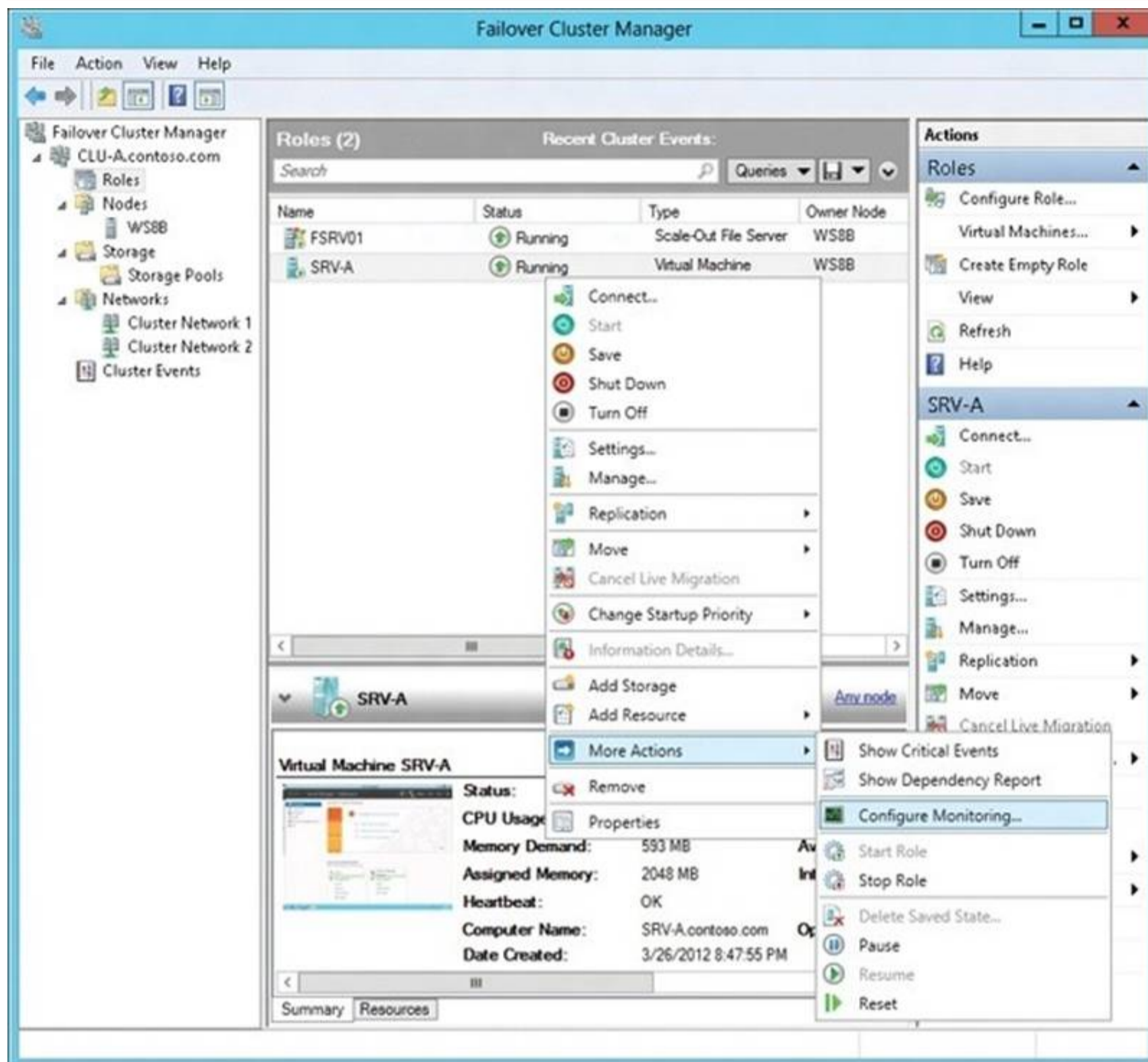
Command line parameters:

☐ Append fail count to end of command line (/fail=%1%)

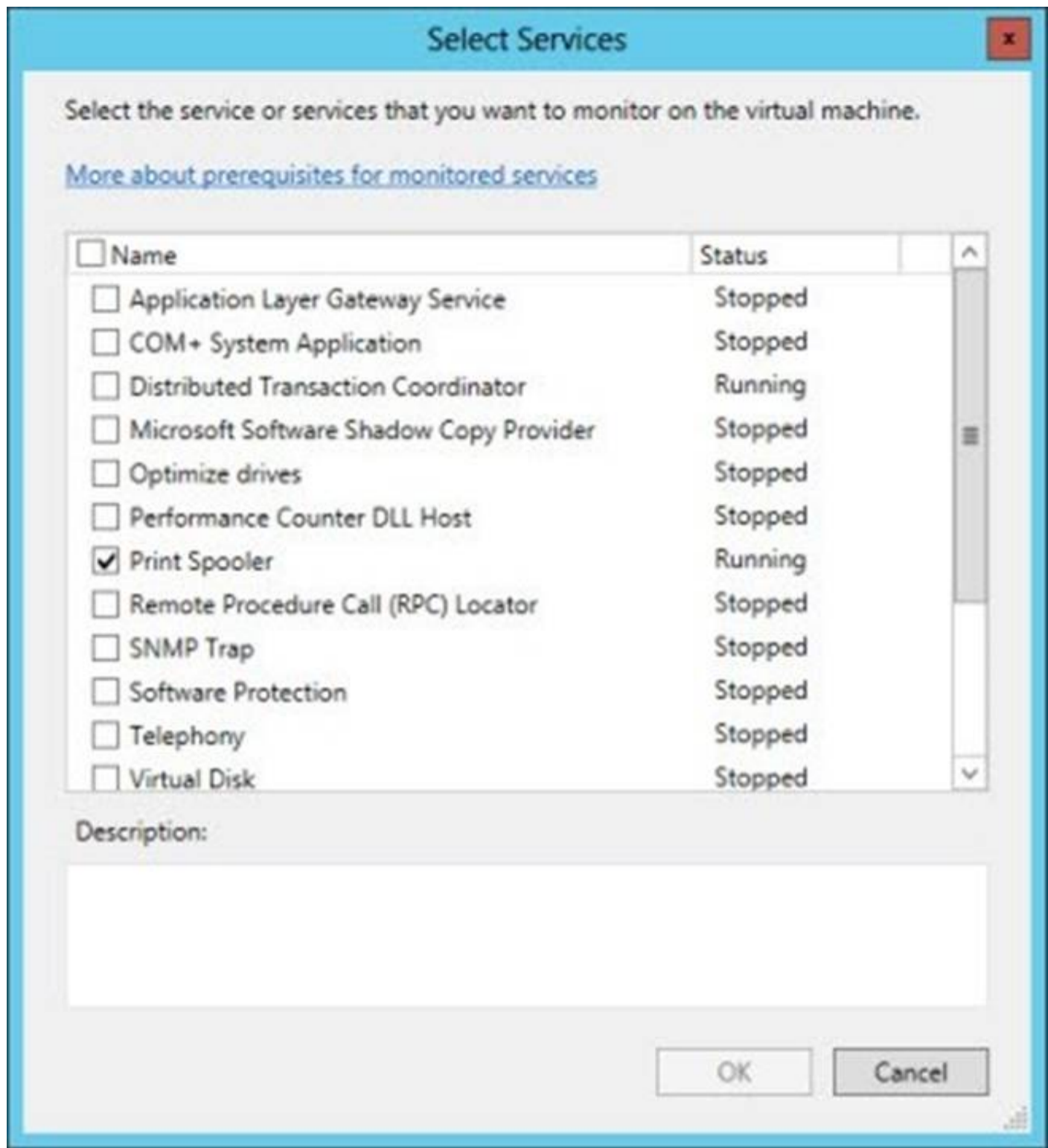
OK Cancel Apply

Within the guest VM, ensure the Virtual Machine Monitoring firewall exception is enabled for the Domain network by using the Windows Firewall with Advanced Security application or by using the Windows PowerShell command below: `Set-NetFirewallRule -DisplayGroup "Virtual Machine Monitoring" -Enabled True`. After the above is true, enabling the monitoring is a simple process:

- ? Launch the Failover Cluster Manager tool.
- ? Navigate to the cluster - Roles.
- ? Right click on the virtual machine role you wish to enable monitoring for and under More Actions select Configure Monitoring.



? The services running inside the VM will be gathered and check the box for the services that should be monitored and click OK.



You are done!

Monitoring can also be enabled using the Add-ClusterVMMonitoredItemcmdlet and - VirtualMachine, with the -Service parameters, as the example below shows:

PS C:\Windows\system32> Add-ClusterVMMonitoredItem -VirtualMachine savdaltst01 - Service spooler

References:

<http://sportstoday.us/technology/windows-server-2012---continuous-availability-%28part-4%29---failover-clustering-enhancements---virtual-machine-monitoring-.aspx>

<http://windowsitpro.com/windows-server-2012/enable-windows-server-2012-failover-cluster-hyper-v-vm-monitoring>

<http://technet.microsoft.com/en-us/library/cc742396.aspx>

### NEW QUESTION 123

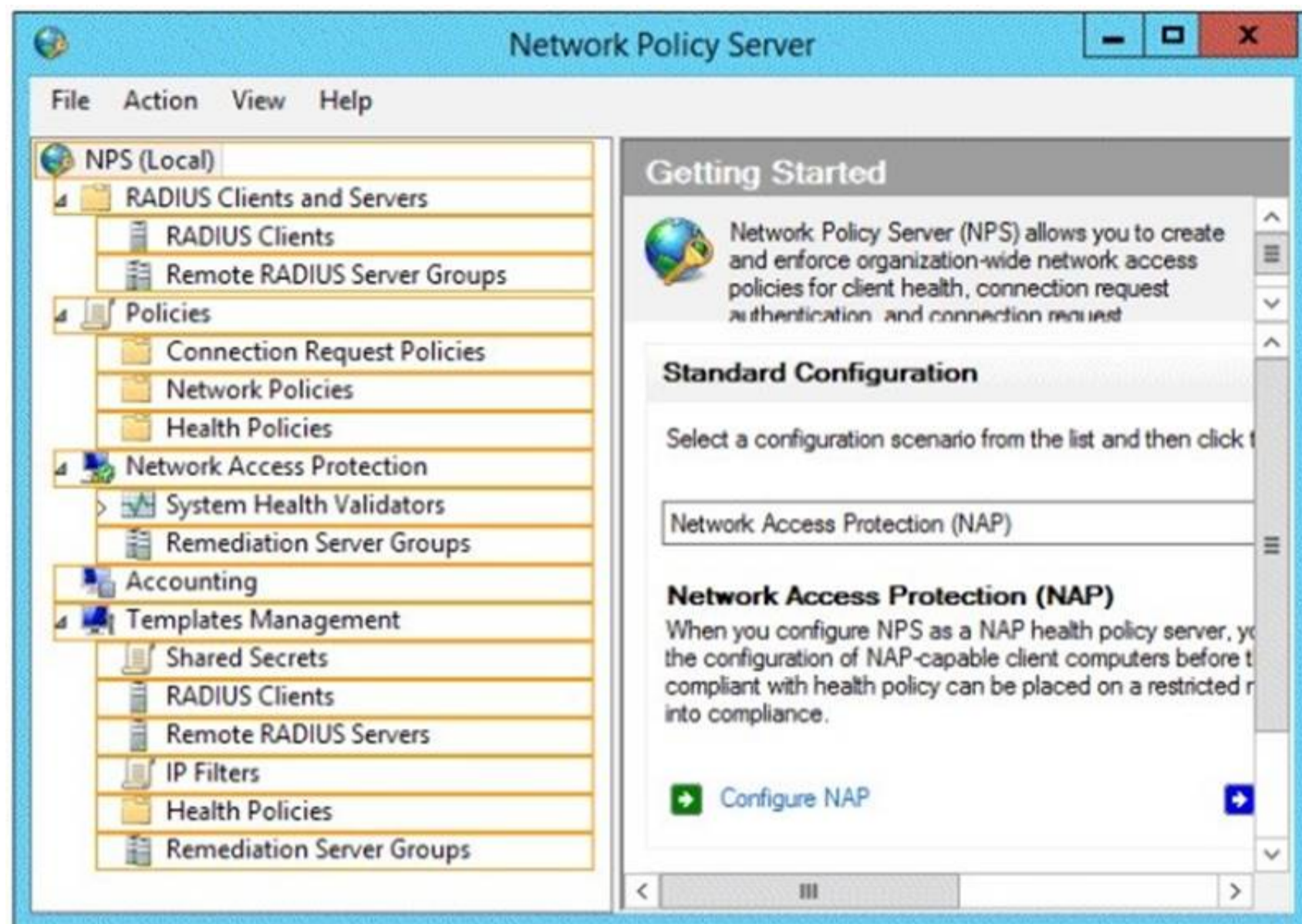
HOTSPOT - (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has the Network Policy Server server role installed. The domain contains a server named Server2 that is configured for RADIUS accounting.

Server1 is configured as a VPN server and is configured to forward authentication requests to Server2.

You need to ensure that only Server2 contains event information about authentication requests from connections to Server1.

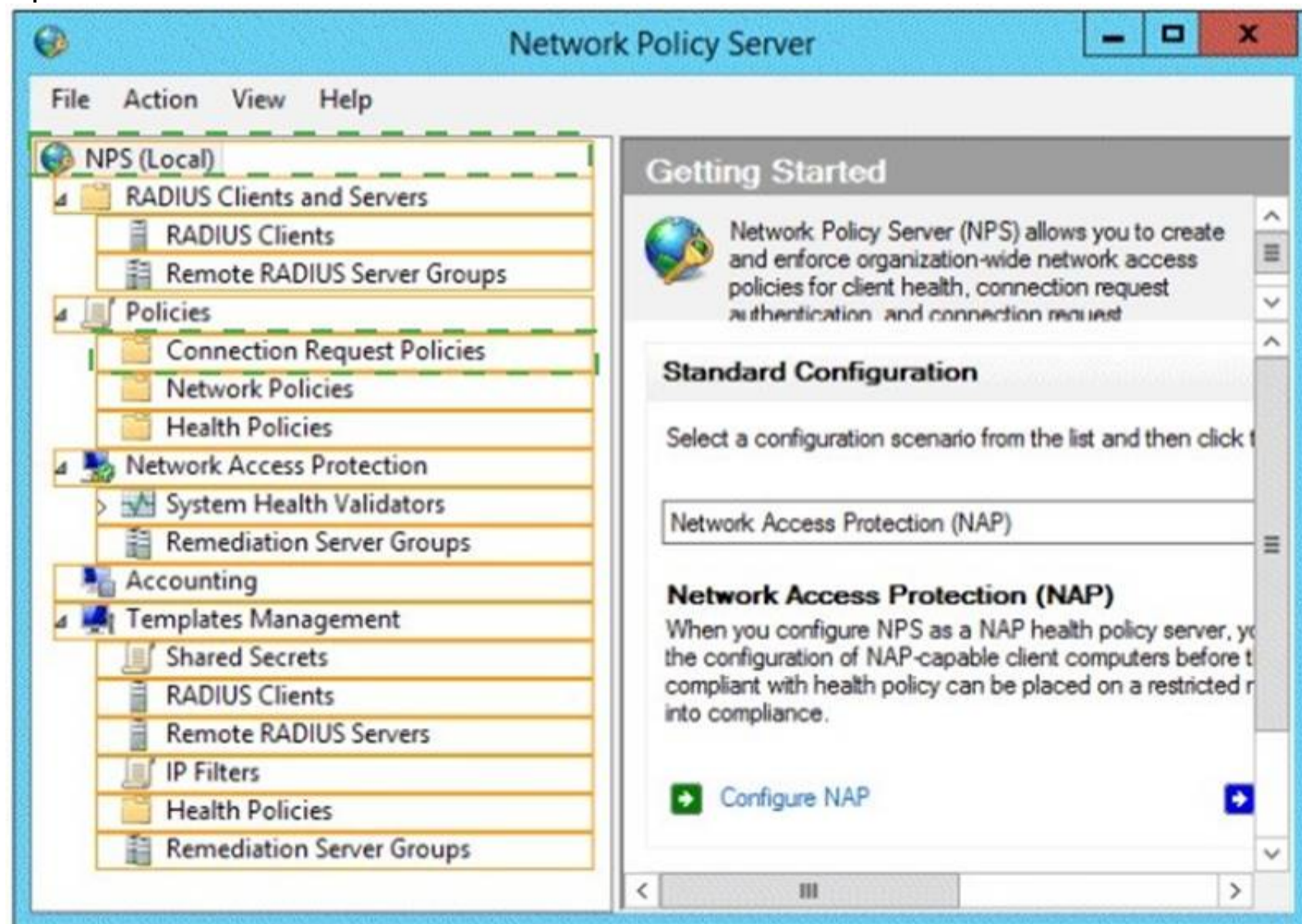
Which two nodes should you configure from the Network Policy Server console? To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 126

- (Topic 2)

Your network contains an Active Directory domain named adatum.com. All domain controllers run Windows Server 2012 R2. The domain contains a virtual

machine named DC2.

On DC2, you run Get-ADDCCloningExcludedApplicationList and receive the output shown in the following table.

Name	Type
App1	Service

You need to ensure that you can clone DC2.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- ☐ A. Create an empty file named DCCloneConfig.xml.
- ☐ B. Add the following information to the DCCloneConfigSchema.xsd file:
- ```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```
- ☐ C. Create an empty file named CustomDCCloneAllowList.xml.
- ☐ D. Create a file named DCCloneConfig.xml that contains the following information:
- ```
<AllowList>
 <Allow>
 <Name>App1</Name>
 <Type>Service</Type>
 </Allow>
</AllowList>
```
- ☐ E. Create a file named CustomDCCloneAllowList.xml that contains the following information:
- ```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```

- A. Option A
 B. Option B
 C. Option C
 D. Option D
 E. Option E

Answer: AE

Explanation:

Because domain controllers provide a distributed environment, you could not safely clone an Active Directory domain controller in the past.

Before, if you cloned any server, the server would end up with the same domain or forest, which is unsupported with the same domain or forest. You would then have to run sysprep, which would remove the unique security information before cloning and then promote a domain controller manually. When you clone a domain controller, you perform safe cloning, which a cloned domain controller automatically runs a subset of the sysprep process and promotes the server to a domain controller automatically.

The four primary steps to deploy a cloned virtualized domain controller are as follows:

? Grant the source virtualized domain controller the permission to be cloned by adding the source virtualized domain controller to the Cloneable Domain Controllers group.

? Run Get-ADDCCloningExcludedApplicationListcmdlet in Windows PowerShell to determine which services and applications on the domain controller are not compatible with the cloning.

? Run New-ADDCCloneConfigFile to create the clone configuration file, which is stored in the C:\Windows\NTDS.

? In Hyper-V, export and then import the virtual machine of the source domain controller.

Run Get-ADDCCloningExcludedApplicationListcmdlet In this procedure, run the Get- ADDCCloningExcludedApplicationListcmdlet on the source virtualized domain controller to identify any programs or services that are not evaluated for cloning. You need to run the Get-ADDCCloningExcludedApplicationListcmdlet before the New- ADDCCloneConfigFilecmdlet because if the New-ADDCCloneConfigFilecmdlet detects an excluded application, it will not create a DCCloneConfig.xml file. To identify applications or services that run on a source domain controller which have not been evaluated for cloning. Get-ADDCCloningExcludedApplicationList

Get-ADDCCloningExcludedApplicationList -GenerateXml

The clone domain controller will be located in the same site as the source domain controller unless a different site is specified in the DCCloneConfig.xml file.

Note:

? The Get-ADDCCloningExcludedApplicationListcmdlet searches the local domain controller for programs and services in the installed programs database, the services control manager that are not specified in the default and user defined inclusion list. The applications in the resulting list can be added to the user defined

exclusion list if they are determined to support cloning. If the applications are not cloneable, they should be removed from the source domain controller before the clone media is created. Any application that appears in cmdlet output and is not included in the user defined inclusion list will force cloning to fail.

? The Get-ADDCCloningExcludedApplicationListcmdlet needs to be run before the New- ADDCCloneConfigFilecmdlet is used because if the New- ADDCCloneConfigFilecmdlet detects an excluded application, it will not create a DCCloneConfig.xml file.

? DCCloneConfig.xml is an XML configuration file that contains all of the settings the cloned DC will take when it boots. This includes network settings, DNS, WINS, AD site name, new DC name and more. This file can be generated in a few different ways.

The New-ADDCCloneConfigcmdlet in PowerShell By hand with an XML editor

By editing an existing config file, again with an XML editor (Notepad is not an XML editor.)

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

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

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

PS C:\Users\Administrator.DC01>
```

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

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

Name
----
WLMS
Type
----
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>
```

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

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

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

CustomDCCloneAllowList - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<dc:CustomDCCloneAllowList xmlns:dc="uri:microsoft.com:schemas:CustomDCCloneAllowList">
  <Allow>
    <Name>WLMS</Name>
    <Type>Service</Type>
  </Allow>
</dc:CustomDCCloneAllowList>
```

You can populate the XML file. . . . doesn't need to be empty. . . .

```
Administrator: Windows PowerShell
PS C:\Users\Administrator.DC01> New-ADDCCloneConfigFile -Static -IPv4Address 10.10.10.202 -IPv4DefaultGateway 10.10.10.1
-IPv4SubnetMask 255.255.255.0 -IPv4DNSResolver 10.10.10.73,10.10.10.202 -CloneComputerName DC02 -SiteName Default-First
-Site-Name
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or later.
Passed: The domain controller hosting the PDC FSMO role (DC01.accusource.local) was located and running Windows Server 2012 or later.

Verifying authorization: Checking if this domain controller is a member of the 'Cloneable Domain Controllers' group...
Located the local domain controller: (DC01.accusource.local).
Querying the 'Cloneable Domain Controllers' group...
Pass: The local domain controller is a member of the 'Cloneable Domain Controllers' group.

Starting test: Validating the cloning allow list.
NOTE: C:\Windows\NTDS\CustomDCCloneAllowList.xml is being used as the defined inclusion list.
No excluded applications were detected.
Pass: No excluded applications were detected.

No valid clone configuration files were found at any of the supported locations.
All preliminary validation checks passed.

Starting creation of the clone configuration file...
Finding the path to the Directory Service database...
The clone configuration file was generated at:
C:\Windows\NTDS\DCCloneConfig.xml
Generating the clone configuration file content...
The clone configuration file has been created.

PS C:\Users\Administrator.DC01>
```

```

DCCloneConfig - Notepad
File Edit Format View Help
<?xml version="1.0"?>
<d3c:DCCloneConfig xmlns:d3c="uri:microsoft.com:schemas:DCCloneConfig">
  <ComputerName>DC02</ComputerName>
  <SiteName>Default-First-Site-Name</SiteName>
  <IPSettings>
    <IPv4Settings>
      <StaticSettings>
        <Address>10.10.10.202</Address>
        <SubnetMask>255.255.255.0</SubnetMask>
        <DefaultGateway>10.10.10.1</DefaultGateway>
        <DNSResolver>10.10.10.73</DNSResolver>
        <DNSResolver>10.10.10.202</DNSResolver>
      </StaticSettings>
    </IPv4Settings>
  </IPSettings>
</d3c:DCCloneConfig>

```

References:

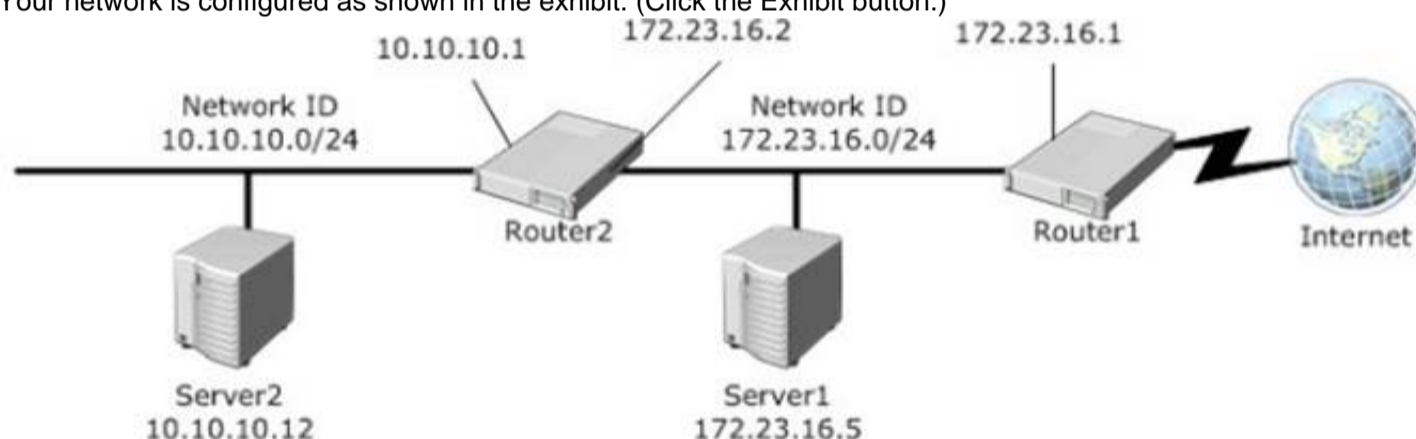
<http://technet.microsoft.com/en-us/library/hh831734.aspx>

<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>

NEW QUESTION 128

- (Topic 2)

Your network is configured as shown in the exhibit. (Click the Exhibit button.)



Server1 regularly accesses Server2.

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

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

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

Answer: A

Explanation:

Destination - specifies either an IP address or host name for the network or host. subnetmask - specifies a subnet mask to be associated with this route entry. If subnetmask

is not specified, 255.255.255.255 is used.

gateway - specifies either an IP address or host name for the gateway or router to use when forwarding.

costmetric - assigns an integer cost metric (ranging from 1 through 9,999) to be used in calculating the fastest, most reliable, and/or least expensive routes. If costmetric is not specified, 1 is used.

interface - specifies the interface to be used for the route that uses the interface number. If an interface is not specified, the interface to be used for the route is determined from the gateway IP address.

References:

<http://support.microsoft.com/kb/299540/en-us>

<http://technet.microsoft.com/en-us/library/cc757323%28v=ws.10%29.aspx>

NEW QUESTION 130

HOTSPOT - (Topic 2)

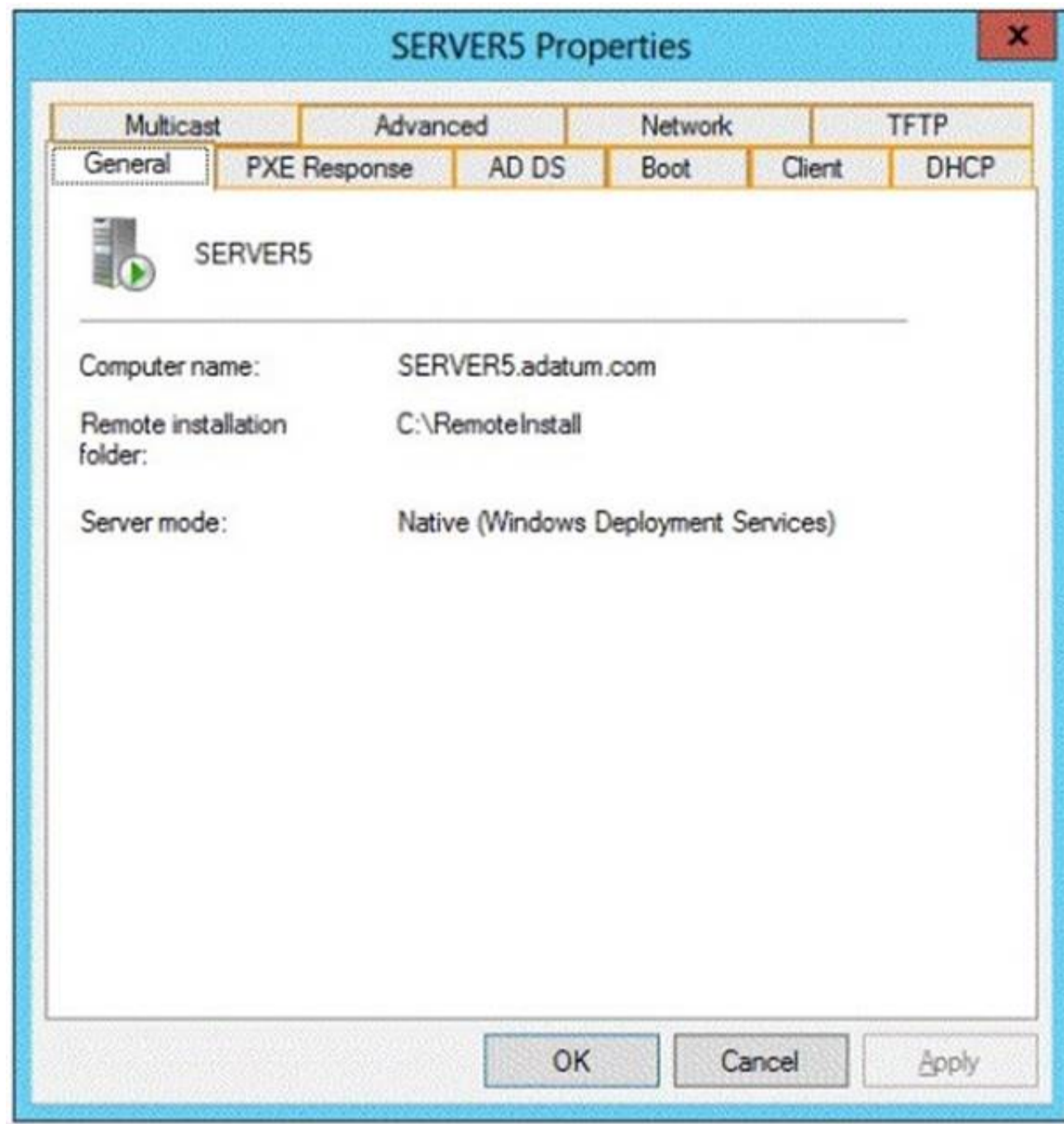
You have a server named Servers that runs Windows Server 2012 R2. Servers has the Windows Deployment Services server role installed.

Server5 contains several custom images of Windows 8.

You need to ensure that when 32-bit client computers start by using PXE, the computers automatically install an image named Image 1.

What should you configure?

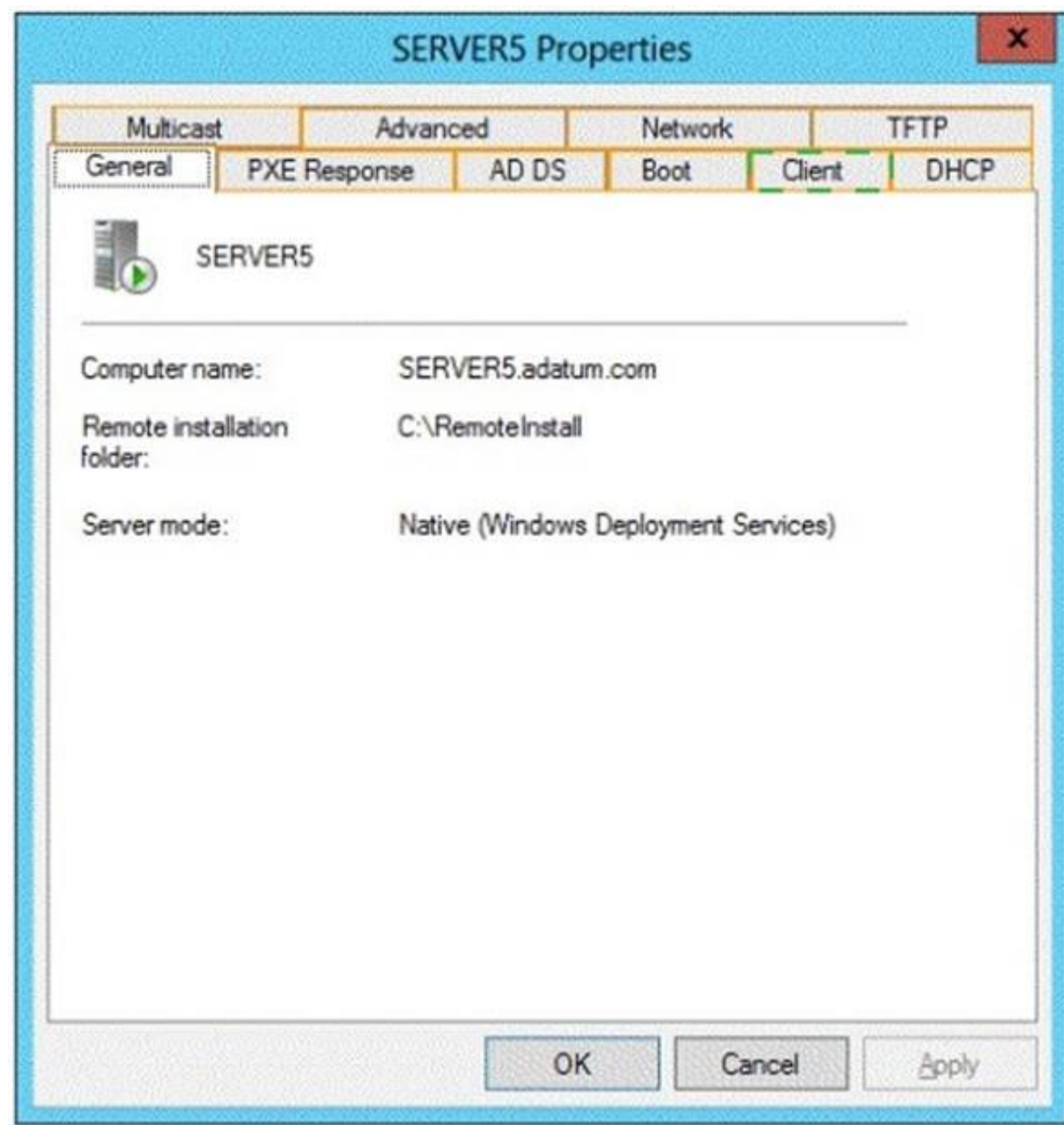
To answer, select the appropriate tab in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

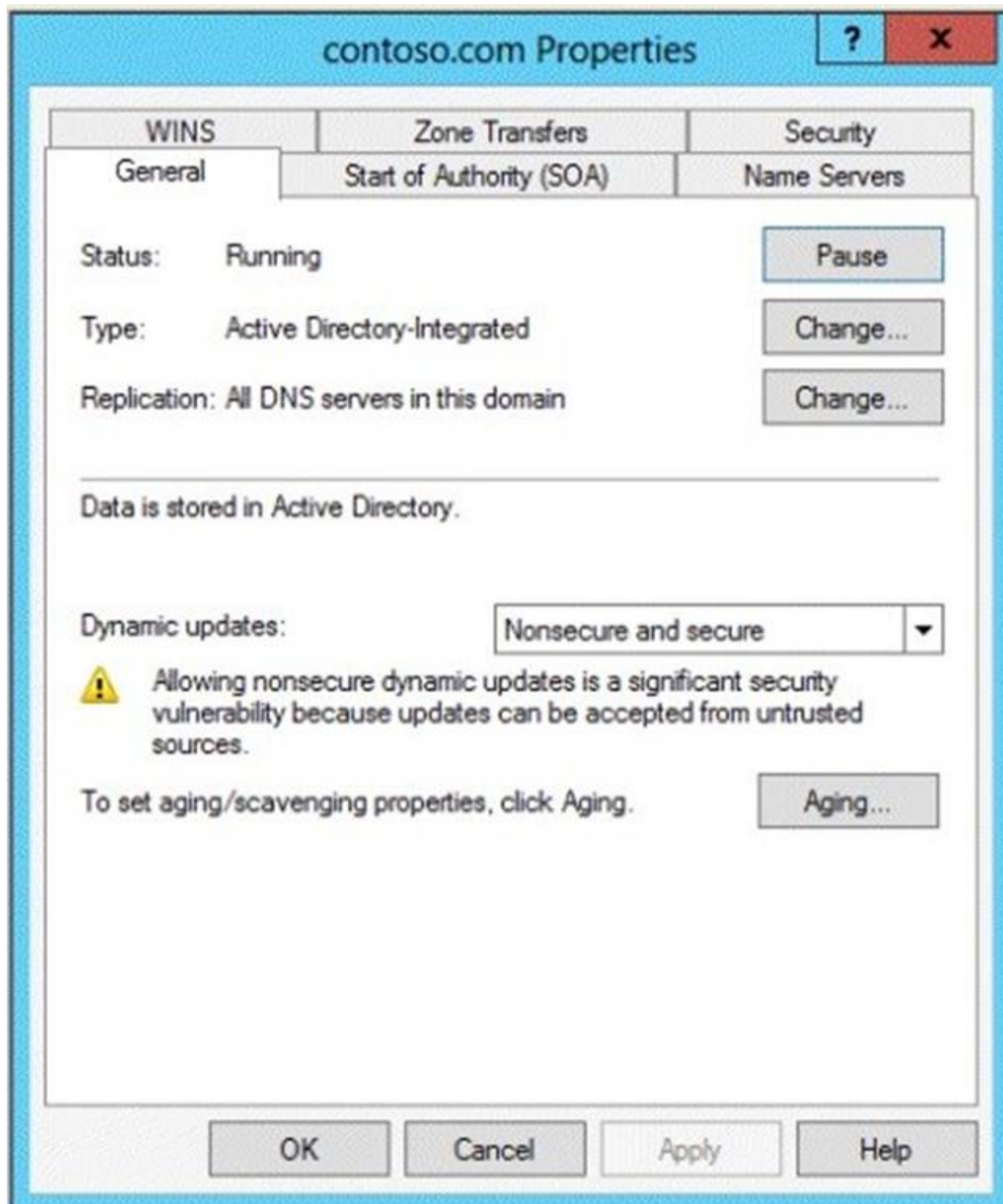
Explanation:



NEW QUESTION 132

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1. DC1 is a DNS server for contoso.com. The properties of the contoso.com zone are configured as shown in the exhibit. (Click the Exhibit button.)



The domain contains a server named Server1 that is part of a workgroup named Workgroup. Server1 is configured to use DC1 as a DNS server. You need to ensure that Server1 dynamically registers a host (A) record in the contoso.com zone. What should you configure?

- A. The workgroup name of Server1
- B. The Security settings of the contoso.com zone
- C. The Dynamic updates setting of the contoso.com zone
- D. The primary DNS suffix of Server1

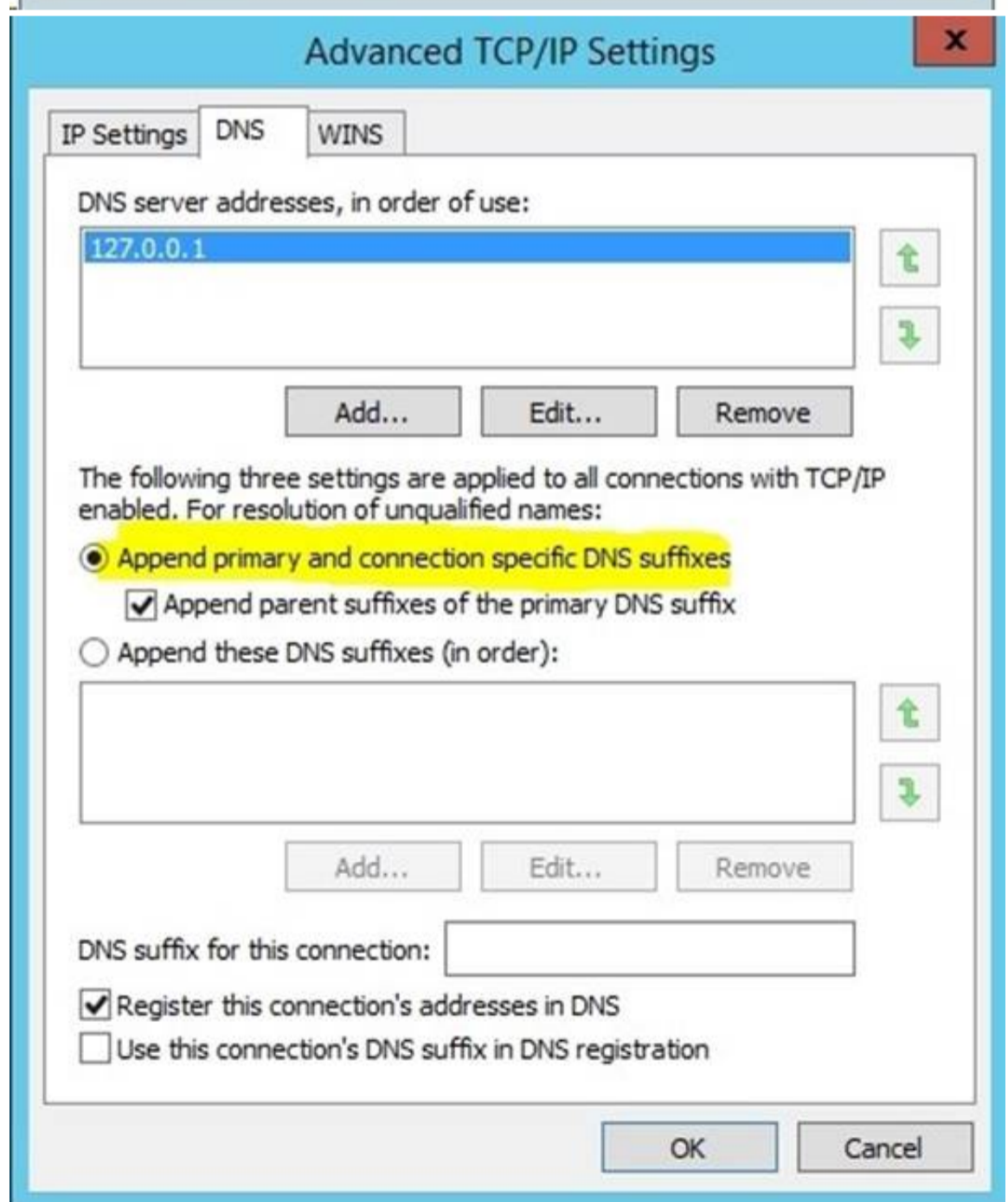
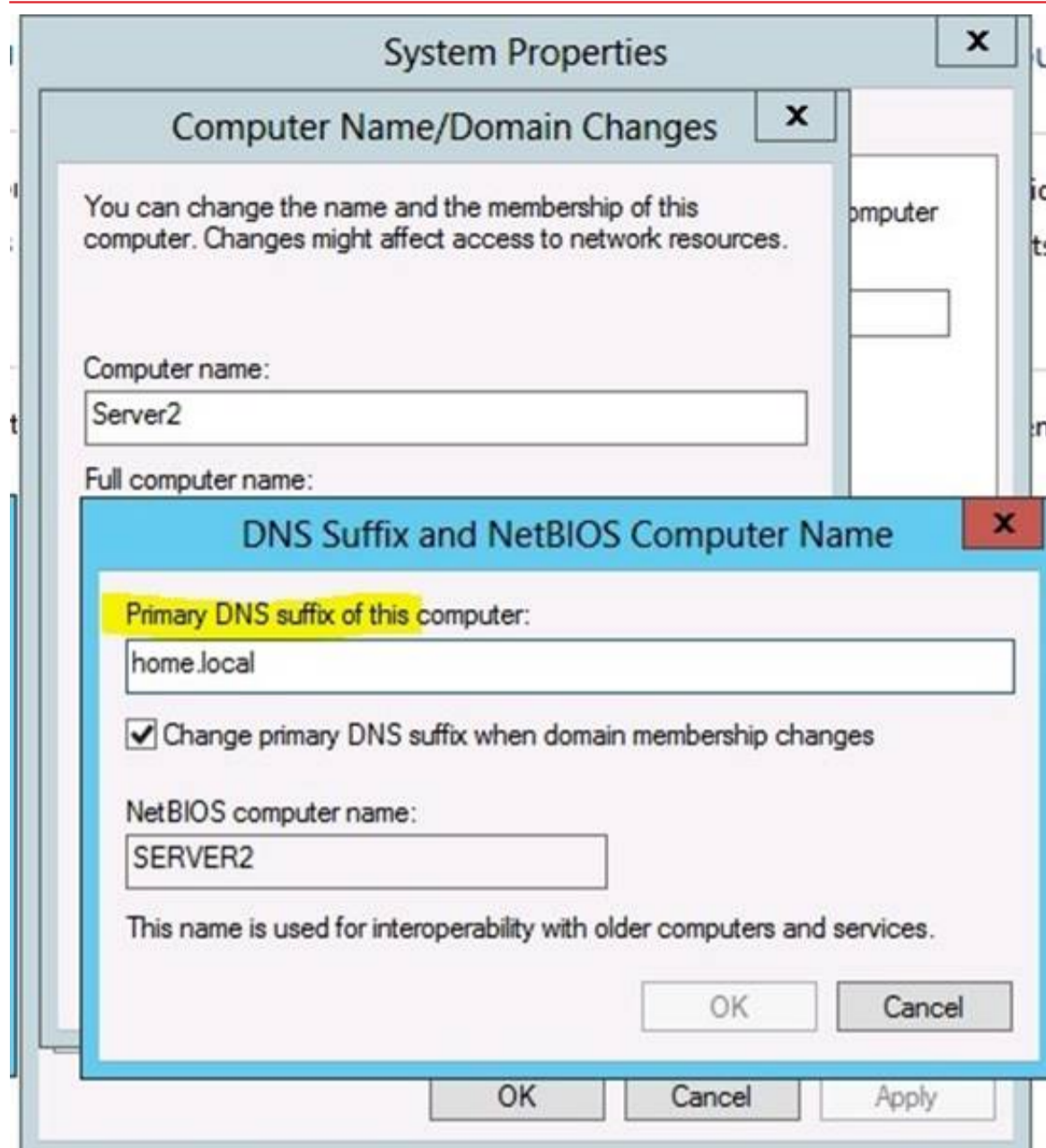
Answer: D

Explanation:

When any computer or a standalone server is added to a domain as a member, the network identifies that computer with its Fully Qualified Domain Name or FQDN. A Fully Qualified Domain Name consist of a hostname and the DNS suffix separated by a "." called period. An example for this can be server01.msftdomain.com where "server01" is the hostname of the computer and "msftdomain.com" is the DNS suffix which follows the hostname. A complete FQDN of a client computer or a member server uniquely identifies that computer in the entire domain.

Primary DNS suffix must manually be added in Windows 8 computer to change its hostname to Fully Qualified Domain Name so that it becomes eligible to send queries and receive responses from the DNS server. Following are the steps which can be implemented to add primary DNS suffix to a Windows 8 computer hostname:

- ? Log on to Windows 8 computer with administrator account.
- ? From the options available on the screen click Control Panel.
- ? On the opened window click More Settings from the left pane.
- ? On the next window click System and Security category and on the appeared window click System.
- ? On View basic information about your computer window click Change settings under Computer name, domain, and workgroup settings section.
- ? On System Properties box make sure that Computer Name tab is selected and click Change button.
- ? On Computer Name/Domain Changes box click More button.
- ? On DNS Suffix and NetBIOS Computer Name box type in the DNS domain name as the DNS suffix to the Windows 8 computer under Primary DNS suffix of this computer field.
- ? Click Ok button on all the boxes and restart the computer to allow changes to take effect.



For years, Windows DNS has supported dynamic updates, whereas a DNS client host registers and dynamically updates the resource records with a DNS server. If a host's IP address changes, the resource record (particularly the A record) for the host is automatically updated, while the host utilizes the DHCP server to dynamically update its Pointer (PTR) resource record. Therefore, when a user or service needs to contact a client PC, it can look up the IP address of the host. With larger organizations, this becomes an essential feature, especially for clients that frequently move or change locations and use DHCP to automatically obtain an IP address. For dynamic DNS updates to succeed, the zone must be configured to accept dynamic updates:



References:

<http://technet.microsoft.com/en-us/library/cc778792%28v=ws.10%29.aspx>
<http://technet.microsoft.com/en-us/library/cc778792%28v=ws.10%29.aspx>
<http://www.advicehow.com/adding-primary-dns-suffix-in-microsoft-windows-8/>
<http://technet.microsoft.com/en-us/library/cc959611.aspx>

NEW QUESTION 136

- (Topic 2)

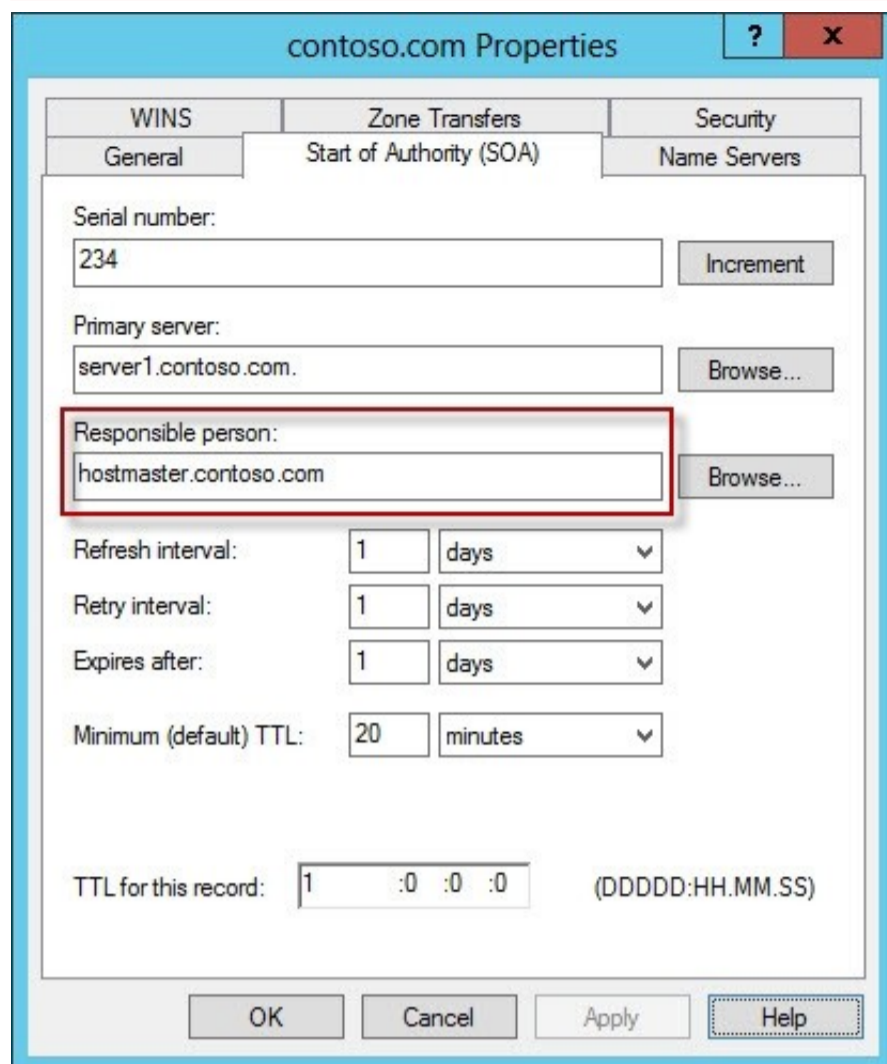
You have a DNS server named Server1 that runs Windows Server 2012 R2. On Server1, you create a DNS zone named contoso.com. You need to specify the email address of the person responsible for the zone. Which type of DNS record should you configure?

- 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.



The screenshot shows the 'contoso.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The 'Responsible person' field is highlighted with a red box and contains the text 'hostmaster.contoso.com'. Other fields include 'Serial number' (234), 'Primary server' (server1.contoso.com.), 'Refresh interval' (1 days), 'Retry interval' (1 days), 'Expires after' (1 days), 'Minimum (default) TTL' (20 minutes), and 'TTL for this record' (1 :0 :0 :0).

```
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 138

- (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 .adm 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 .adm 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 140

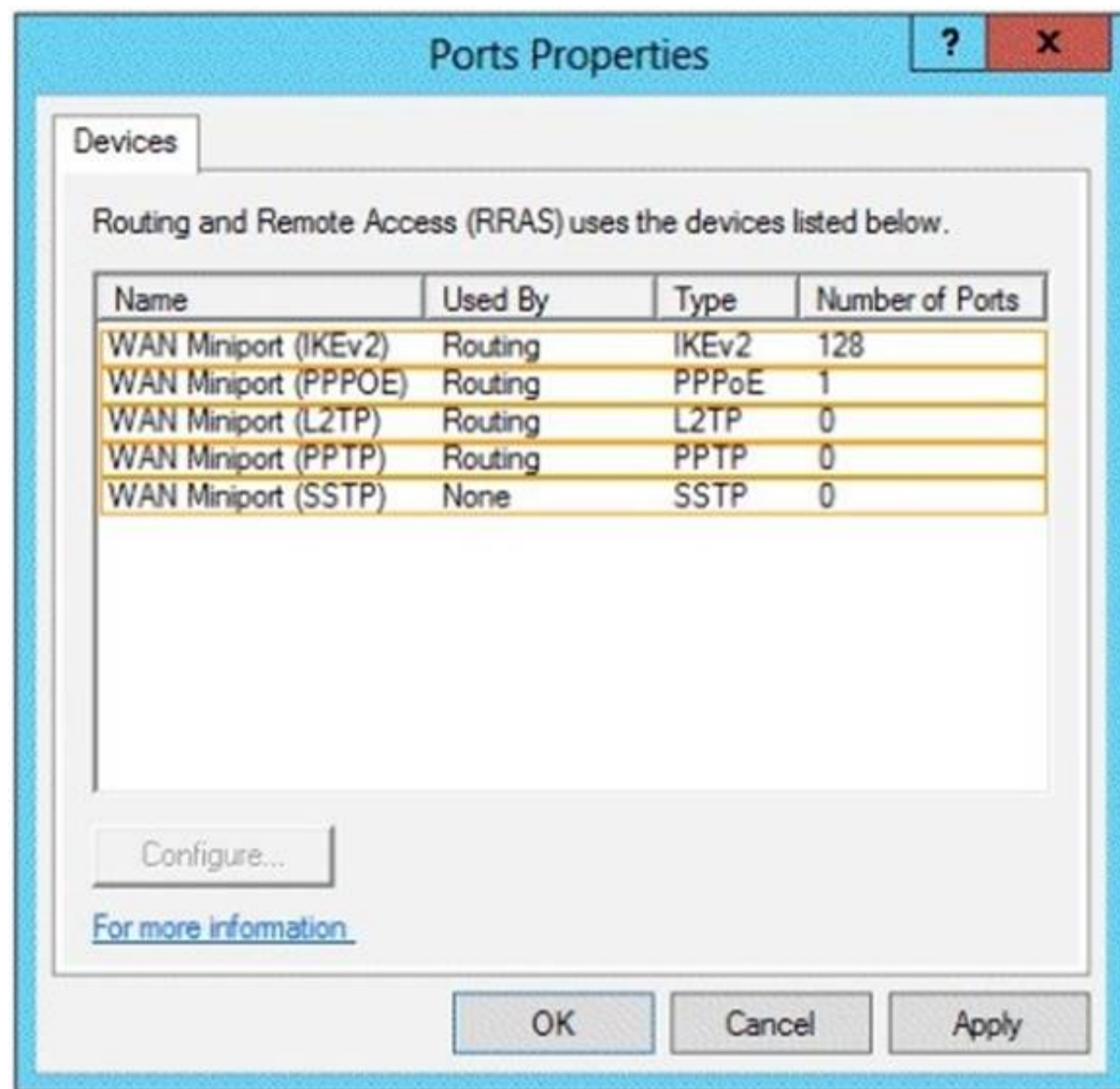
HOTSPOT - (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Access server role installed.

You need to configure the ports on Server1 to ensure that client computers can establish VPN connections to Server1. The solution must NOT require the use of certificates or pre-shared keys.

What should you modify?

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The four types of tunneling protocols used with a VPN/RAS server running on Windows Server 2012 include:

Point-to-Point Tunneling Protocol (PPTP): A VPN protocol based on the legacy Point-to-Point protocol used with modems. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality.

Layer 2 Tunneling Protocol (L2TP): Used with IPsec to provide security. L2TP supports either computer certificates or a preshared key as the authentication method for IPsec. IKEv2: IKE is short for Internet Key Exchange, which is a tunneling protocol that uses IPsec Tunnel Mode protocol. The message is encrypted with one of the following protocols by using encryption keys that are generated from the IKEv2 negotiation process.

Secure Socket Tunneling Protocol (SSTP): Introduced with Windows Server 2008, which uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls

References:

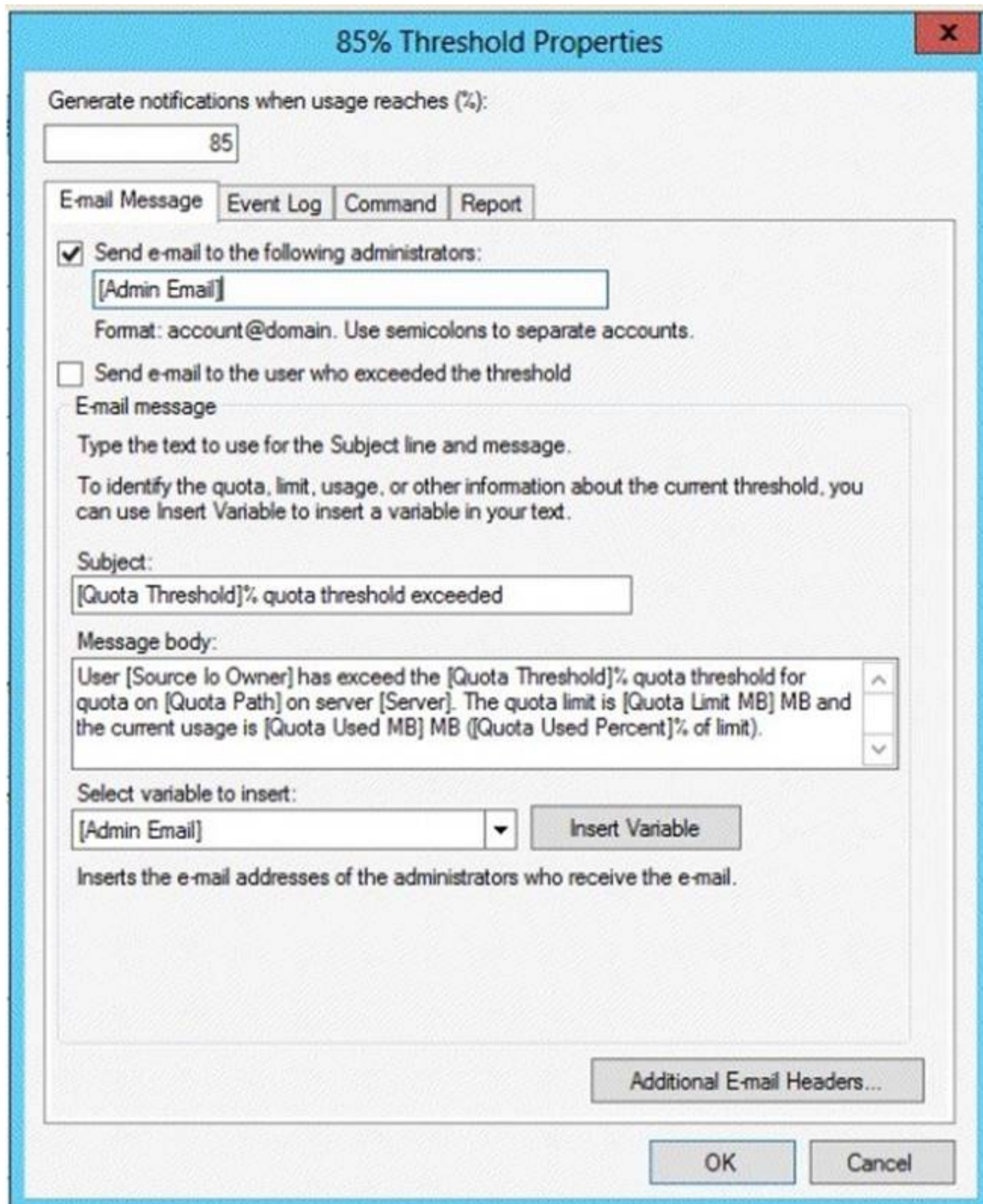
http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

NEW QUESTION 144

- (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 File Server Resource Manager role service installed.

You configure a quota threshold as shown in the exhibit. (Click the Exhibit button.)



85% Threshold Properties

Generate notifications when usage reaches (%):

E-mail Message | Event Log | Command | Report

☒ Send e-mail to the following administrators:

 Format: account@domain. Use semicolons to separate accounts.

☐ Send e-mail to the user who exceeded the threshold

E-mail message
 Type the text to use for the Subject line and message.
 To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.

Subject:

Message body:

Select variable to insert:

Inserts the e-mail addresses of the administrators who receive the e-mail.

You need to ensure that a user named User1 receives an email notification when the threshold is exceeded. What should you do?

- A. Create a performance counter alert.
- B. Create a classification rule.
- C. Modify the members of the Performance Log Users group.
- D. Configure the File Server Resource Manager Options.

Answer: D

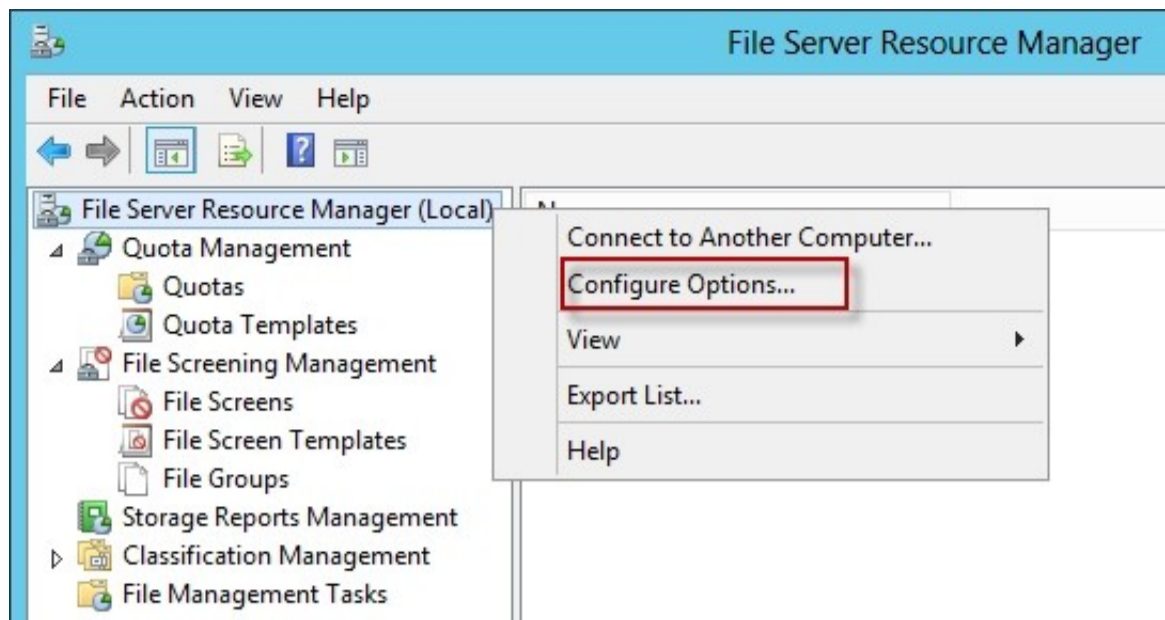
Explanation:

When you create quotas and file screens, you have the option of sending e-mail notifications to users when their quota limit is approaching or after they have attempted to save files that have been blocked. If you want to routinely notify certain administrators of quota and file screening events, you can configure one or more default recipients.

To send these notifications, you must specify the SMTP server to be used for forwarding the e-mail messages.

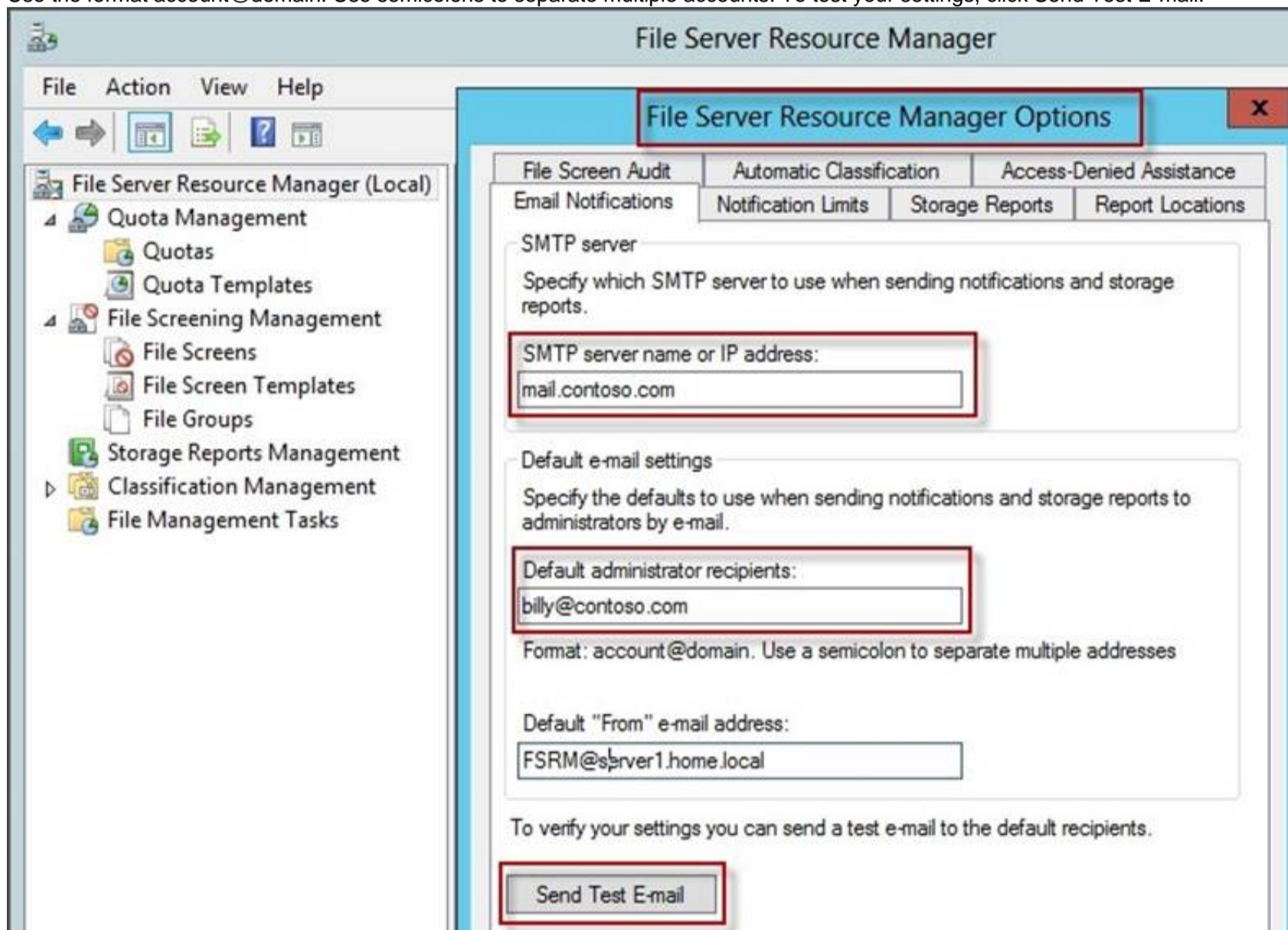
To configure e-mail options

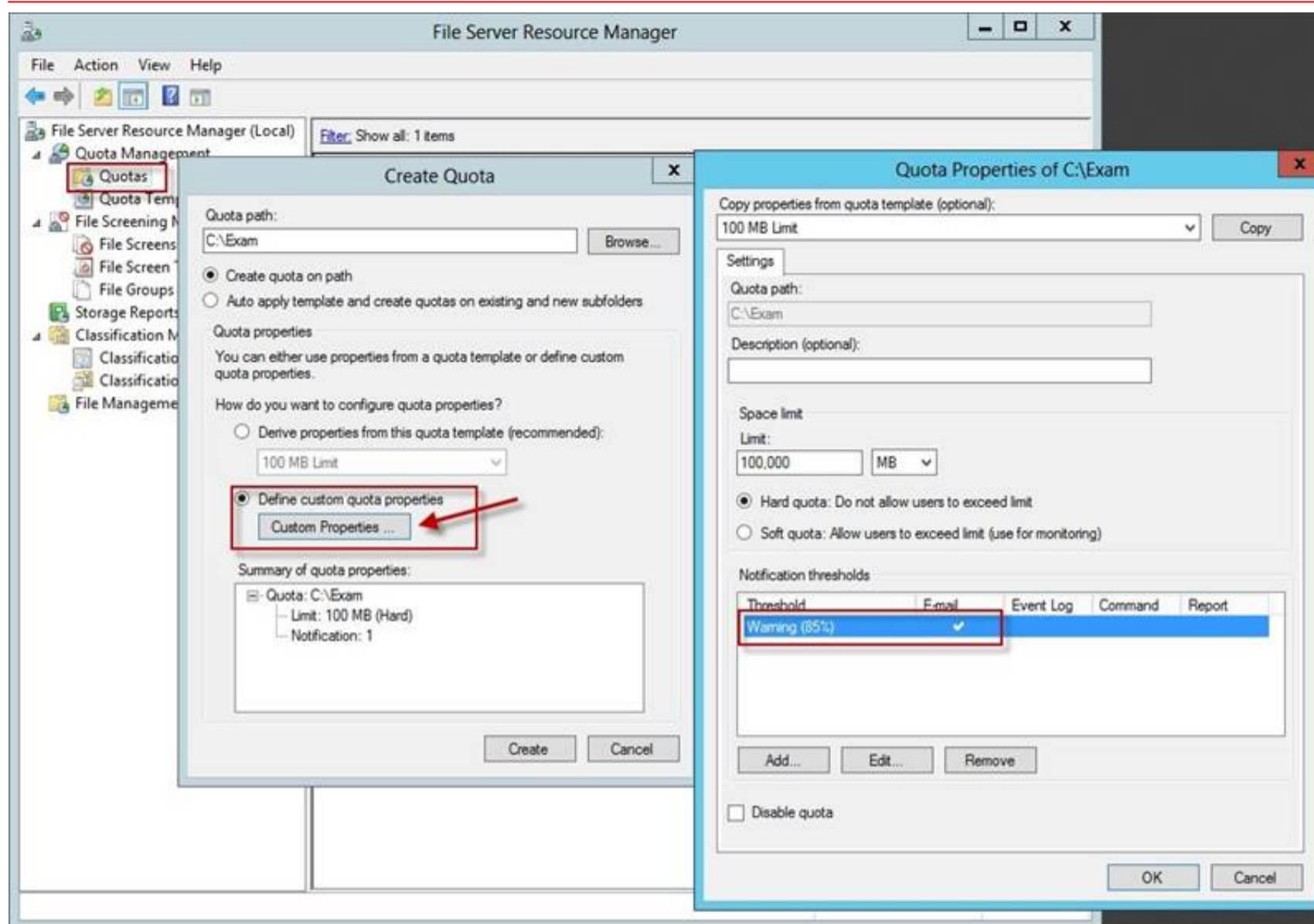
In the console tree, right-click File Server Resource Manager, and then click Configure options. The File Server Resource Manager Options dialog box opens.



On the E-mail Notifications tab, under SMTP server name or IP address, type the host name or the IP address of the SMTP server that will forward e-mail notifications.

If you want to routinely notify certain administrators of quota or file screening events, under Default administrator recipients, type each e-mail address. Use the format account@domain. Use semicolons to separate multiple accounts. To test your settings, click Send Test E-mail.





NEW QUESTION 148

- (Topic 3)

Your network contains an Active Directory domain named contoso.com.

All user accounts reside in an organizational unit (OU) named OU1. All of the users in the marketing department are members of a group named Marketing. All of the users in the human resources department are members of a group named HR.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preferences of GPO1 to add two shortcuts named Link1 and Link2 to the desktop of each user.

You need to ensure that Link1 only appears on the desktop of the users in Marketing and that Link2 only appears on the desktop of the users in HR.

What should you configure?

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

Answer: D

Explanation:

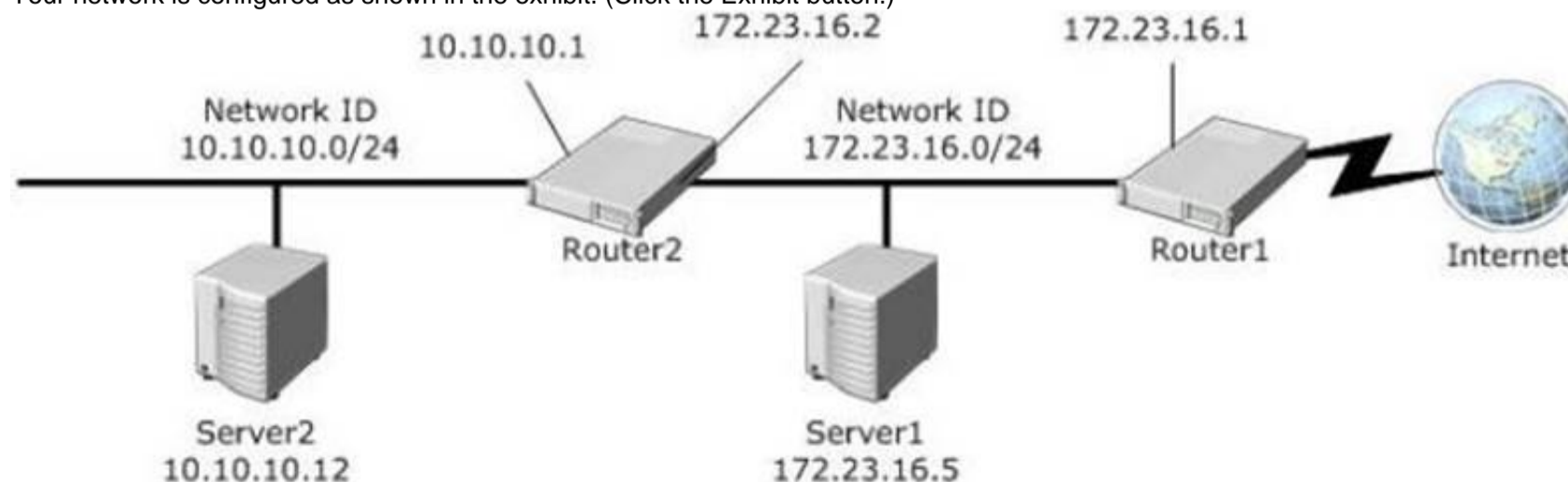
You can use item-level targeting to change the scope of individual preference items, so they apply only to selected users or computers. Within a single Group Policy object (GPO), you can include multiple preference items, each customized for selected users or computers and each targeted to apply settings only to the relevant users or computers.

Reference: <http://technet.microsoft.com/en-us/library/cc733022.aspx>

NEW QUESTION 151

- (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 Router1.

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 155

- (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 user accounts were authenticated by RODC01. 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

Explanation:

Gets the Active Directory accounts that are authenticated by a read-only domain controller or that are in the revealed list of the domain controller.

Reference: Get-ADDomainControllerPasswordReplicationPolicyUsage <https://technet.microsoft.com/en-us/library/ee617194.aspx>

NEW QUESTION 158

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 160

- (Topic 3)

You deploy a Windows Server Update Services (WSUS) server named Server01.

You plan to use a Group Policy object (GPO) to configure all client computers to use Server01 as a Microsoft Update server and to assign the client computers to computer groups.

You need to ensure that the computers are assigned to the correct computer groups automatically when the GPO is deployed. Which two actions should you perform before you deploy the GPO? Each correct answer presents part of the solution.

- A. From Windows PowerShell, run the Approve-WSUSUpdate cmdlet.
- B. From the Update Services console, modify the Computers option.
- C. From Windows PowerShell, run the Add-WSUSComputer cmdlet.
- D. From the Update Services console, manually create the computer groups.
- E. From the Update Services console, modify the Products and Classifications options.

Answer: BD

Explanation:

References:

[https://technet.microsoft.com/en-us/library/dd939829\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd939829(v=ws.10).aspx)

NEW QUESTION 161

- (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 whether the members of the Protected Users group will be prevented from authenticating by using NTLM.

Which cmdlet should you use?

- A. Get-ADGroupMember
- B. Get-ADDomainControllerPasswordReplicationPolicy
- C. Get-ADDomainControllerPasswordReplicationPolicyUsage
- D. Get-ADDomain
- E. Get-ADOptionalFeature
- F. Get-ADAccountAuthorizationGroup
- G. Get-ADAuthenticationPolicySilo
- H. Get-ADAuthenticatonPolicy

Answer: D

Explanation:

If the domain functional level is Windows Server 2012 R2, members of the (Protected Users) group can no longer authenticate by using NTLM authentication. So we need to check the domain functional level with Get-ADDomain. <https://technet.microsoft.com/en-us/library/Dn518179.aspx>

NEW QUESTION 165

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. You create a new user account named Admin5.

You need to ensure that Admin5 can create Group Policy objects (GPOs) and link the GPOs to all of the organizational units (OUs) in the domain. Admin5 must be prevented from modifying GPOs created by other administrators.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. From Active Directory Users and Computers, modify the members of the Network Configuration Operators group.
- B. From Active Directory Users and Computers, modify the Security settings of the Admin5 user account.
- C. From Group Policy Management, click the Group Policy Objects node and modify the Delegation settings.
- D. From Group Policy Management, click the contoso.com node and modify the Delegationsettings.
- E. From Active Directory Users and Computers, modify the members of the Group Policy Creator Owners group.

Answer: CD

NEW QUESTION 169

- (Topic 3)

Your network contains two Active Directory forests named contoso.com and adatum.com. All domain controllers run Windows Server 2012 R2.

The adatum.com domain contains a Group Policy object (GPO) named GPO1. An administrator from adatum.com backs up GPO1 to a USB flash drive.

You have a domain controller named dc1.contoso.com. You insert the USB flash drive in dc1.contoso.com.

You need to identify the domain-specific reference in GPO1. What should you do?

- A. From the Migration Table Editor, click Populate from Backup.
- B. From Group Policy Management, run the Group Policy Modeling Wizard.
- C. From Group Policy Management, run the Group Policy Results Wizard.
- D. From the Migration Table Editor, click Populate from GPO.

Answer: A

NEW QUESTION 170

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

DirectAccess is deployed to the network.

Remote users connect to the DirectAccess server by using a variety of network speeds.

The remote users report that sometimes their connection is very slow.

You need to minimize Group Policy processing across all wireless wide area network (WWAN) connections.

Which Group Policy setting should you configure?

- A. Configure Group Policy slow link detection.
- B. Configure Direct Access connections as a fast network connection.

- C. Configure wireless policy processing.
- D. Change Group Policy processing to run asynchronously when a slow network connection is detected.

Answer: A

NEW QUESTION 172

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2008 R2. You plan to test Windows Server 2012 R2 by using native-boot virtual hard disks (VHDs). You have a Windows image file named file1.wim. You need to add an image of a volume to file1.wim. What should you do?

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

Answer: D

Explanation:

The Deployment Image Servicing and Management (DISM) tool is a command-line tool that enables the creation of Windows image (.wim) files for deployment in a manufacturing or corporate IT environment. The /Append-Image option appends a volume image to an existing .wim file allowing you to store many customized Windows images in a fraction of the space. When you combine two or more Windows image files into a single .wim, any files that are duplicated between the images are only stored once.

Incorrect:

Not A, Not B: Imagex has been retired and replaced by dism.

Reference: Append a Volume Image to an Existing Image Using DISM <https://technet.microsoft.com/en-us/library/hh824916.aspx>

NEW QUESTION 173

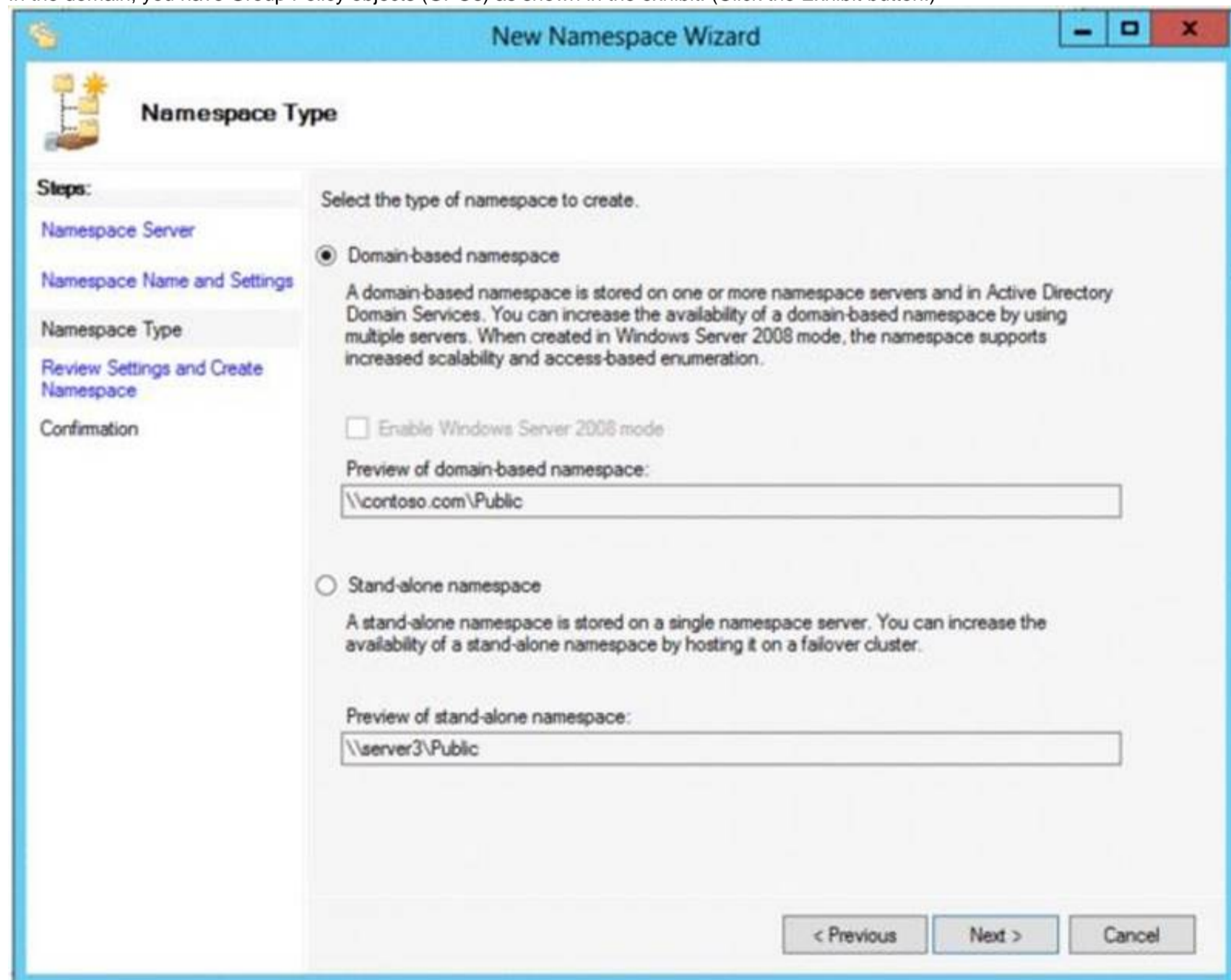
- (Topic 3)

Your network contains an Active Directory domain named contoso.com. The functional level of the forest is Windows Server 2008 R2.

Computer accounts for the marketing department are in an organizational unit (OU) named Departments\Marketing\Computers. User accounts for the marketing department are in an OU named Departments\Marketing\Users.

All of the marketing user accounts are members of a global security group named MarketingUsers. All of the marketing computer accounts are members of a global security group named MarketingComputers.

In the domain, you have Group Policy objects (GPOs) as shown in the exhibit. (Click the Exhibit button.)



You create two Password Settings objects named PSO1 and PSO2. PSO1 is applied to MarketingUsers. PSO2 is applied to MarketingComputers. The minimum password length is defined for each policy as shown in the following table.

Location	Minimum password length
Default Domain Policy	7
GPO1	5
GPO2	6
PSO1	10
PSO2	12

You need to identify the minimum password length required for each marketing user.
What should you identify?

- A. 5
- B. 6
- C. 7
- D. 10
- E. 12

Answer: D

NEW QUESTION 175

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. All users have client computers that run Windows 8.1.

All computer accounts reside in an organizational unit (OU) named OU1. All of the computer accounts for the marketing department are members of a group named Marketing. All of the computer accounts for the human resources department are members of a group named HR Computers.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preferences of GPO1 to add two shortcuts named Link1 and Link2 to the desktop.

You need to ensure that Link1 only appears on the desktop of client computers that have more than 80 GB of free disk space and that Link2 only appears on the desktop of client computers that have less than 80 GB of free disk space.

What should you configure?

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

Answer: C

Explanation:

References: [https://technet.microsoft.com/en-us/library/dn789189\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn789189(v=ws.11).aspx)

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 (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 links them to the domain: "DirectAccess Server Settings" contains Connection Security Settings and Firewall inbound 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 183

- (Topic 3)

Your network contains an Active Directory domain named adatum.com.

You need to audit changes to the files in the SYSVOL shares on all of the domain controllers. The solution must minimize the amount of SYSVOL replication traffic caused by the audit.

Which two settings should you configure? (Each correct answer presents part of the solution. Choose two.)

- A. Audit Policy\Audit system events
- B. Advanced Audit Policy Configuration\DS Access
- C. Advanced Audit Policy Configuration\Global Object Access Auditing
- D. Audit Policy\Audit object access
- E. Audit Policy\Audit directory service access
- F. Advanced Audit Policy Configuration\Object Access

Answer: DF

NEW QUESTION 184

.....

Relate Links

100% Pass Your 70-411 Exam with ExamBible Prep Materials

<https://www.exambible.com/70-411-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>