

Exam Questions 70-411

Administering Windows Server 2012

<https://www.2passeasy.com/dumps/70-411/>



NEW QUESTION 1

HOTSPOT - (Topic 1)

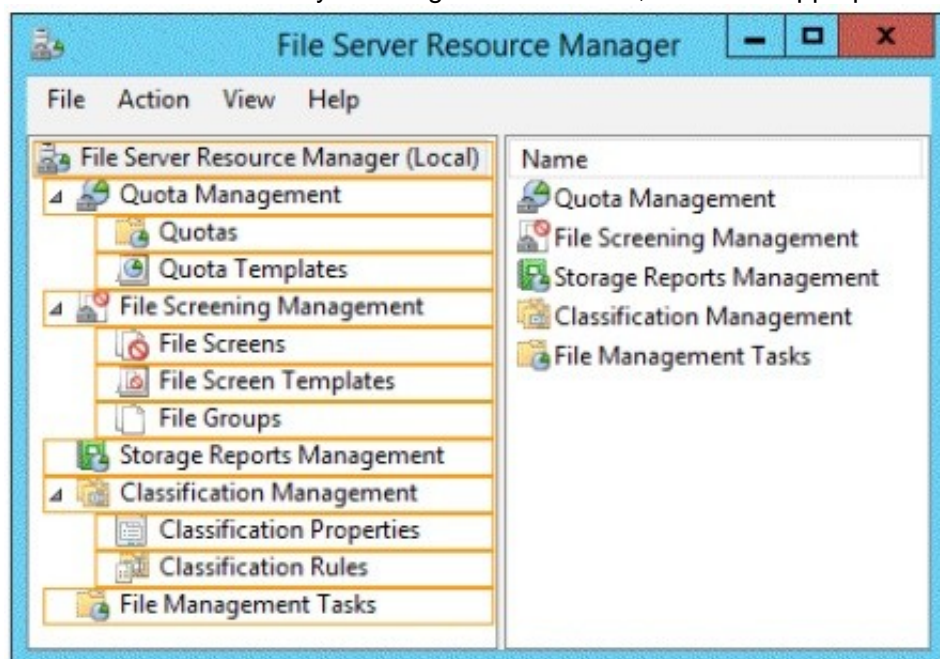
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.

You need to configure Server1 to meet the following requirements:

? Ensure that old files in a folder named Folder1 are archived automatically to a folder named Archive1.

? Ensure that all storage reports are saved to a network share.

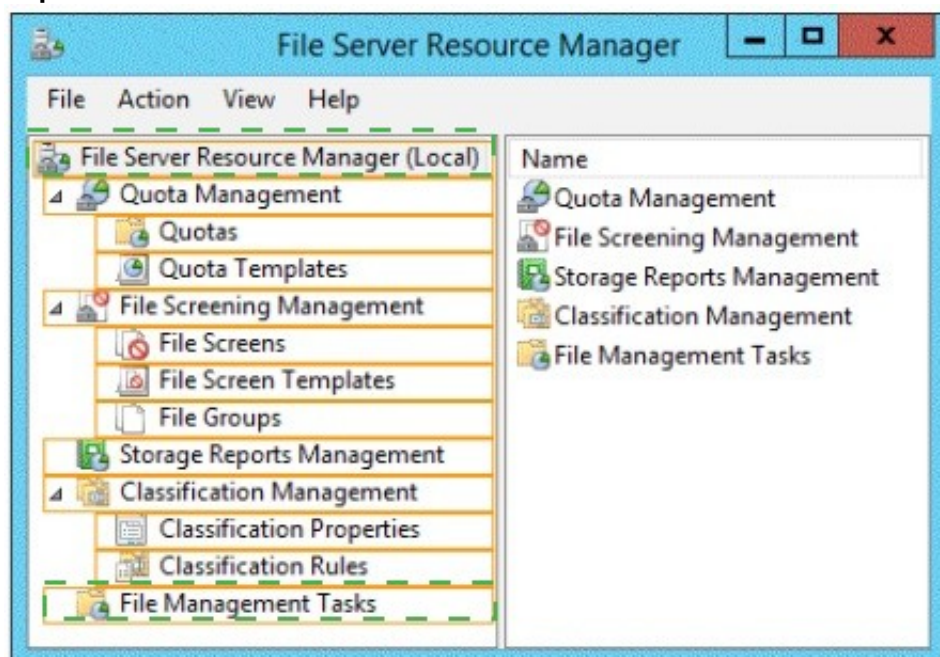
Which two nodes should you configure? To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2

- (Topic 1)

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

All of the user accounts in the marketing department are members of a group named Contoso\MarketingUsers. All of the computer accounts in the marketing department are members of a group named Contoso\MarketingComputers.

A domain user named User1 is a member of the Contoso\MarketingUsers group. A computer named Computer1 is a member of the Contoso\MarketingComputers group.

You have five Password Settings objects (PSOs). The PSOs are defined as shown in the following table.

Password setting	Directly applies to	Precedence	Minimum password length
PSO1	Contoso\Domain Users	16	14
PSO2	Contoso\MarketingUsers	20	11
PSO3	Contoso\MarketingComputers	10	12
PSO5	User1	1	10

When User1 logs on to Computer1 and attempts to change her password, she receives an error message indicating that her password is too short.

You need to tell User1 what her minimum password length is. What should you tell User1?

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

Answer: A

Explanation:

One PSO has a precedence value of 2 and the other PSO has a precedence value of 4. In this case, the PSO that has the precedence value of 2 has a higher rank and, hence, is applied to the object.

NEW QUESTION 3

- (Topic 1)

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

You have a Group Policy object (GPO) named GPO1 that contains hundreds of settings. GPO1 is linked to an organizational unit (OU) named OU1. OU1 contains 200 client computers.

You plan to unlink GPO1 from OU1.

You need to identify which GPO settings will be removed from the computers after GPO1 is unlinked from OU1.

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

- A. The managed Administrative Template settings
- B. The unmanaged Administrative Template settings
- C. The System Services security settings
- D. The Event Log security settings
- E. The Restricted Groups security settings

Answer: AD

Explanation:

There are two kinds of Administrative Template policy settings: Managed and Unmanaged . The Group Policy service governs Managed policy settings and removes a policy setting when it is no longer within scope of the user or computer.

References:

[http://technet.microsoft.com/en-us/library/cc778402\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc778402(v=ws.10).aspx) <http://technet.microsoft.com/en-us/library/bb964258.aspx>

NEW QUESTION 4

HOTSPOT - (Topic 1)

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

All DNS servers host a DNS zone named adatum.com. The adatum.com zone is not Active Directory-integrated.

An administrator modifies the start of authority (SOA) record for the adatum.com zone. After the modification, you discover that when you add or modify DNS records in the

adatum.com zone, the changes are not transferred to the DNS servers that host secondary copies of the adatum.com zone.

You need to ensure that the records are transferred to all the copies of the adatum.com zone.

What should you modify in the SOA record for the adatum.com zone? To answer, select the appropriate setting in the answer area.

The screenshot shows the 'adatum.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The 'General' sub-tab is also visible. The 'Serial number' field contains '251' with an 'Increment' button. The 'Primary server' field contains 'server1.contoso.com.' with a 'Browse...' button. The 'Responsible person' field contains 'hostmaster.contoso.com.' with a 'Browse...' button. The 'Refresh interval' is set to '15 minutes'. The 'Retry interval' is set to '10 minutes'. The 'Expires after' is set to '1 days'. The 'Minimum (default) TTL' is set to '1 hours'. The 'TTL for this record' is set to '0:1:0:0' with a format '(DDDD:HH.MM.SS)'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

When a DNS server receives an update through Active Directory replication:

If the serial number of the replicated record is higher than the serial number in the SOA record of the local copy of the zone, the local zone serial number is set to the serial number in the replicated record.

Note Each DNS record in the zone has a copy of the zone serial number at the time when the record was last modified.

If the serial number of the replicated record is the same or lower than the local serial number, and if the local DNS server is configured not to allow zone transfer of the zone, the local zone serial number is not changed.

If the serial number of the replicated record is the same or lower than the local zone serial number, if the DNS server is configured to allow a zone transfer of the zone, and if the local

zone serial number has not been changed since the last zone transfer occurred to a remote DNS server, then the local zone serial number will be incremented.

Otherwise that is if a copy of the zone with the current local zone serial number has not been transferred to a remote DNS server, the local zone serial number is not changed.

NEW QUESTION 5

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2008 R2.

You plan to test Windows Server 2012 R2 by using native-boot virtual hard disks (VHDs). You attach a new VHD to Server1.

You need to install Windows Server 2012 R2 in the VHD. What should you do?

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

Answer: B

Explanation:

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

NEW QUESTION 6

HOTSPOT - (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains servers named Server1 and Server2. Both servers have the DFS

Replication role service installed.
You need to configure the DFS Replication environment to meet the following requirements:
? Increase the quota limit of the staging folder.
? Configure the staging folder cleanup process to provide the highest amount of free space possible.
Which cmdlets should you use to meet each requirement? To answer, select the appropriate options in the answer area.

Answer Area

Increase the quota limit of the staging folder.

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

Answer Area

Increase the quota limit of the staging folder.

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Increase the quota limit of the staging folder.

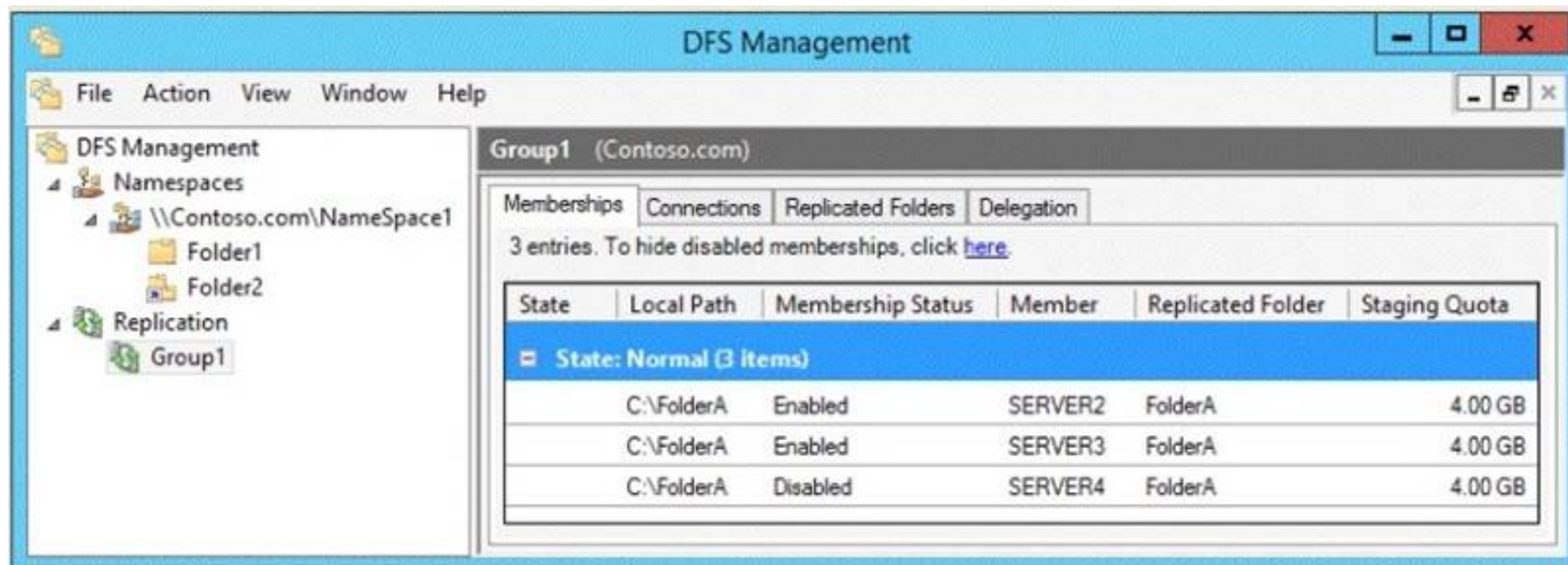
Set-DfsrGroupSchedule
Set-DfsrMembership
Set-DfsrReplicatedFolder
Set-DfsrServiceConfiguration

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

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

NEW QUESTION 7

HOTSPOT - (Topic 1)
Your network contains an Active Directory domain named contoso.com. The domain contains three servers named Server2, Server3, and Server4. Server2 and Server4 host a Distributed File System (DFS) namespace named Namespace1.
You open the DFS Management console as shown in the exhibit. (Click the Exhibit button.)



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

Answer Area

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

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

Answer Area

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 8

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs.

The domain is renamed to adatum.com. Group Policies no longer function correctly.

You need to ensure that the existing GPOs are applied to users and computers. You want to achieve this goal by using the minimum amount of administrative effort.

What should you use?

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

Answer: C

Explanation:

You can use the gpfixup command-line tool to fix the dependencies that Group Policy objects (GPOs) and Group Policy links in Active Directory Domain Services (AD DS) have on Domain Name System (DNS) and NetBIOS names after a domain rename operation.

Reference: [http://technet.microsoft.com/en-us/library/hh852336\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/hh852336(v=ws.10).aspx)

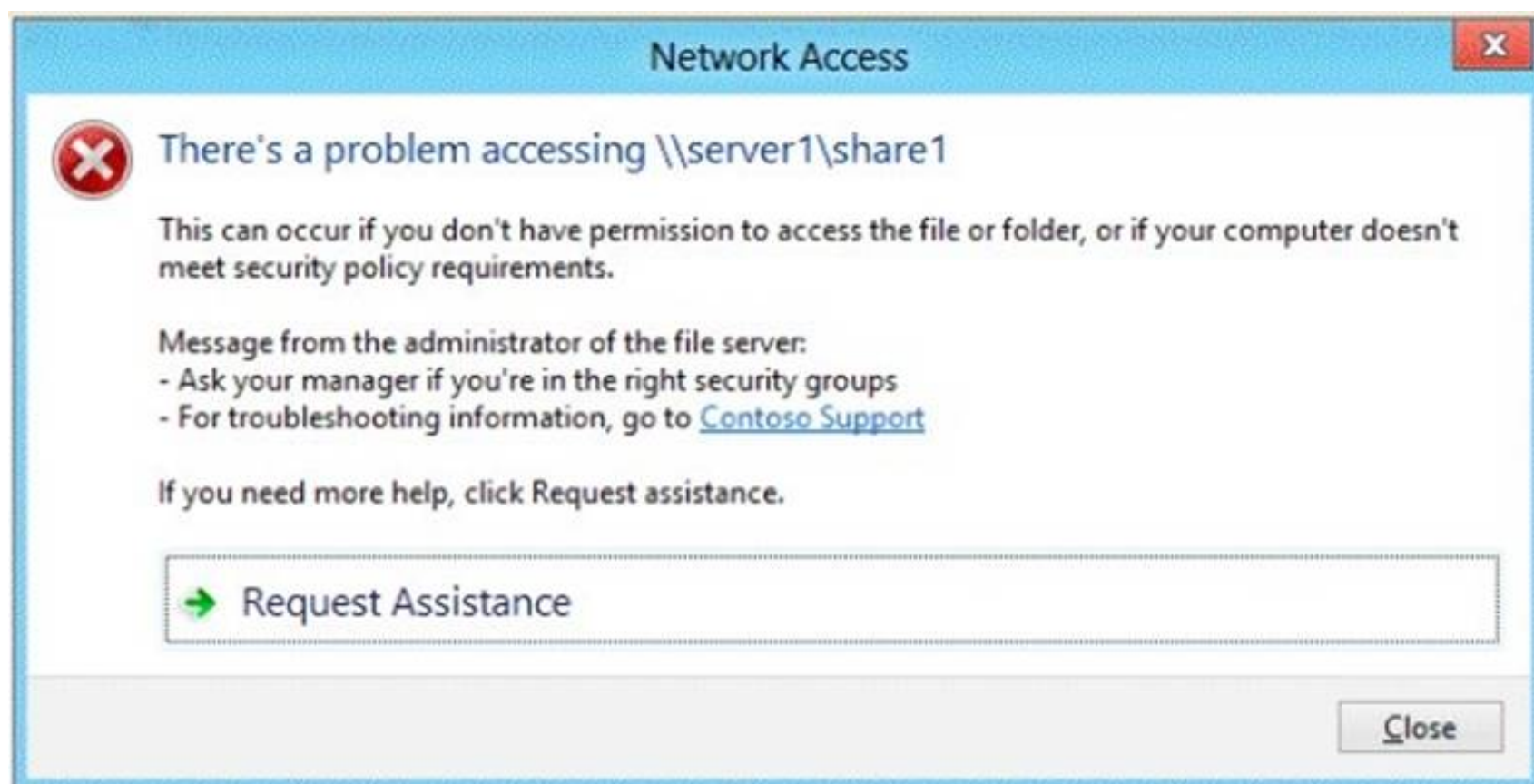
NEW QUESTION 9

- (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.)



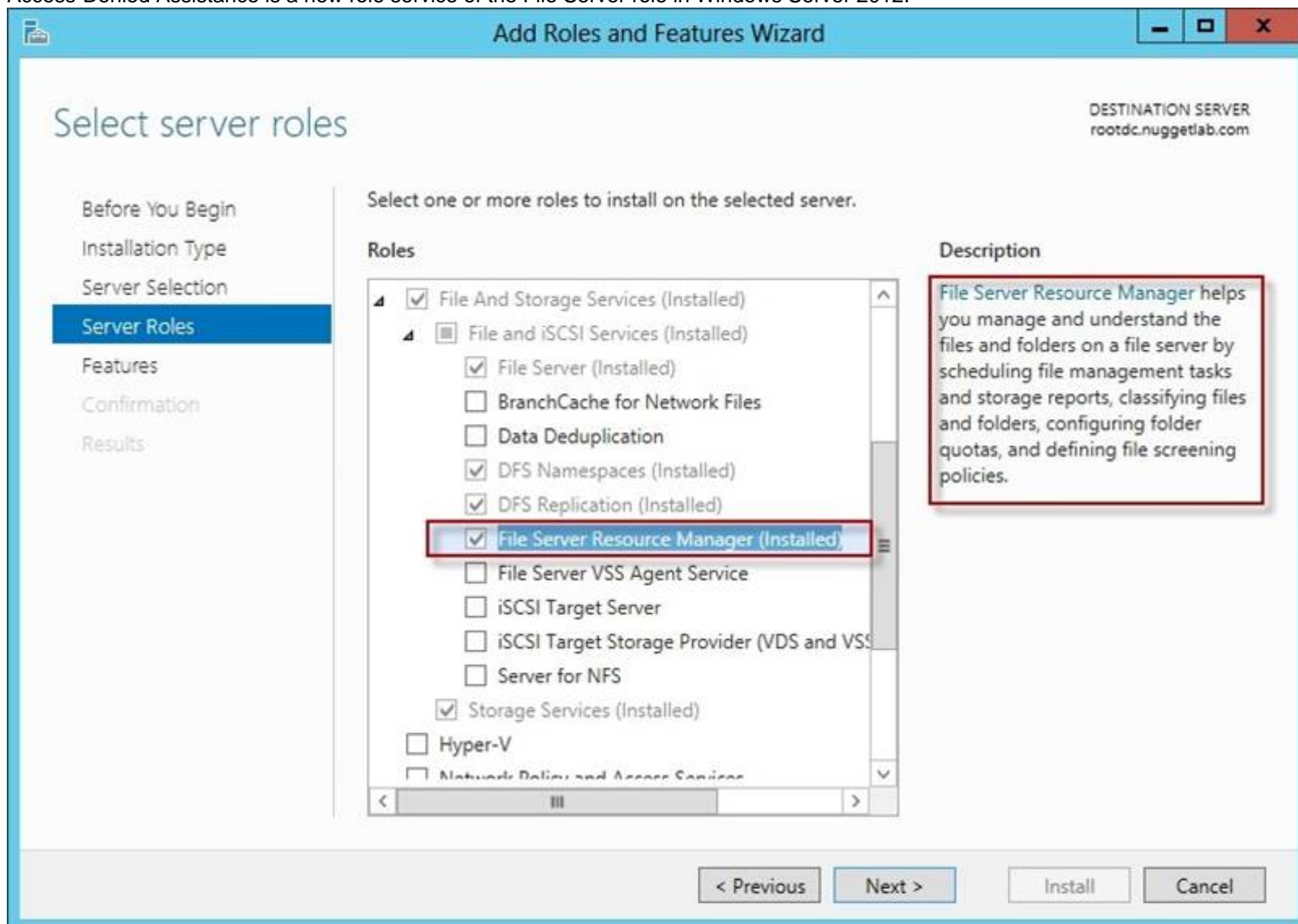
You deploy a new file server named Server2 that runs Windows Server 2012 R2.
You need to configure Server2 to display the same custom Access Denied message as Server1.
What should you install on Server2?

- 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.

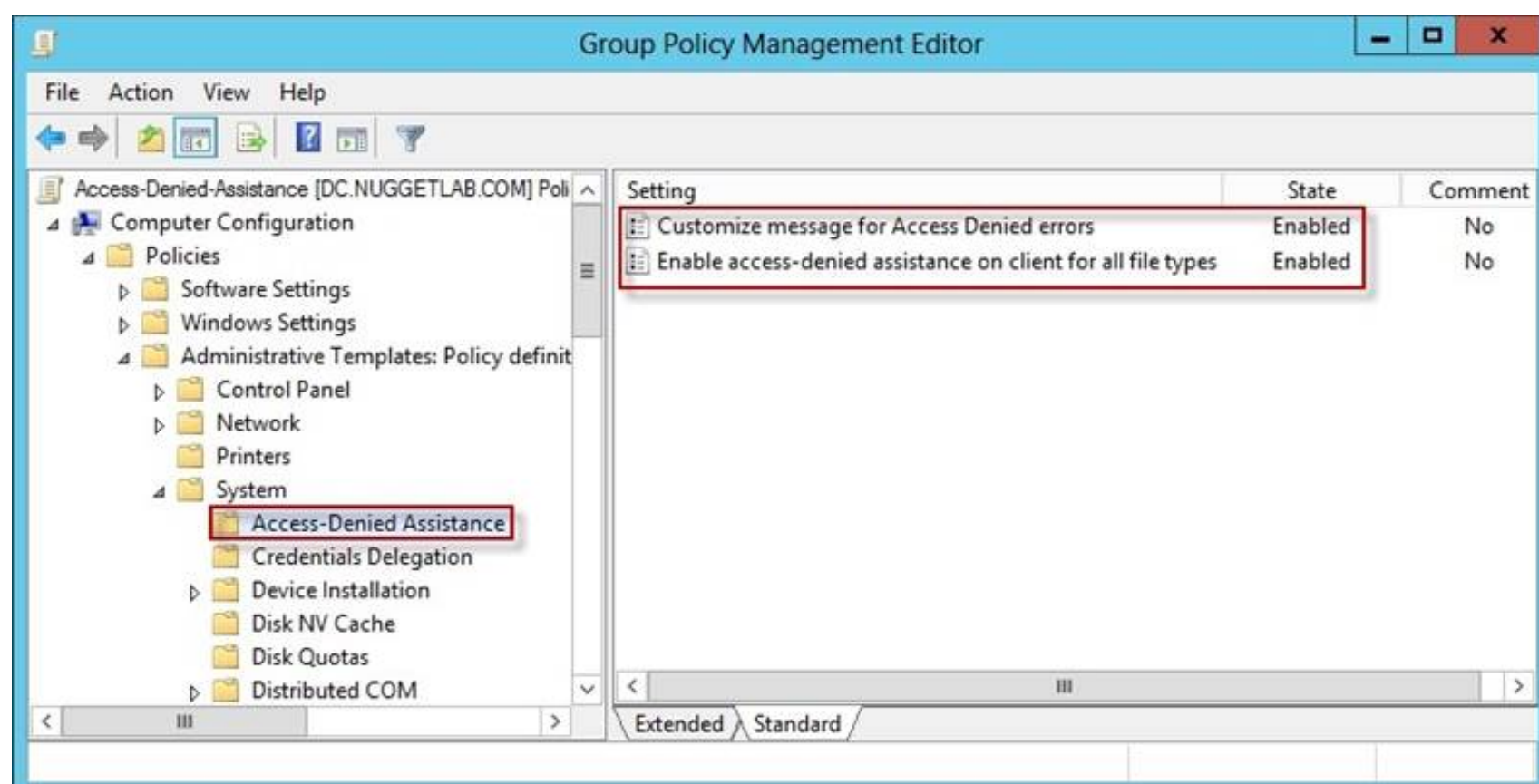
Because Access-Denied Assistance relies up on e-mail notifications, we also need to configure each relevant file server with a Simple Mail Transfer Protocol (SMTP) server address. Let's do that quickly with Windows PowerShell:

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

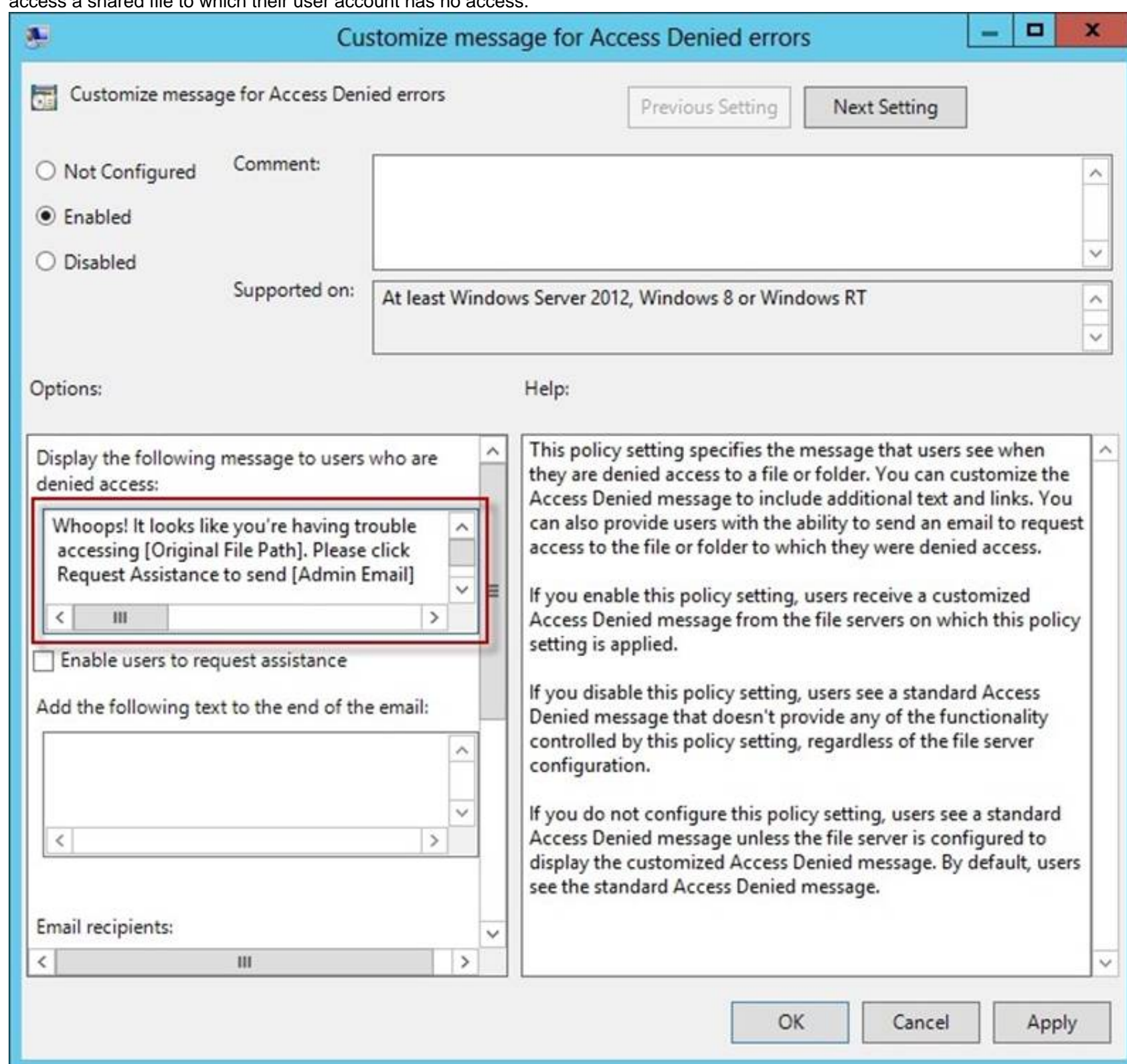
You can enable Access-Denied Assistance either on a per-server basis or centrally via Group Policy. To my mind, the latter approach is infinitely preferable from an administration standpoint.

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.

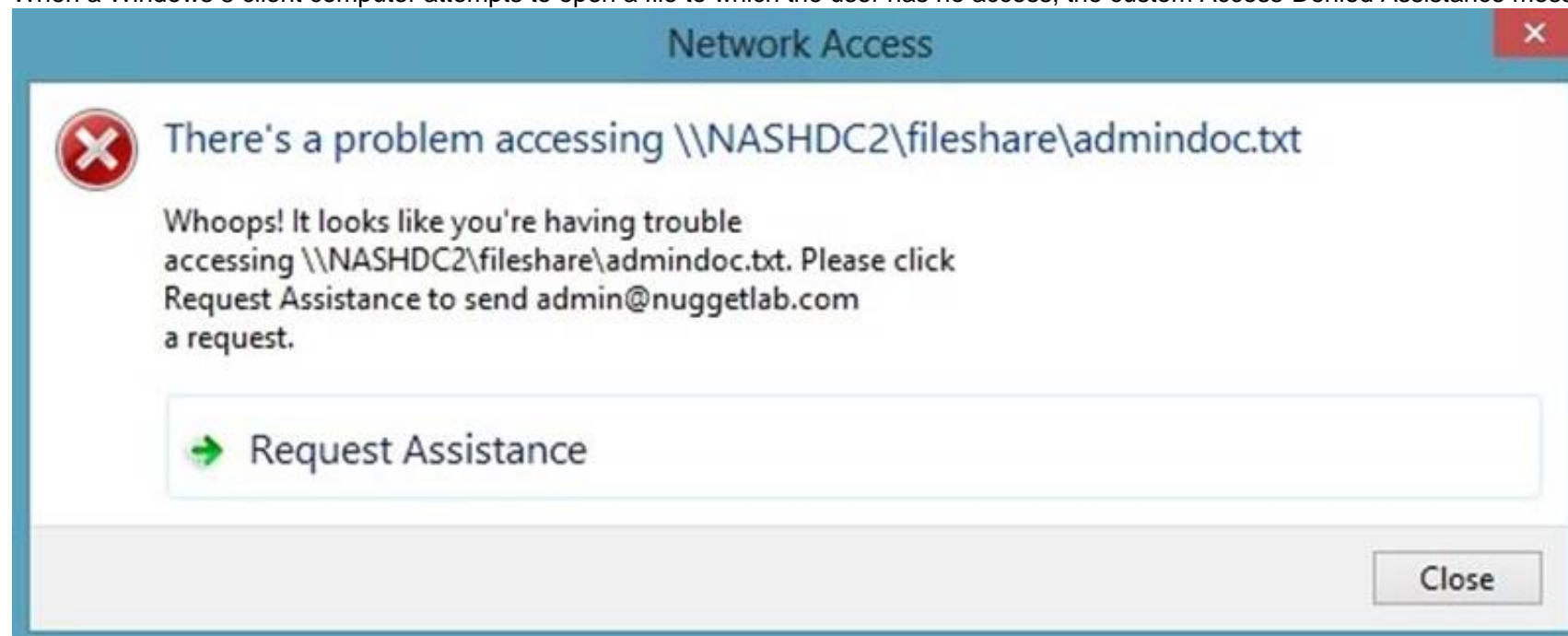
For instance, we can insert pre-defined macros to swap in the full path to the target file, the administrator e-mail address, and so forth. See this example: Whoops! It looks like you're having trouble accessing [Original File Path]. Please click Request Assistance to send [Admin Email] a help request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

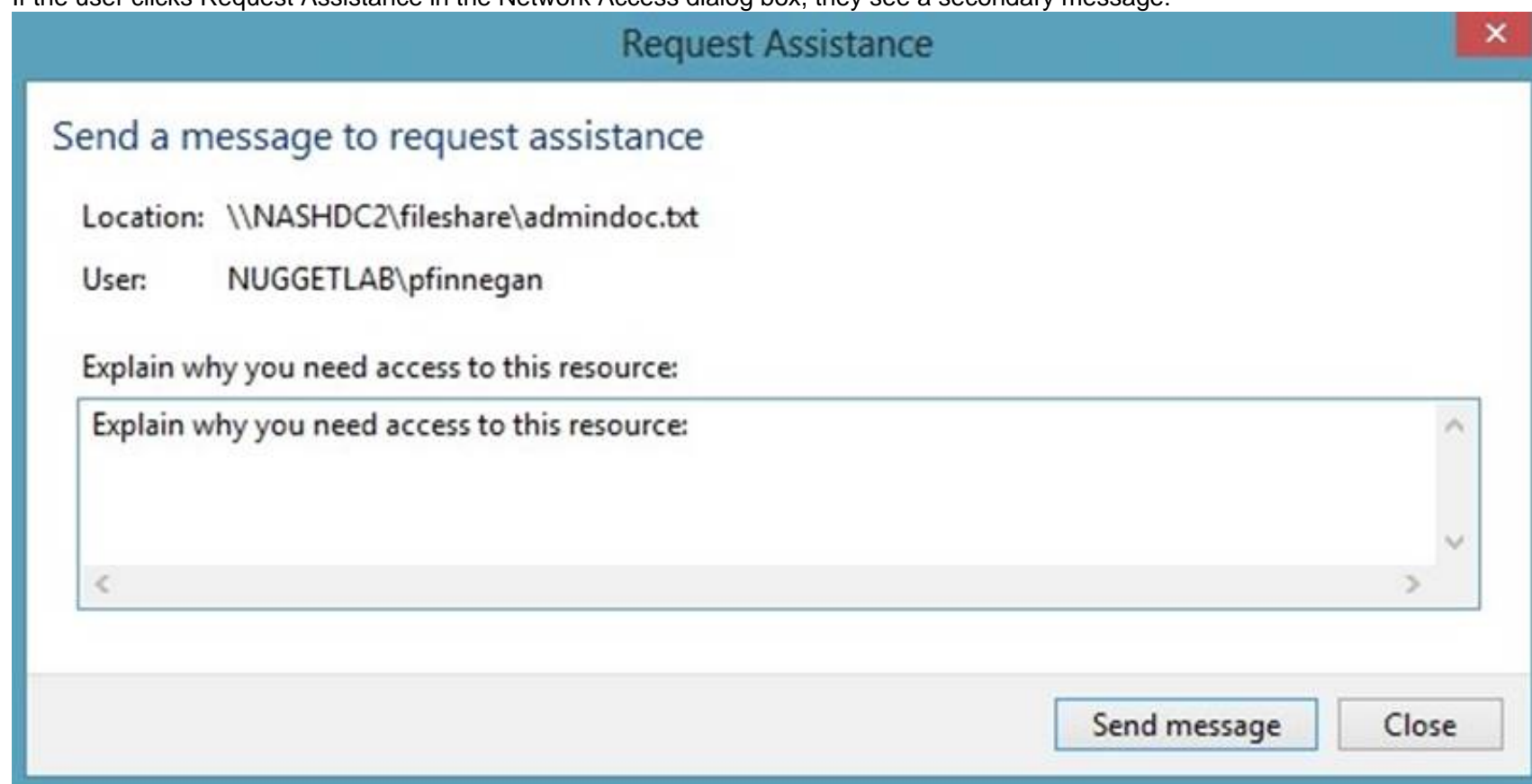
The Enable access-denied assistance on client for all file types policy should be enabled to force client computers to participate in Access-Denied Assistance. Again, you must make sure to target your GPO scope accordingly to "hit" your domain workstations as well as your Windows Server 2012 file servers.

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 10

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a Web server named www.contoso.com. The Web server is available on the Internet.

You implement DirectAccess by using the default configuration.

You need to ensure that users never attempt to connect to www.contoso.com by using DirectAccess. The solution must not prevent the users from using DirectAccess to access other resources in contoso.com.

Which settings should you configure in a Group Policy object (GPO)?

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

Answer: C

Explanation:

For DirectAccess, the NRPT must be configured with the namespaces of your intranet with a leading dot (for example, internal.contoso.com or .corp.contoso.com). For a DirectAccess client, any name request that matches one of these namespaces will be sent to the specified intranet Domain Name System (DNS) servers.

Include all intranet DNS namespaces that you want DirectAccess client computers to access.

There are no command line methods for configuring NRPT rules. You must use Group Policy settings. To configure the NRPT through Group Policy, use the Group Policy add-in at Computer Configuration \Policies\Windows Settings\Name Resolution Policy in the Group Policy object for DirectAccess clients. You can create a new NRPT rule and edit or delete existing rules. For more information, see Configure the NRPT with Group Policy.

NEW QUESTION 10

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a read-only domain controller (RODC) named R0DC1.

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 R0DC1. The solution must not provide RODC_Admins with the ability to manage Active Directory objects.

What should you do?

- A. From Active Directory Sites and Services, run the Delegation of Control Wizard.
- B. From a command prompt, run the dsadd computer command.
- C. From Active Directory Site and Services, configure the Security settings of the R0DC1 server object.
- D. From a command prompt, run the dsmgmt local roles command.

Answer: D

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 13

- (Topic 1)

You have a server named WSUS1 that runs Windows Server 2012 R2. WSUS1 has the Windows Server Update Services server role installed and has one volume.

You add a new hard disk to WSUS1 and then create a volume on the hard disk.

You need to ensure that the Windows Server Update Services (WSUS) update files are stored on the new volume.

What should you do?

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

Answer: D

Explanation:

Local Storage Considerations

If you decide to store update files on your server, the recommended minimum disk size is 30 GB. However, depending on the synchronization options you specify, you might need to use a larger disk. For example, when specifying advanced synchronization options, as in the following procedure, if you select options to download multiple languages and/or the option to download express installation files, your server disk can easily reach 30 GB. Therefore if you choose any of these options, install a larger disk (for example, 100 GB).

If your disk gets full, you can install a new, larger disk and then move the update files to the new location. To do this, after you create the new disk drive, you will need to run the WSUSutil.exetool (with the movecontent command) to move the update files to the new disk. For this procedure, see Managing WSUS from the Command Line.

For example, if D:\WSUS1 is the new path for local WSUS update storage, D:\move. log is the path to the log file, and you wanted to copy the old files to the new location, you would type: wsusutil.exe movecontent D:\WSUS1\ D:\move. Log.

Note: If you do not want to use WSUSutil.exe to change the location of local WSUS update storage, you can also use NTFS functionality to add a partition to the current location of local WSUS update storage. For more information about NTFS, go to Help and Support Center in Windows Server 2003.

Syntax

At the command line %drive%\Program Files\Update Services\Tools>, type: wsusutilmovecontentcontentpathlogfile -skipcopy [/?]

The parameters are defined in the following table.

contentpath - the new root for content files. The path must exist. logfile - the path and file name of the log file to create.

-skipcopy - indicates that only the server configuration should be changed, and that the content files should not be copied.

/help or /? - displays command-line help for movecontent command.

References:

<http://blogs.technet.com/b/sus/archive/2008/05/19/wsus-how-to-change-the-location-where-wsus-stores-updates-locally.aspx>

[http://technet.microsoft.com/en-us/library/cc720475\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc720475(v=ws.10).aspx)

<http://technet.microsoft.com/en-us/library/cc708480%28v=ws.10%29.aspx> [http://technet.microsoft.com/en-us/library/cc720466\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc720466(v=ws.10).aspx)

<http://technet.microsoft.com/en-us/library/cc708480%28v=ws.10%29.aspx>

NEW QUESTION 16

- (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 and has the Network Policy Server role service installed.

An administrator creates a RADIUS client template named Template1. You create a RADIUS client named Client1 by using Template 1.

You need to modify the shared secret for Client1. What should you do first?

- A. Configure the Advanced settings of Template1.
- B. Set the Shared secret setting of Template1 to Manual.
- C. Clear Enable this RADIUS client for Client1.
- D. Clear Select an existing template for Client1.

Answer: D

Explanation:

Clear checkmark for Select an existing template in the new client wizard. In New RADIUS Client, in Shared secret, do one of the following:

Bullet Ensure that Manual is selected, and then in Shared secret, type the strong password that is also entered on the RADIUS client. Retype the shared secret in Confirm shared secret.

New RADIUS Client

Settings

Advanced

☒ Enable this RADIUS client

☒ Select an existing template:

Template 1

Name and Address

Friendly name:

Client 1

Address (IP or DNS):

192.168.1.1

Verify...

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual☐ Generate

Shared secret:

...

Confirm shared secret:

...

OK

Cancel

NEW QUESTION 21

- (Topic 1)

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

Server1 has the 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 22

- (Topic 1)

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

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

You need to ensure that end-to-end encryption is used between clients and Server2 when the clients connect to the network by using DirectAccess.

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

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

Answer: BE

Explanation:

Unsure about these answers:

? A public key infrastructure must be deployed.

? Windows Firewall must be enabled on all profiles.

? ISATAP in the corporate network is not supported. If you are using ISATAP, you should remove it and use native IPv6.

? Computers that are running the following operating systems are supported as DirectAccess clients:

Windows Server® 2012 R2

Windows 8.1 Enterprise

Windows Server® 2012

Windows 8 Enterprise Windows Server® 2008 R2 Windows 7 Ultimate

Windows 7 Enterprise

? Force tunnel configuration is not supported with KerbProxy authentication.

? Changing policies by using a feature other than the DirectAccess management console or Windows PowerShell cmdlets is not supported.

? Separating NAT64/DNS64 and IPHTTPS server roles on another server is not supported.

NEW QUESTION 24

- (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 26

HOTSPOT - (Topic 1)

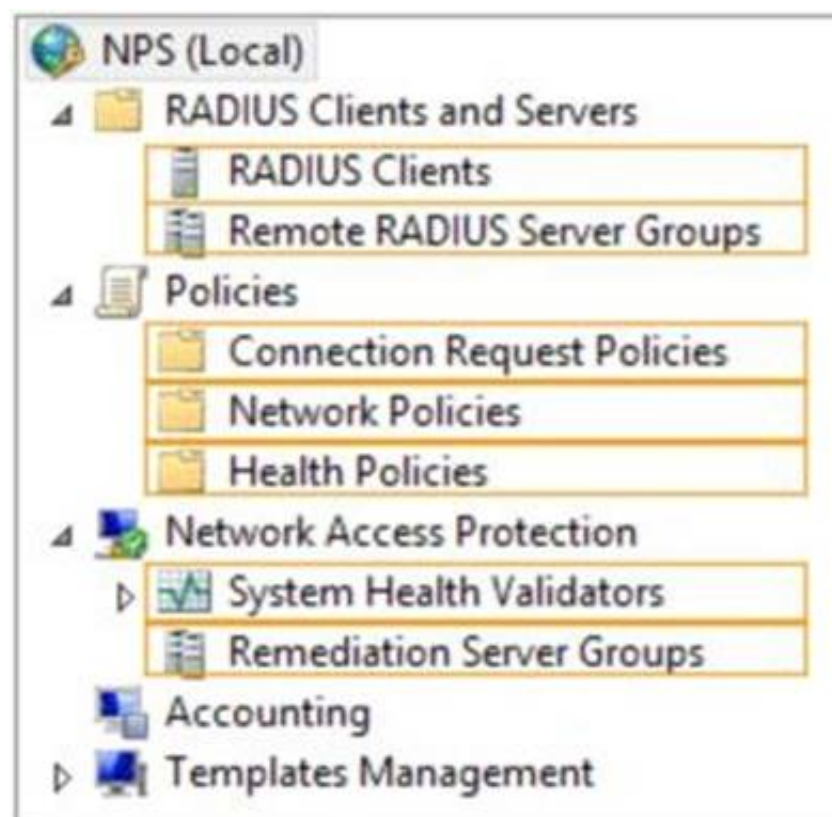
Your network contains a RADIUS server named Server1.

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.

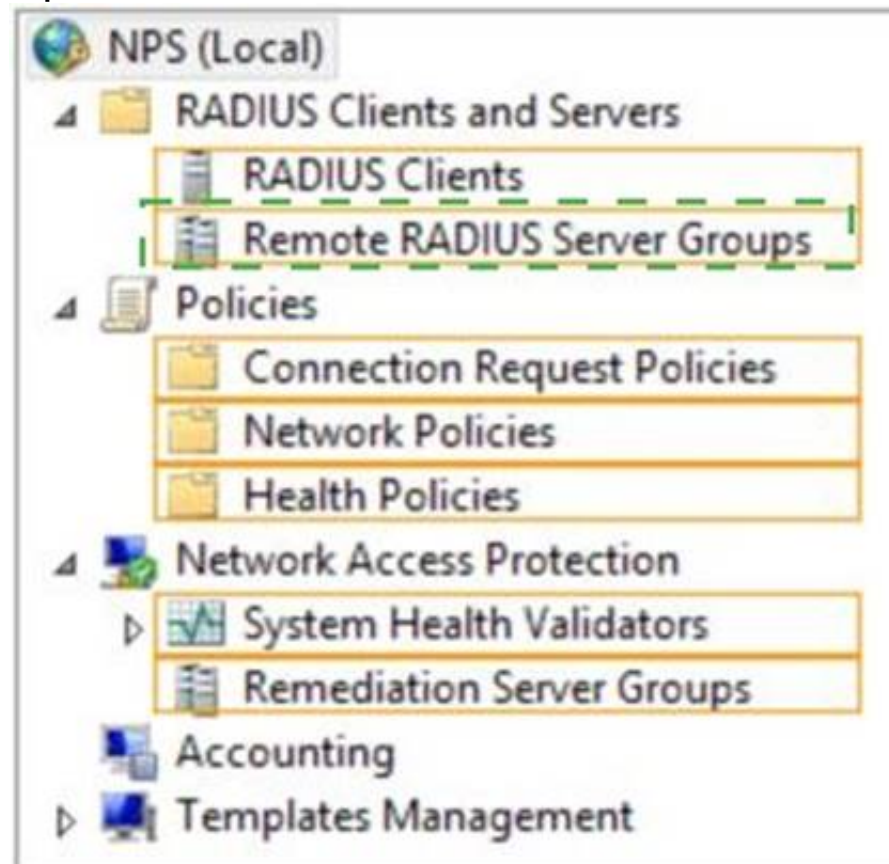
What else should you configure on Server2? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



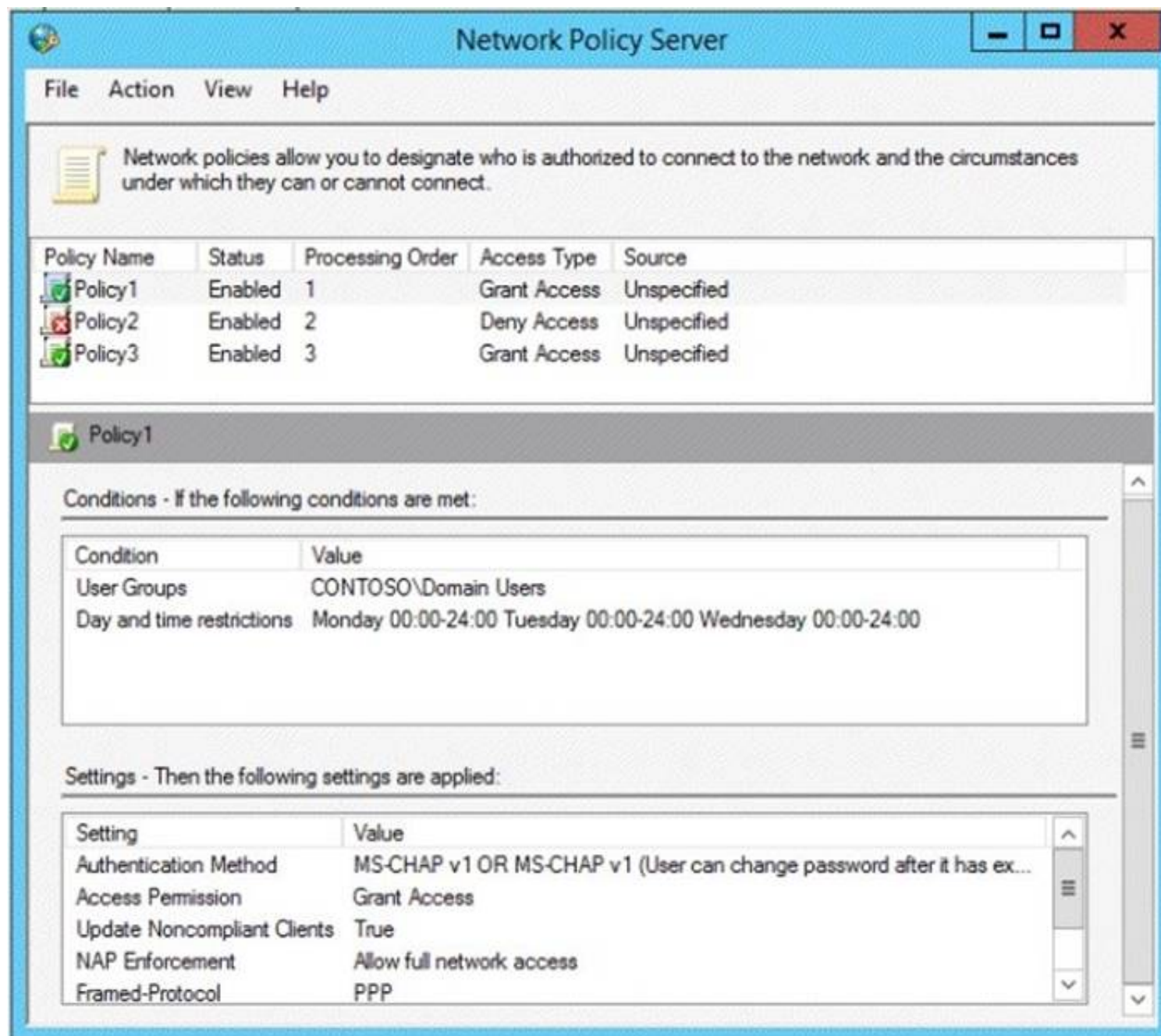
NEW QUESTION 28

HOTSPOT - (Topic 1)

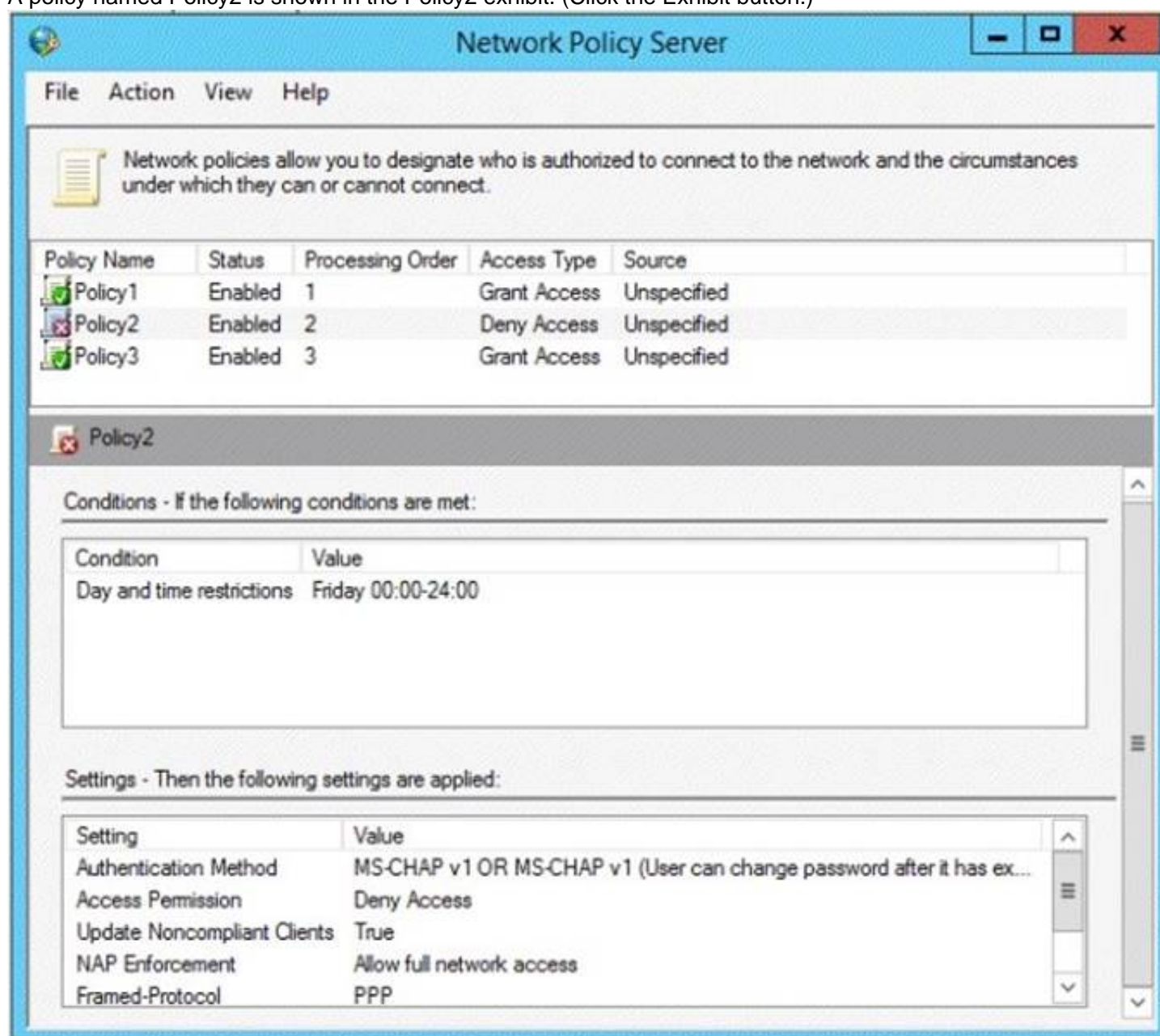
Your network contains an Active Directory named contoso.com. You have users named User1 and user2.

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.

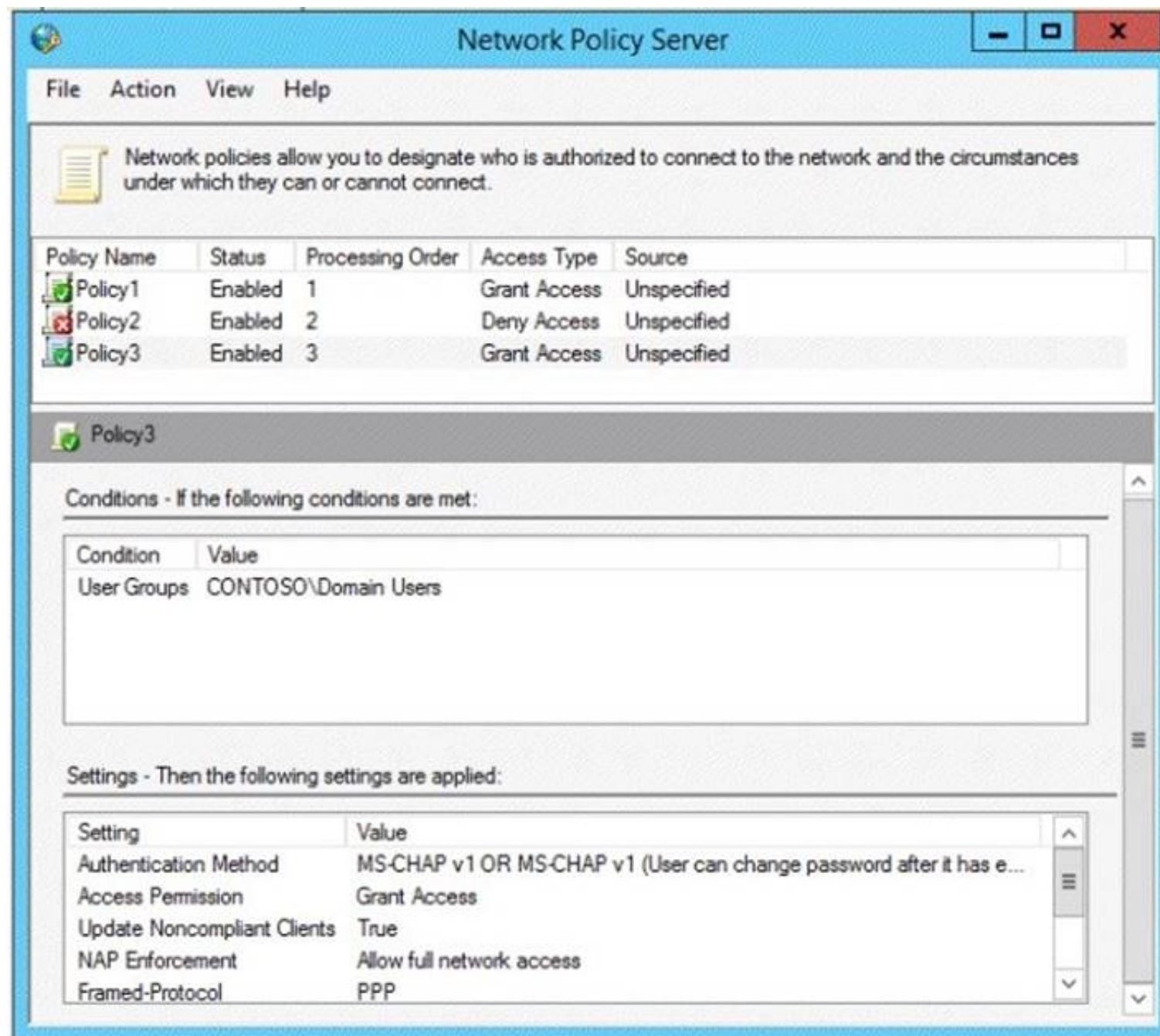
A policy named Policy1 is shown in the Policy1 exhibit. (Click the Exhibit button.)



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 33

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.

You create an Active Directory snapshot of DC1 each day.

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 34

- (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.

Server1 has a folder named Folder1 that is used by the human resources department. You need to ensure that an email notification is sent immediately to the human resources

manager when a user copies an audio file or a video file to Folder1.

What should you configure on Server1?

- A. a storage report task
- B. a file screen exception
- C. a file screen
- D. a file group

Answer: C

Explanation:

Create file screens to control the types of files that users can save, and generate notifications when users attempt to save unauthorized files.

With File Server Resource Manager (FSRM) you can create file screens that prevent users

from saving unauthorized files on volumes or folders. File Screen Enforcement:

You can create file screens to prevent users from saving unauthorized files on volumes or folders. There are two types of file screen enforcement: active and passive enforcement. Active file screen enforcement does not allow the user to save an unauthorized file. Passive file screen enforcement allows the user to save the file, but notifies the user that the file is not an authorized file. You can configure notifications, such as events logged to the event log or e-mails sent to users and administrators, as part of active and passive file screen enforcement.

NEW QUESTION 38

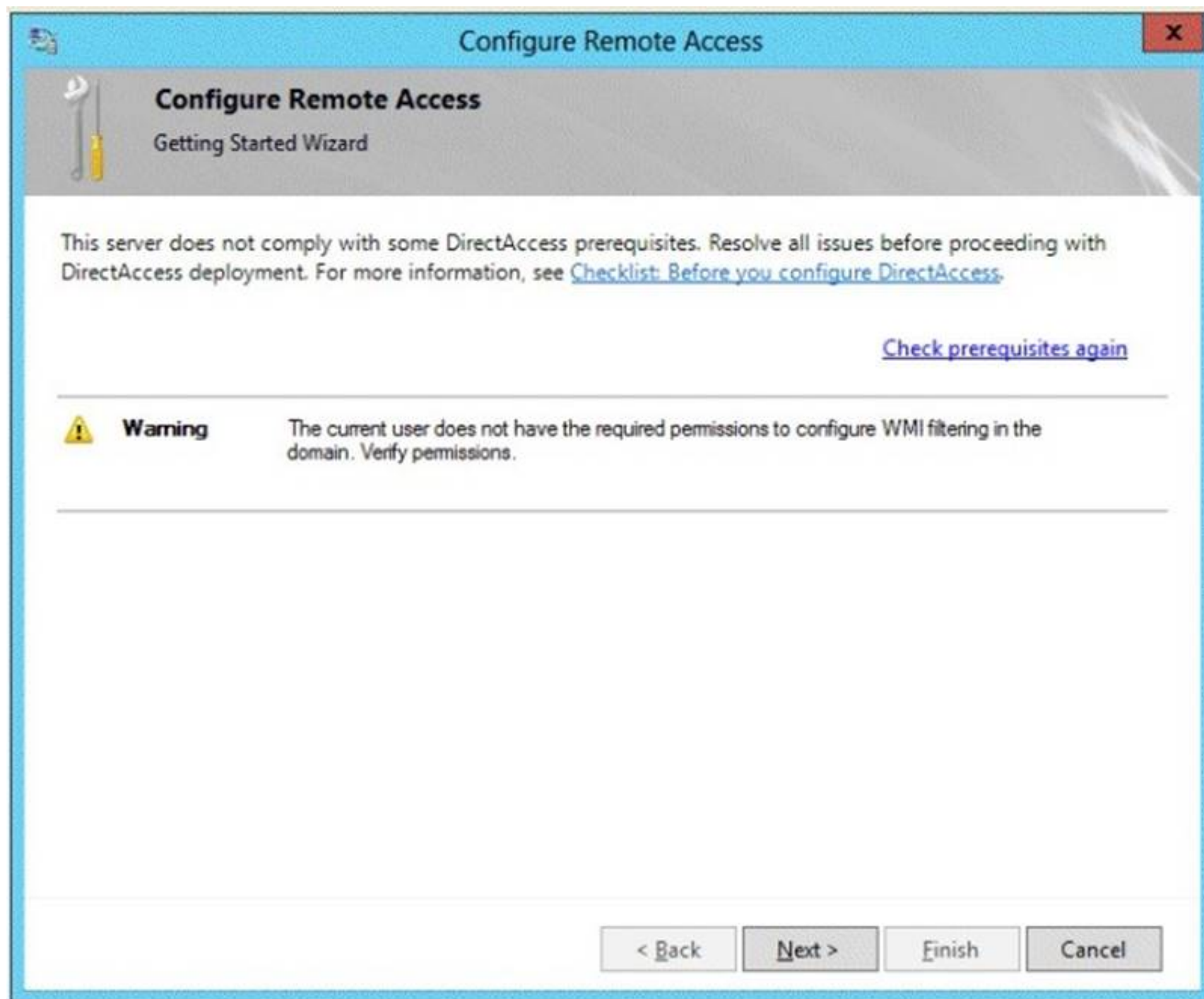
- (Topic 1)

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

Server1 has the Remote Access server role installed.

You log on to Server1 by using a user account named User2.

From the Remote Access Management Console, you run the Getting Started Wizard and you receive a warning message as shown in the exhibit. (Click the Exhibit button.)



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

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

Answer: B

Explanation:

You must have privileges to create WMI filters in the domain in which you want to create the filter. Permissions can be changed by adding a user to the Administrators group.

Administrators (A built-in group)

After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group. The Administrators group has built-in capabilities that give its members full control over the system. The group is the default owner of any object that is created by a member of the group.

This example logs in as a test user who is not a domain user or an administrator on the server. This results in the error specifying that DA can only be configured by a user with local administrator permissions.

References:

[http://technet.microsoft.com/en-us/library/cc780416\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc780416(v=ws.10).aspx) [http://technet.microsoft.com/en-us/library/cc775497\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc775497(v=ws.10).aspx)

NEW QUESTION 42

- (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.

Each time a user receives an access-denied message after attempting to access a folder on Server1, an email notification is sent to a distribution list named DL1.

You create a folder named Folder1 on Server1, and then you configure custom NTFS permissions for Folder1.

You need to ensure that when a user receives an access-denied message while attempting to access Folder1, an email notification is sent to a distribution list named DL2. The solution must not prevent DL1 from receiving notifications about other access-denied messages.

What should you do?

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

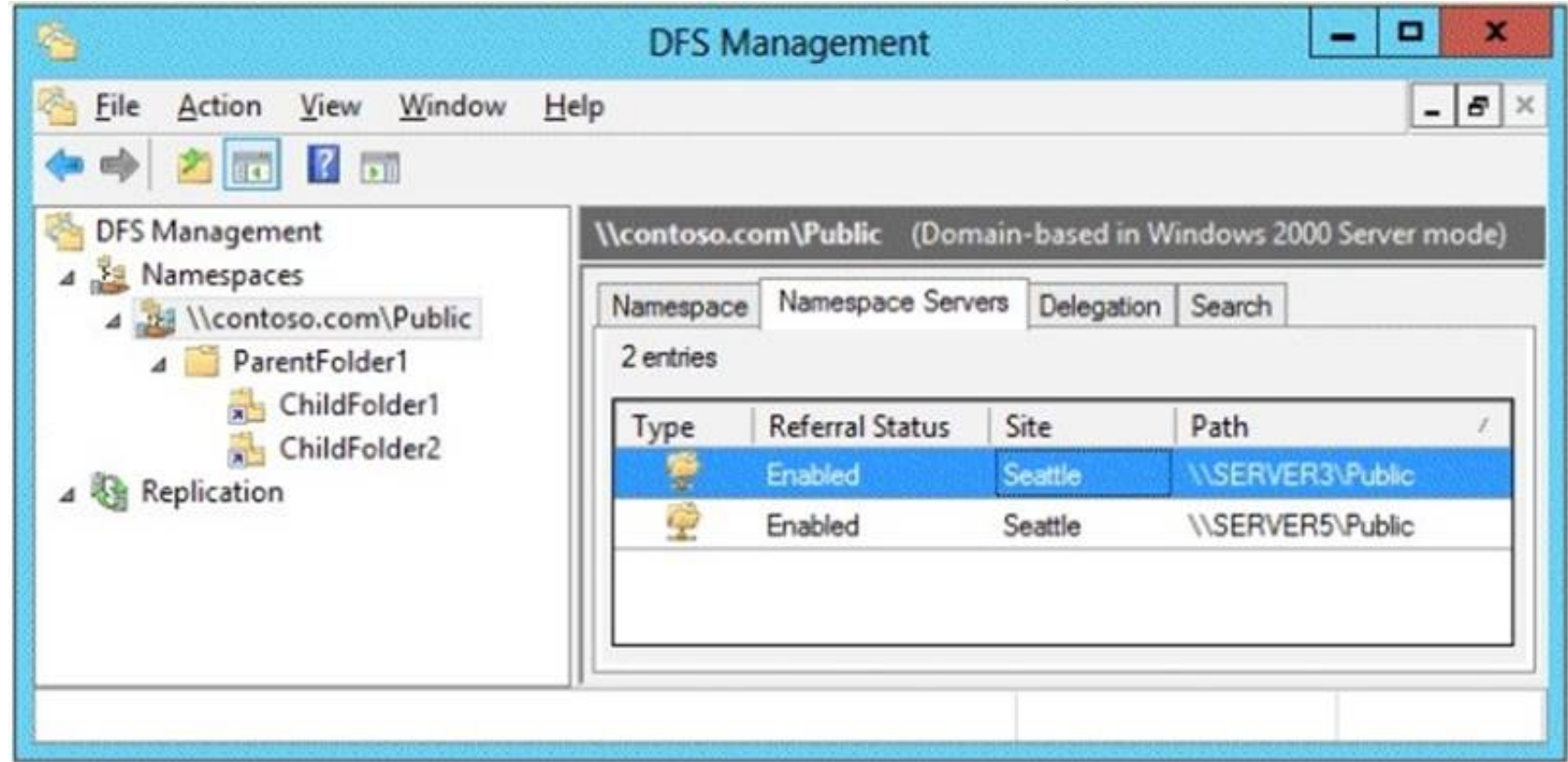
Answer: A

Explanation:

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

NEW QUESTION 47

- (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 49

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

Network policy Properties

Overview | Conditions | Constraints | Settings

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

Settings:

RADIUS Attributes

Standard
Vendor Specific

Network Access Protection

NAP Enforcement

Extended State

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

Specify whether you want to enforce Network Access Protection for this policy.

☒ Allow full network access
Allows unrestricted network access for clients when the connection request matches the policy. Use this option for reporting mode.

☐ Allow full network access for a limited time
Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date: 6/1/2007 Time: 12:00:00 PM

☐ Allow limited access
Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL
To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

Configure...

Auto remediation

☒ Enable auto-remediation of client computers
Automatically remediate computers that do not meet health requirements defined in this policy.

OK Cancel Apply

Network Policy Server

File Action View Help

NPS (Local)

RADIUS Clients and Servers

RADIUS Clients

Remote RADIUS Server Group

Policies

Connection Request Policies

Network Policies

Health Policies

Network Access Protection

System Health Validators

Remediation Server Group

Accounting

System Health Validators allow SHVs, configure the SHVs and

Name

Windows Security Health Validator

Windows Security Health Validator

Status - Configured

Error Code Configurations:

SHV unable to contact required services

SHA unable to contact required services

SHA not responding to NAP Client

SHV not responding

Vendor specific error code received

Windows Security Health Validator Properties

Settings

To open and configure the system health validator program, click Configure.

Configure...

Error code resolution

Select how to resolve the following error codes that may be returned for this system health validator and its associated system health agent when a client requests network access.

SHV unable to contact required services Noncompliant

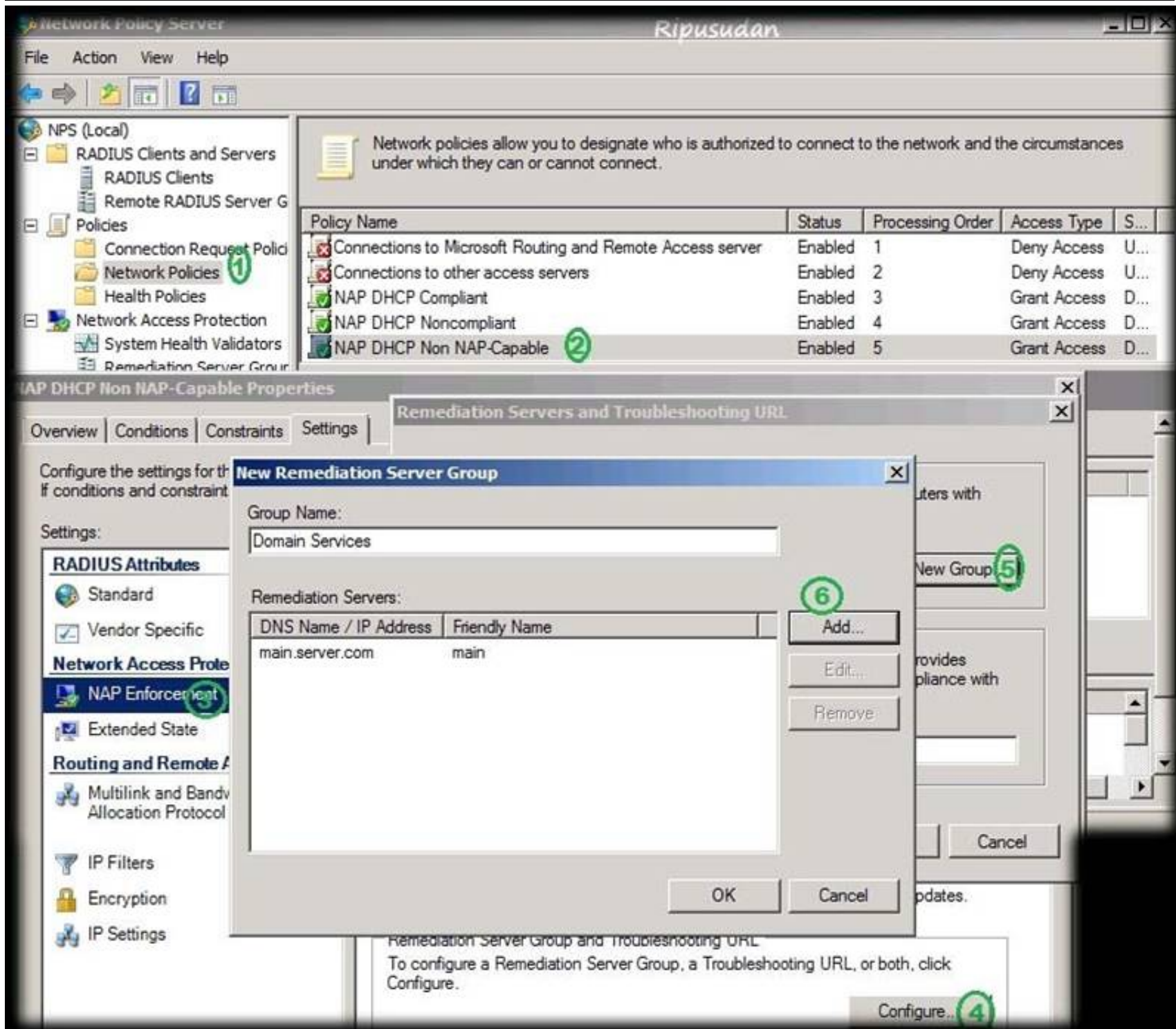
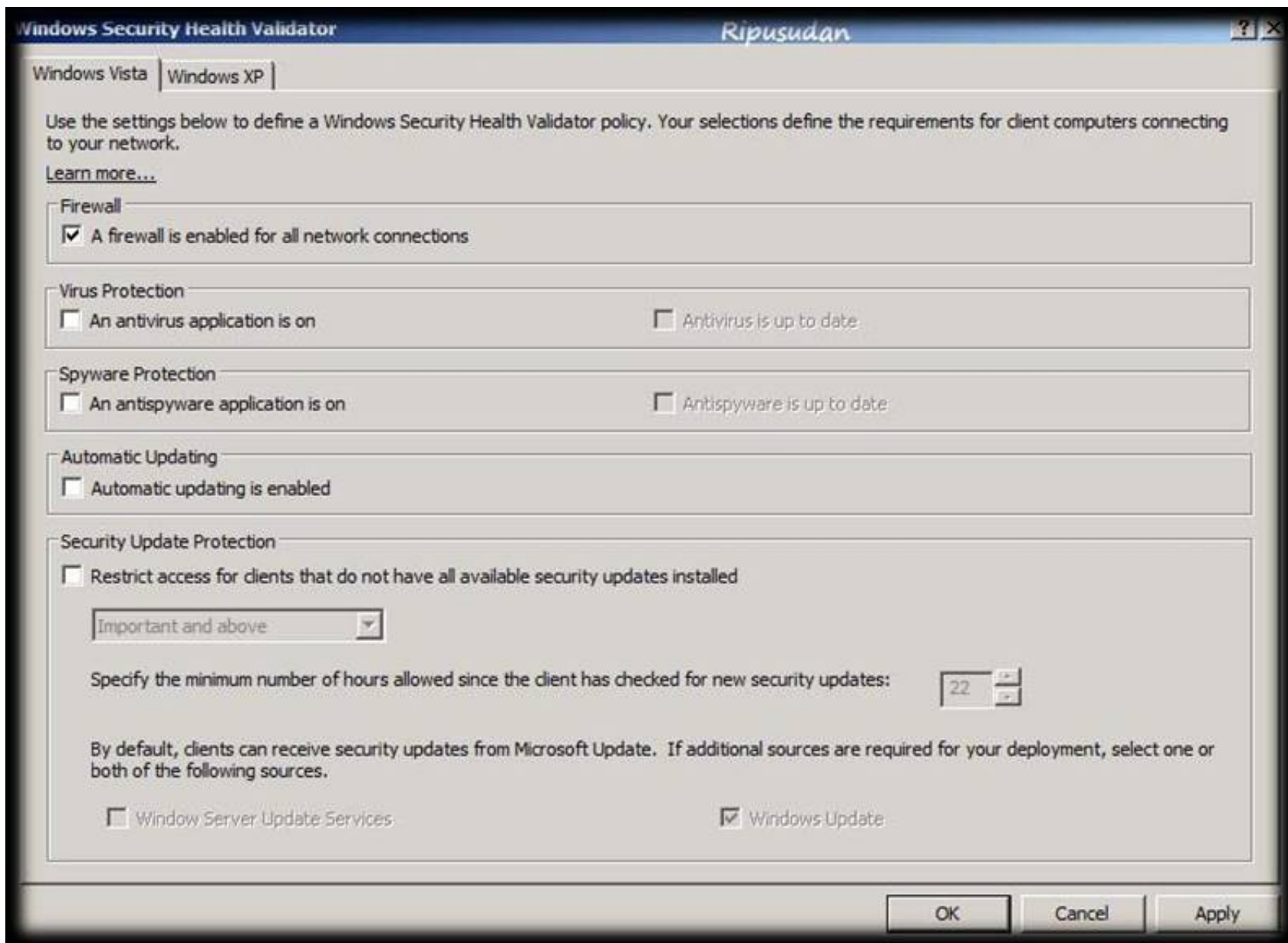
SHA unable to contact required services Noncompliant

SHA not responding to NAP Client Noncompliant

SHV not responding Noncompliant

Vendor specific error code received Noncompliant

OK Cancel Apply



* 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 52

- (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 53

DRAG DROP - (Topic 1)

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

A partner company has an Active Directory forest named adatum.com. The adatum.com forest contains an NPS server named NPS2.

You plan to grant users from adatum.com VPN access to your network. You need to authenticate the users from adatum.com on VPN1.

What should you create on each NPS server?

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

Objects	Answer Area
a connection request policy	NPS1: Object
a network policy	Object
a RADIUS client	
a remote RADIUS server group	NPS2: Object

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Objects	Answer Area
a connection request policy	NPS1: a connection request policy
a network policy	a remote RADIUS server group
a RADIUS client	
a remote RADIUS server group	NPS2: a RADIUS client

NEW QUESTION 55

- (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 56

- (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>

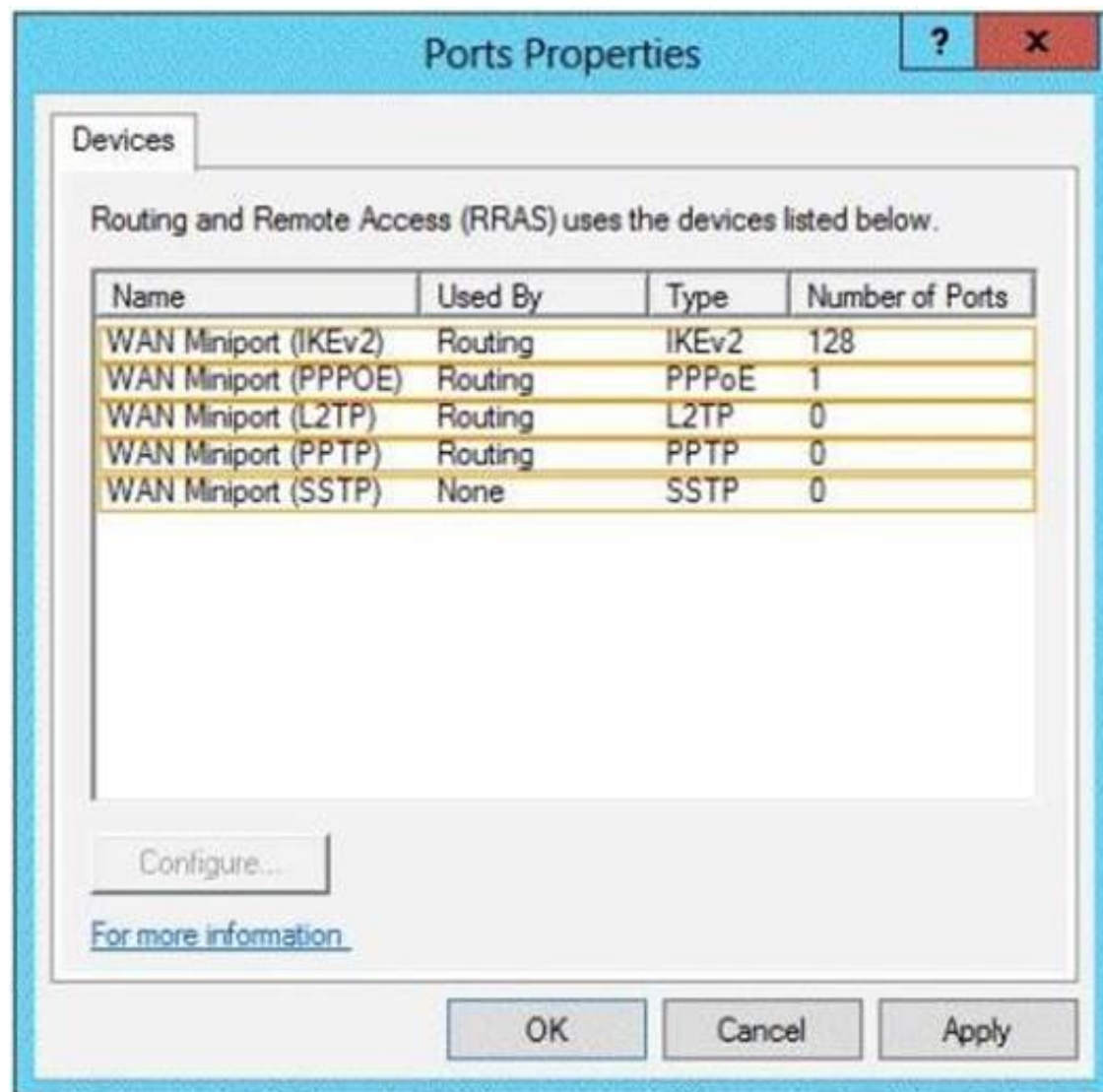
NEW QUESTION 61

HOTSPOT - (Topic 1)

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 by using TCP port 443.

What should you modify? To answer, select the appropriate object in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

[http://technet.microsoft.com/en-us/library/cc771298\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx)

Secure Socket Tunneling Protocol (SSTP) is a new tunneling protocol that uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls and Web proxies that might block PPTP and L2TP/IPsec traffic.

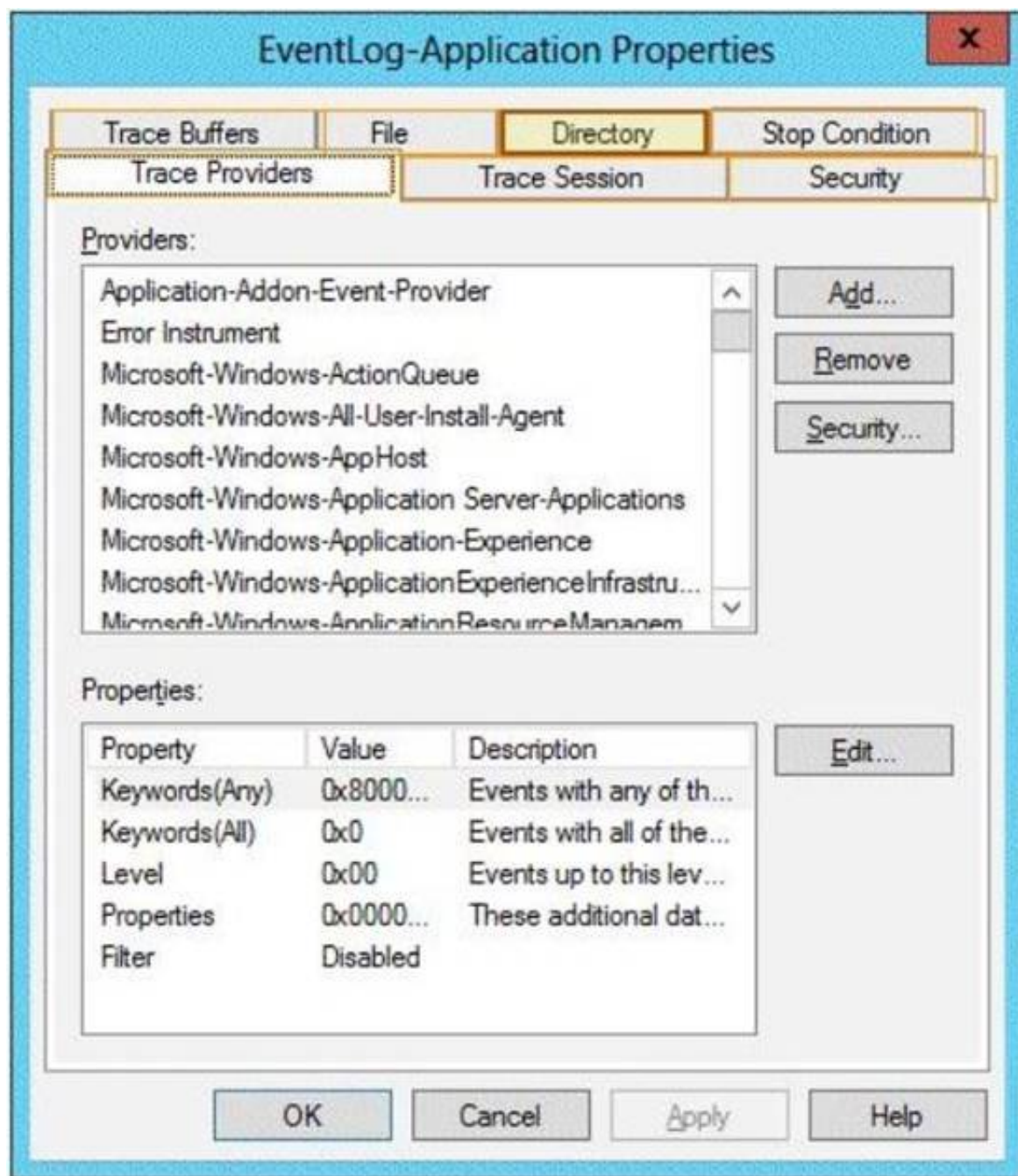
NEW QUESTION 64

HOTSPOT - (Topic 1)

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

You enable the EventLog-Application event trace session.

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 69

- (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.

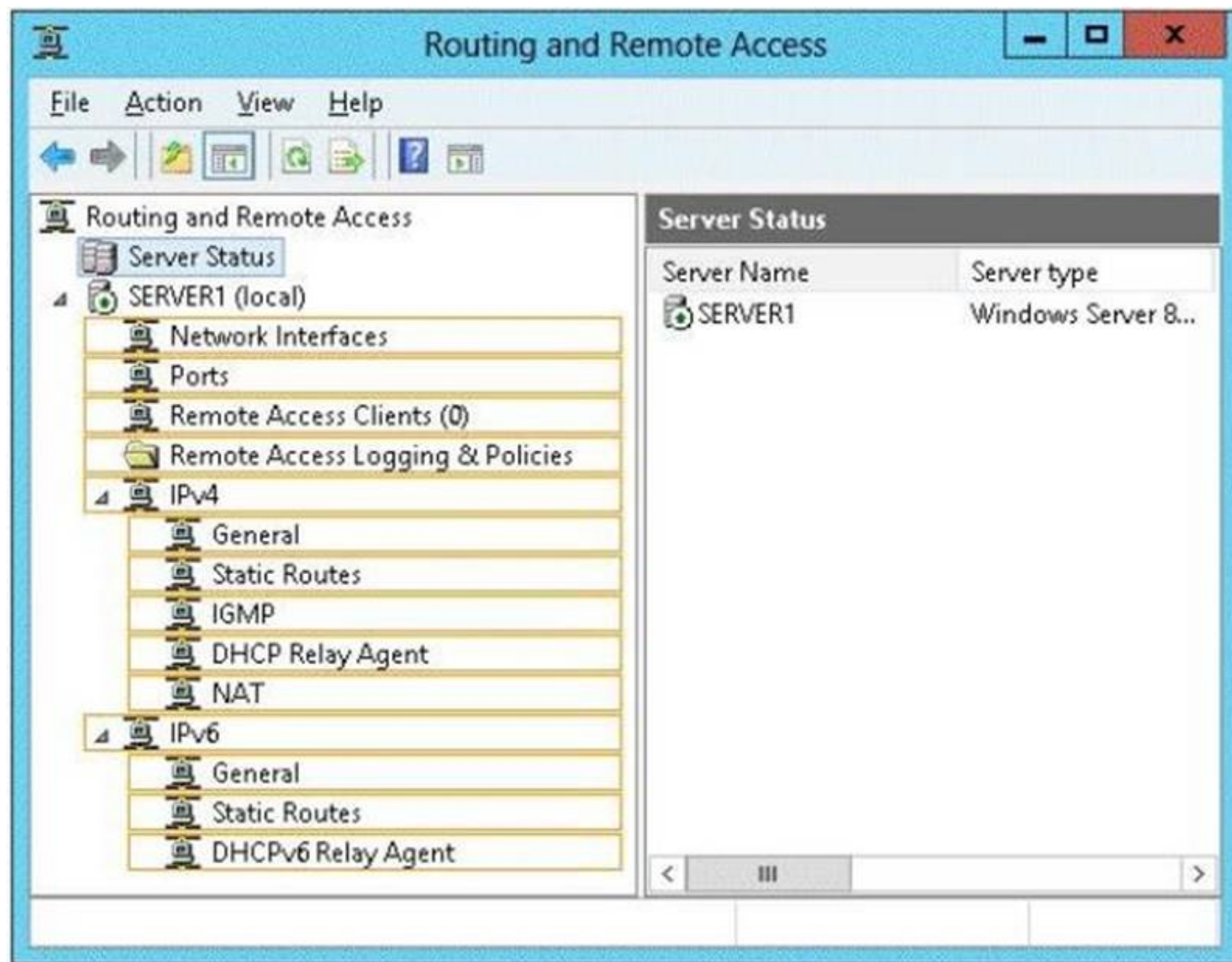
NEW QUESTION 73

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.

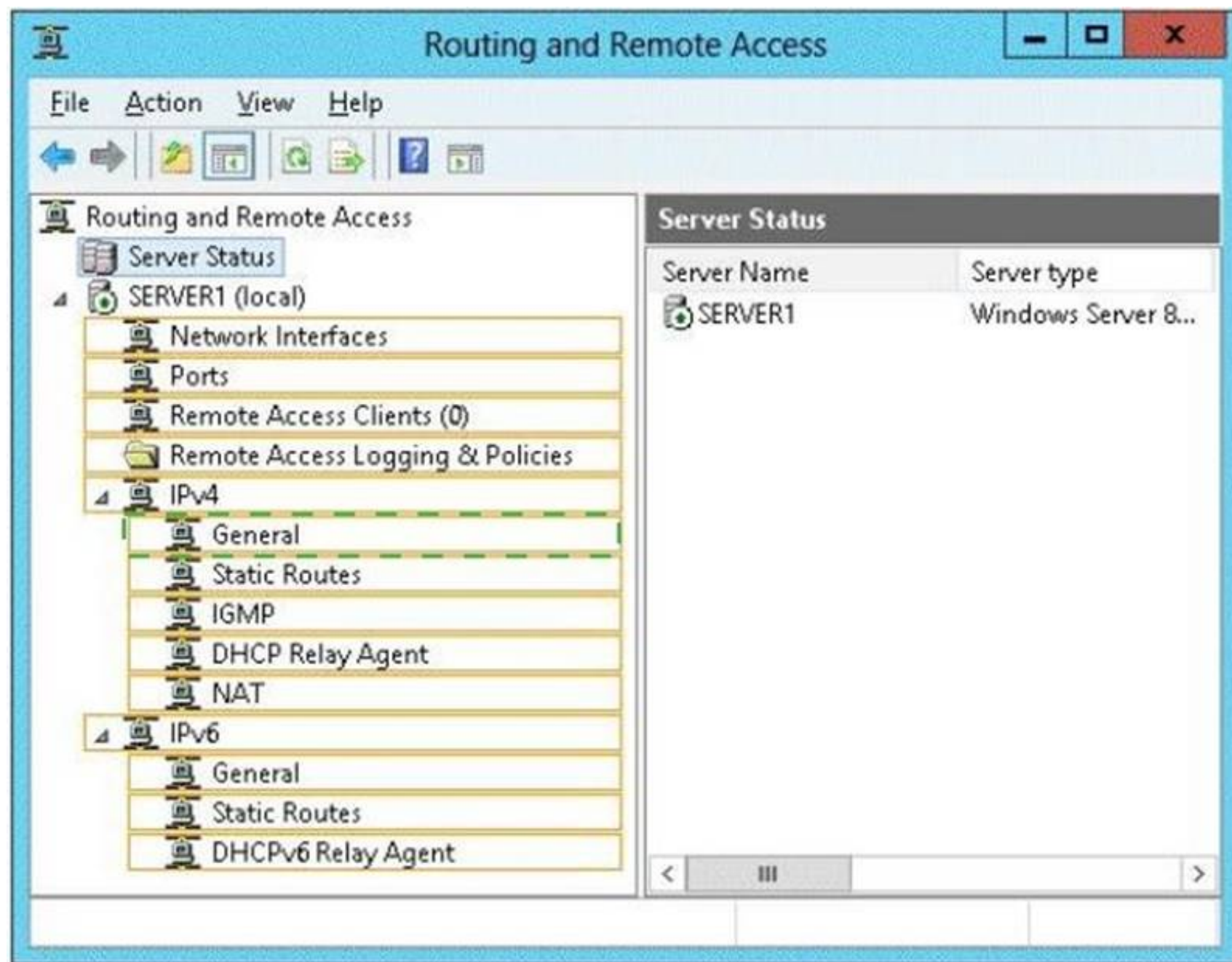
Which node should you use to add the RIP version 2 routing protocol? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**NEW QUESTION 75**

- (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?

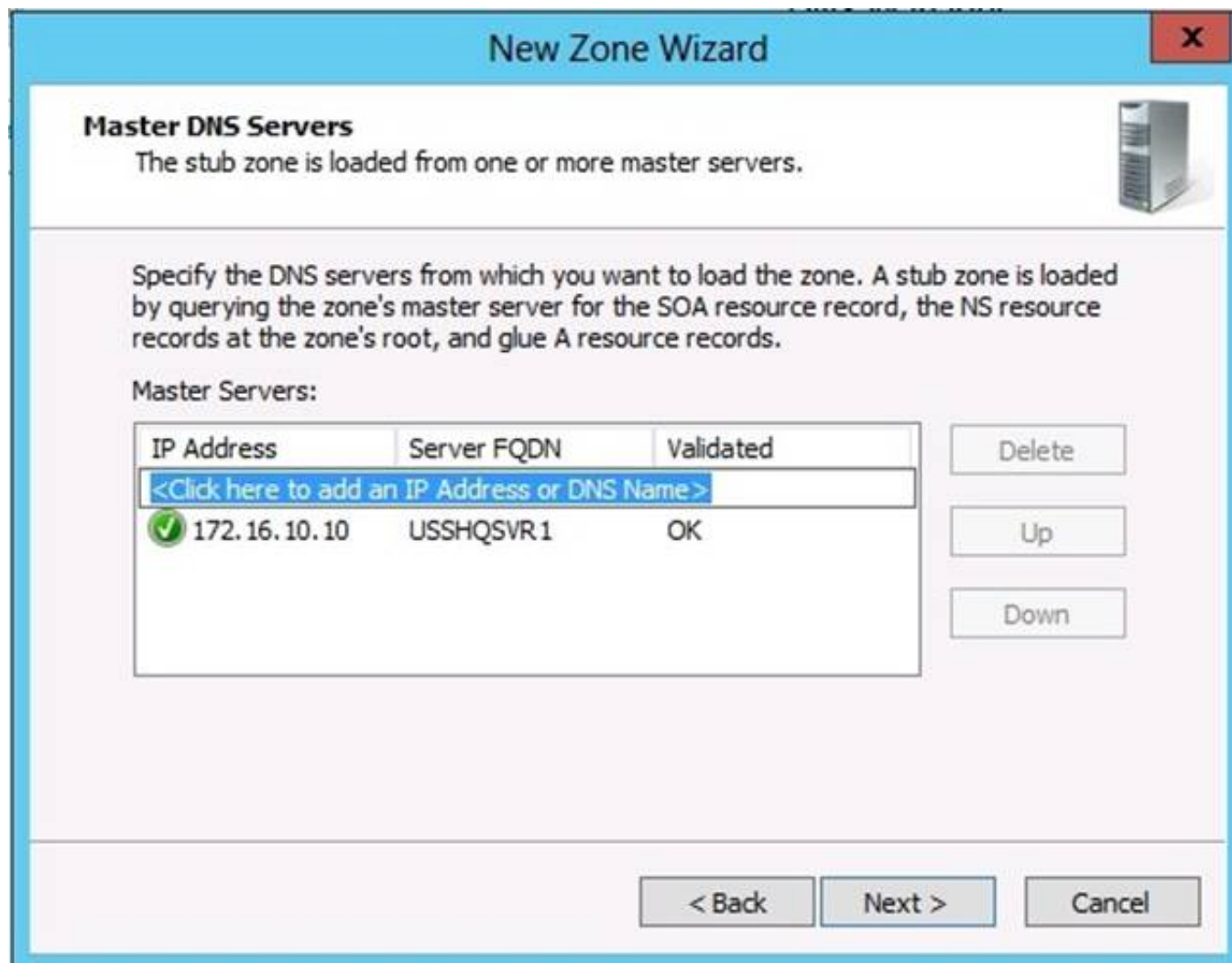
- A. Secondary
- B. Stub
- C. Reverse lookup
- D. Primary

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 76

- (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 78

- (Topic 1)

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

All user accounts for the marketing department reside in an organizational unit (OU) named OU1. All user accounts for the finance department reside in an organizational unit (OU) named OU2.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU2. You configure the Group Policy preference of GPO1 to add a shortcut named Link1 to the desktop.

You discover that when a user signs in, the Link1 is not added to the desktop. You need to ensure that when a user signs in, Link1 is added to the desktop. What should you do?

- A. Enforce GPO1.

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

Answer: D

Explanation:

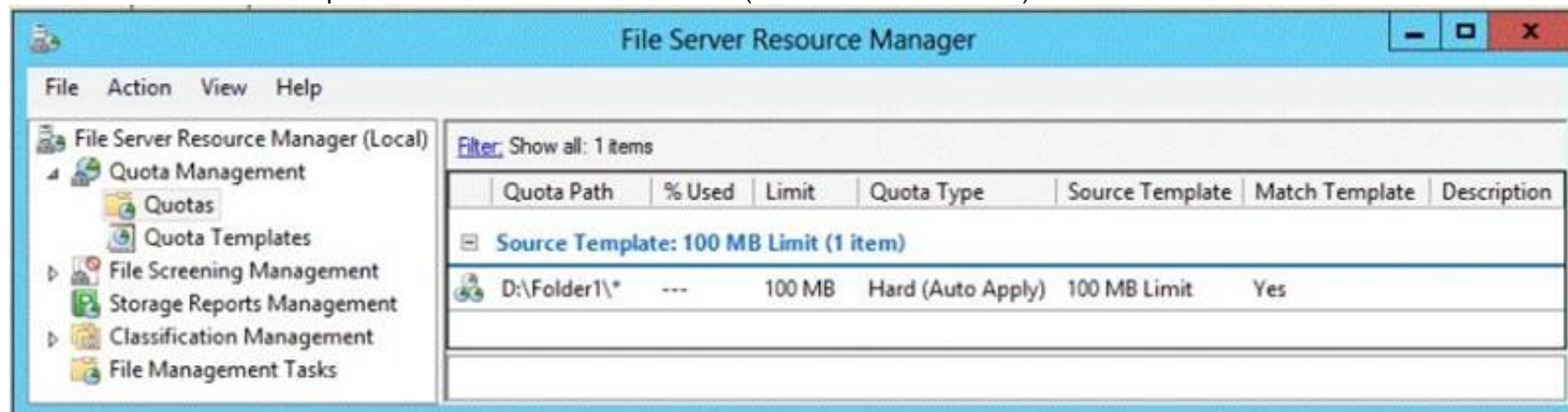
Security filtering is a way of refining which users and computers will receive and apply the settings in a Group Policy object (GPO). Using security filtering, you can specify that only certain security principals within a container where the GPO is linked apply the GPO. Security group filtering determines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

NEW QUESTION 79

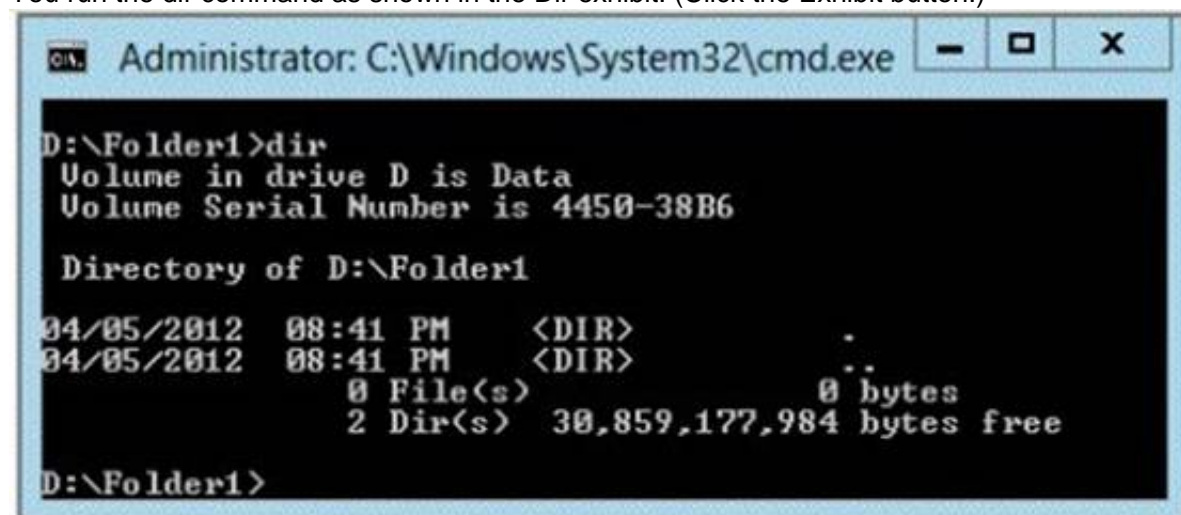
- (Topic 1)

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

An administrator creates a quota as shown in the Quota exhibit. (Click the Exhibit button.)



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



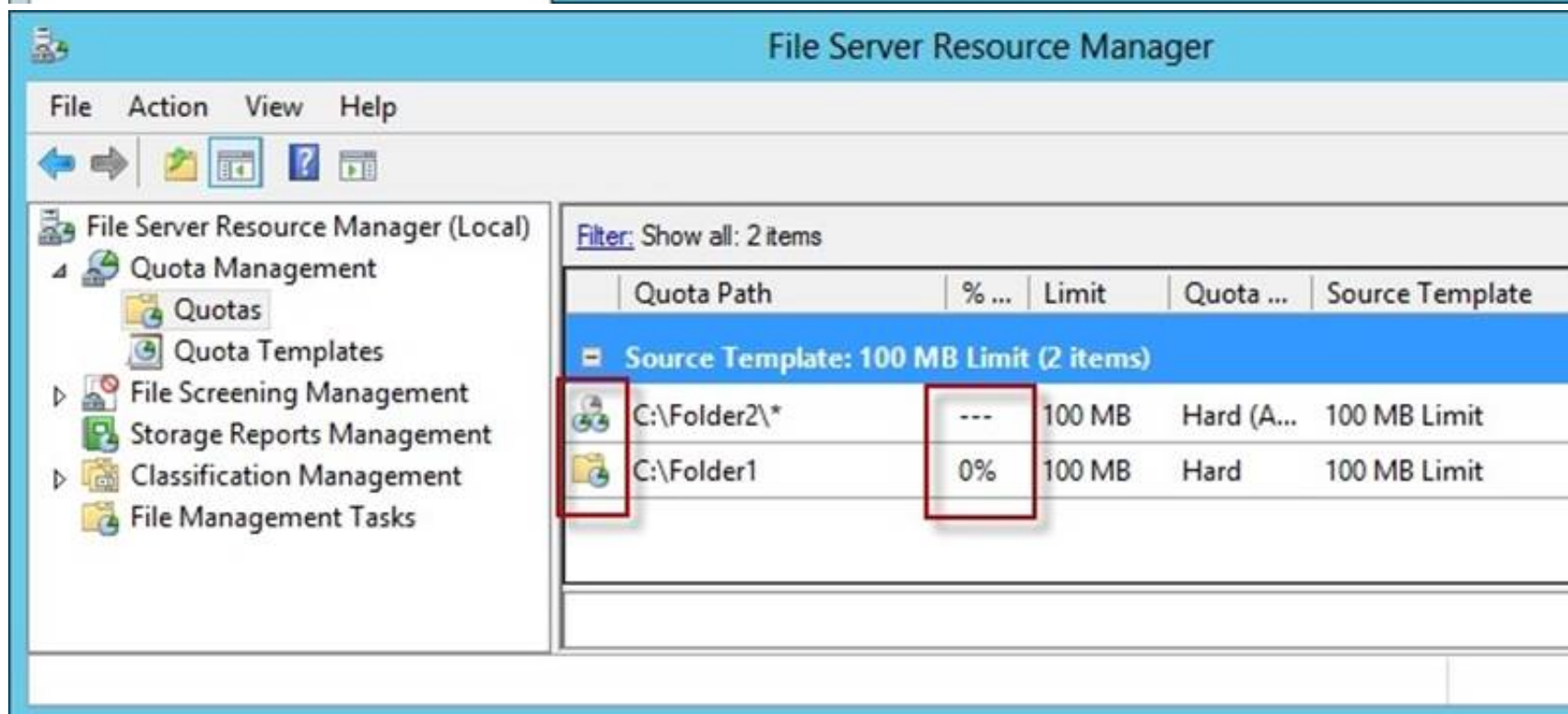
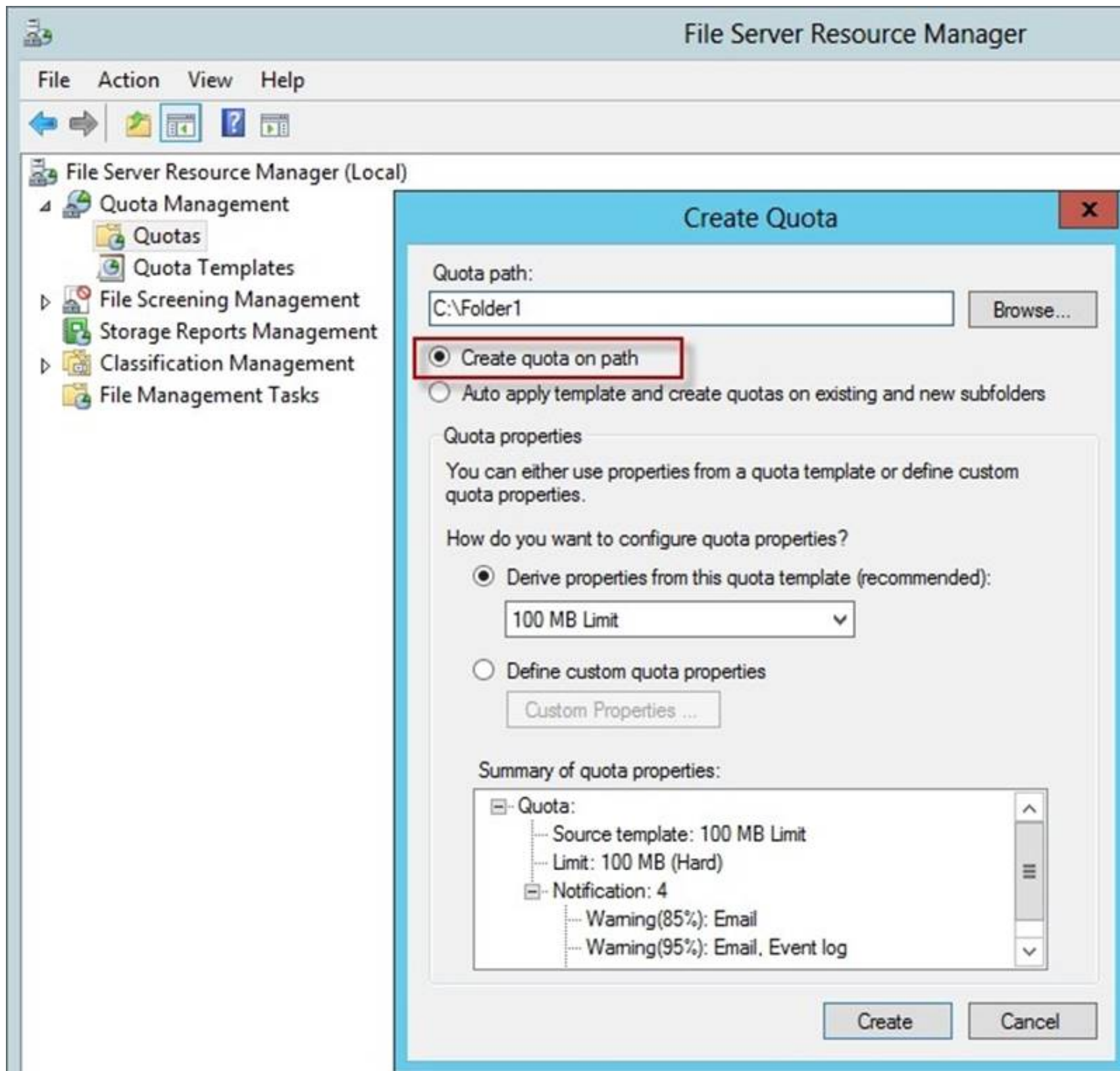
You need to ensure that D:\Folder1 can only consume 100 MB of disk space. What should you do?

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

Answer: A

Explanation:

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




```
Administrator: Command Prompt

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

Directory of C:\Folder1

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

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

Directory of C:\Folder2

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

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

NEW QUESTION 82

- (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:

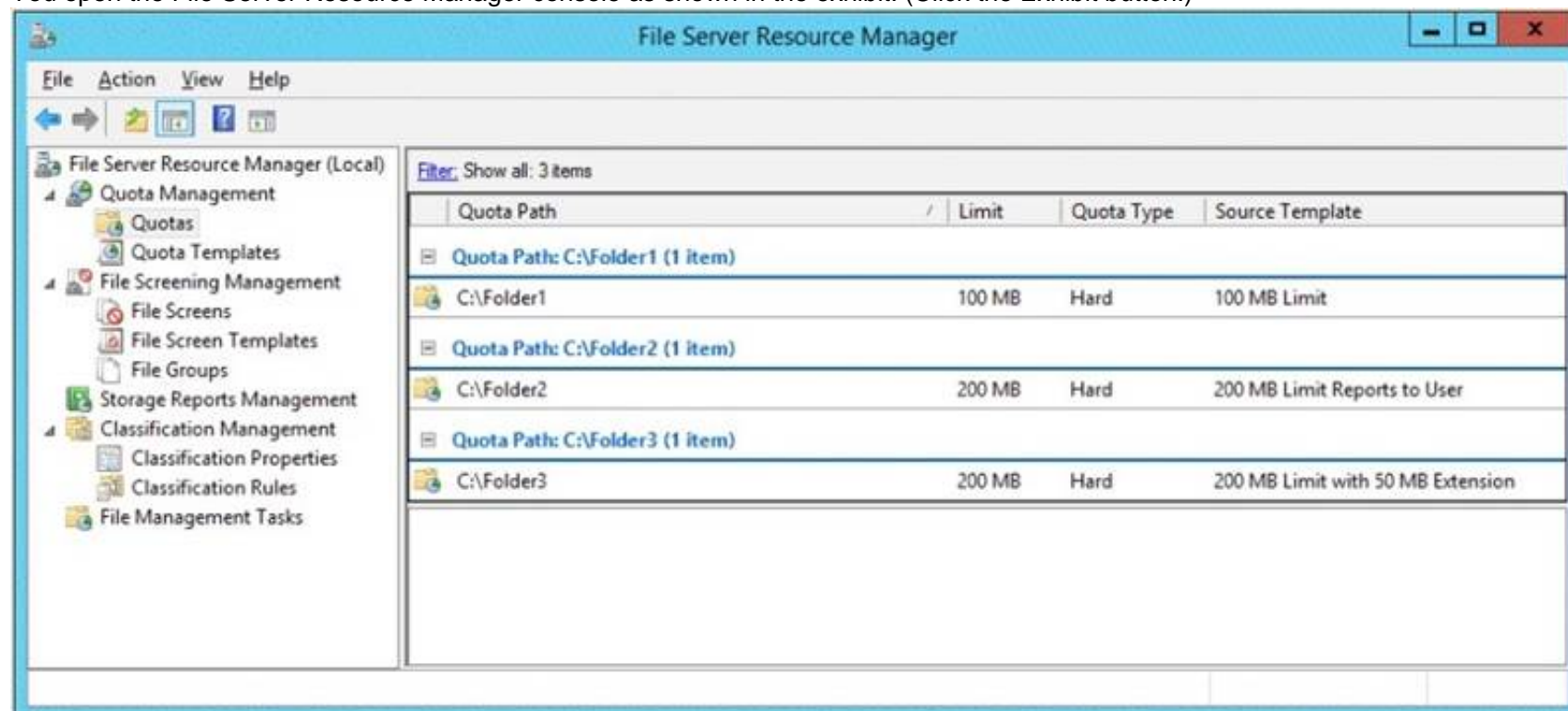
Environment Variable preference items allow you to create, update, replace, and delete user and system environment variables or semicolon-delimited segments of the PATH variable. Before you create an Environment Variable preference item, you should review the behavior of each type of action possible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

NEW QUESTION 87

- (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.

Create Quota

Quota path:

☐ Create quota on path

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

Quota properties

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

How do you want to configure quota properties?

☒ Derive properties from this quota template (recommended):

100 MB Limit

☐ Define custom quota properties

Summary of quota properties:

- [-] Auto Apply Quota:
 - Source template: 100 MB Limit
 - Limit: 100 MB (Hard)
 - [-] Notification: 4
 - Warning(85%): Email
 - Warning(95%): Email, Event log

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

NEW QUESTION 90

- (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 92

- (Topic 1)

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

In a remote site, a support technician installs a server named DC10 that runs Windows Server 2012 R2. DC10 is currently a member of a workgroup.

You plan to promote DC10 to a read-only domain controller (RODC).

You need to ensure that a user named Contoso\User1 can promote DC10 to a RODC in the contoso.com domain. The solution must minimize the number of permissions assigned to User1.

What should you do?

- A. From Active Directory Users and Computers, run the Delegation of Control Wizard on the contoso.com domain object.

- B. From Active Directory Administrative Center, pre-create an RODC computer account.
- C. From Ntdsutil, run the local roles command.
- D. Join DC10 to the domai
- E. Run dsmod and specify the /server switch.

Answer: B

Explanation:

A staged read only domain controller (RODC) installation works in two discrete phases:

1. Staging an unoccupied computer account
2. Attaching an RODC to that account during promotion

Reference: Install a Windows Server 2012 R2 Active Directory Read-Only Domain Controller (RODC)

NEW QUESTION 97

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs.

A network administrator accidentally deletes the Default Domain Policy GPO. You do not have a backup of any of the GPOs.

You need to recreate the Default Domain Policy GPO. What should you use?

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

Answer: A

Explanation:

Dcgpofix

Restores the default Group Policy objects to their original state (that is, the default state after initial installation).

Reference: [http://technet.microsoft.com/en-us/library/hh875588\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/hh875588(v=ws.10).aspx)

NEW QUESTION 98

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 102

- (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 103

HOTSPOT - (Topic 1)

Your company has two offices. The offices are located in Montreal and Seattle.

The network contains an Active Directory domain named contoso.com. The domain contains servers named Server1 and Server2. Server1 is located in the Seattle office. Server2 is located in the Montreal office. Both servers run Windows Server 2012 R2 and have the Windows Server Update Services (WSUS) server role installed.

You need to configure Server2 to download updates that are approved on Server1 only.

What cmdlet should you run? To answer, select the appropriate options in the answer area.

Answer Area

Answer Area

Add-WsusComputer
Approve-WsusUpdate
Set-WsusClassification
Set-WsusProduct
Set-WsusServerSynchronizatio

-SERVERNAME Server1
-UpdateServer Server1
-UssServerName Server1

-Replica
-SyncFromMu
-UseSsl

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Add-WsusComputer
Approve-WsusUpdate
Set-WsusClassification
Set-WsusProduct
Set-WsusServerSynchronizatio

-ServerName Server1
-UpdateServer Server1
-UssServerName Server1

-Replica
-SyncFromMu
-UseSsl

NEW QUESTION 105

DRAG DROP - (Topic 1)

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

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

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

Actions

Answer Area

GPO5

GPO3

GPO2

GPO1

GPO4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: GPO2
Box 2: GPO4
Box 3: GPO5

Note:
* First at the domain level (GPO2), then at the highest OU level GPO4, and finally at the OU level containing user1 GPO5.
Incorrect:
* Read and Apply group policy are both needed in order for the user or computer to receive and process the policy
Not GPO1: Group1 has Deny Apply Group Policy permissions on GPO1. Not GPO3: Group1 has Deny Read permissions on GPO3.
GPO2 and GPO4 are disabled.
* When a Group Policy Object (GPO) is enforced it means the settings in the Group Policy Object on an Organization Unit (which is shown as a folder within the Active Directory Users and Computers MMC) cannot be overruled by a Group Policy Object (GPO) which is link enabled on an Organizational Unit below the Organizational Unit with the enforced Group Policy Object (GPO).
* Group Policy settings are processed in the following order: 1 Local Group Policy object
2 Site.

3 Domain

4 Organizational units

GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

NEW QUESTION 109

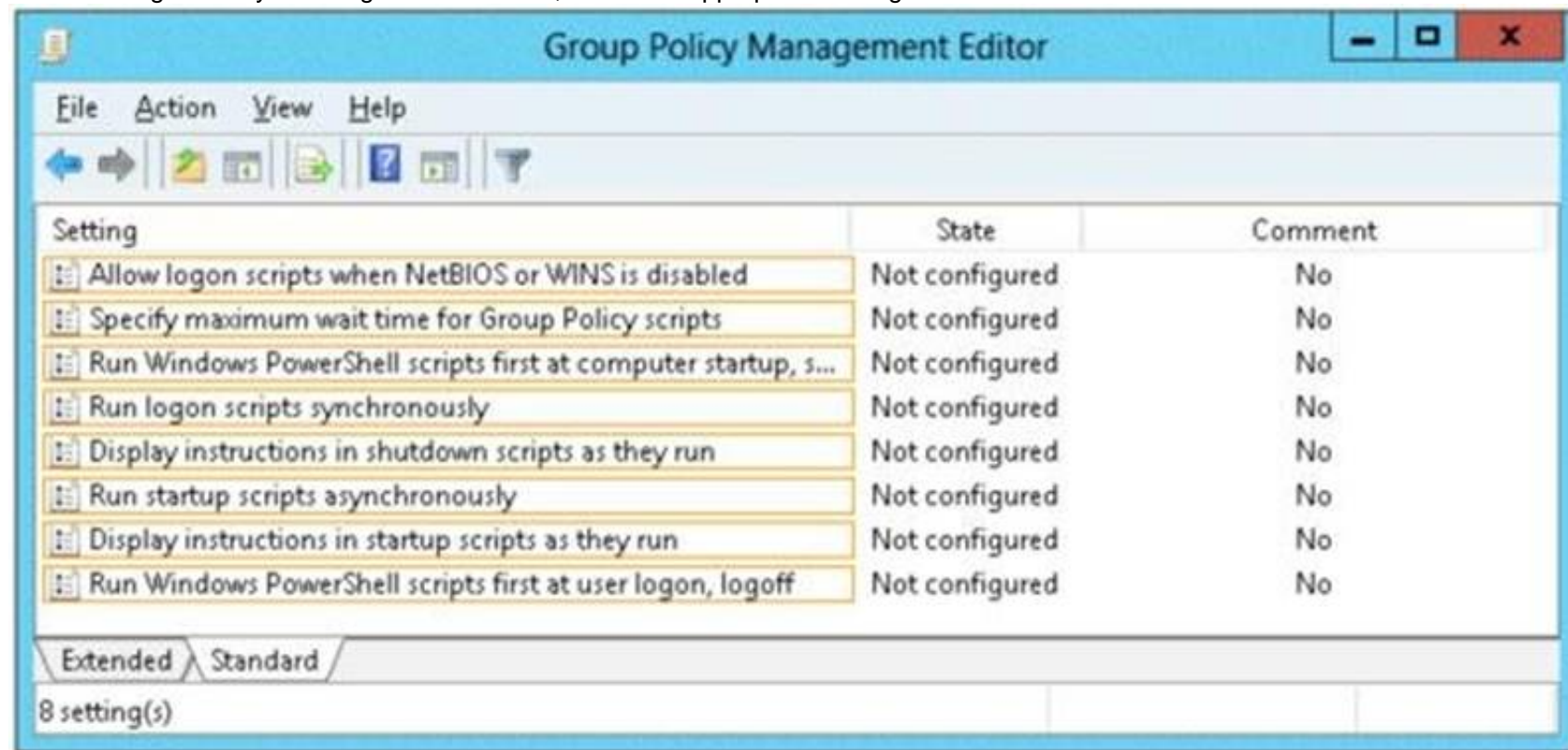
HOTSPOT - (Topic 1)

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

You have several Windows PowerShell scripts that execute when client computers start. When a client computer starts, you discover that it takes a long time before users are prompted to log on.

You need to reduce the amount of time it takes for the client computers to start. The solution must not prevent scripts from completing successfully.

Which setting should you configure? To answer, select the appropriate setting in the answer area.



A. Mastered

B. Not Mastered

Answer: A

Explanation:

Lets the system run startup scripts simultaneously rather than waiting for each to finish <http://technet.microsoft.com/en-us/library/cc939423.aspx>

Directs the system to wait for logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop.

If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.

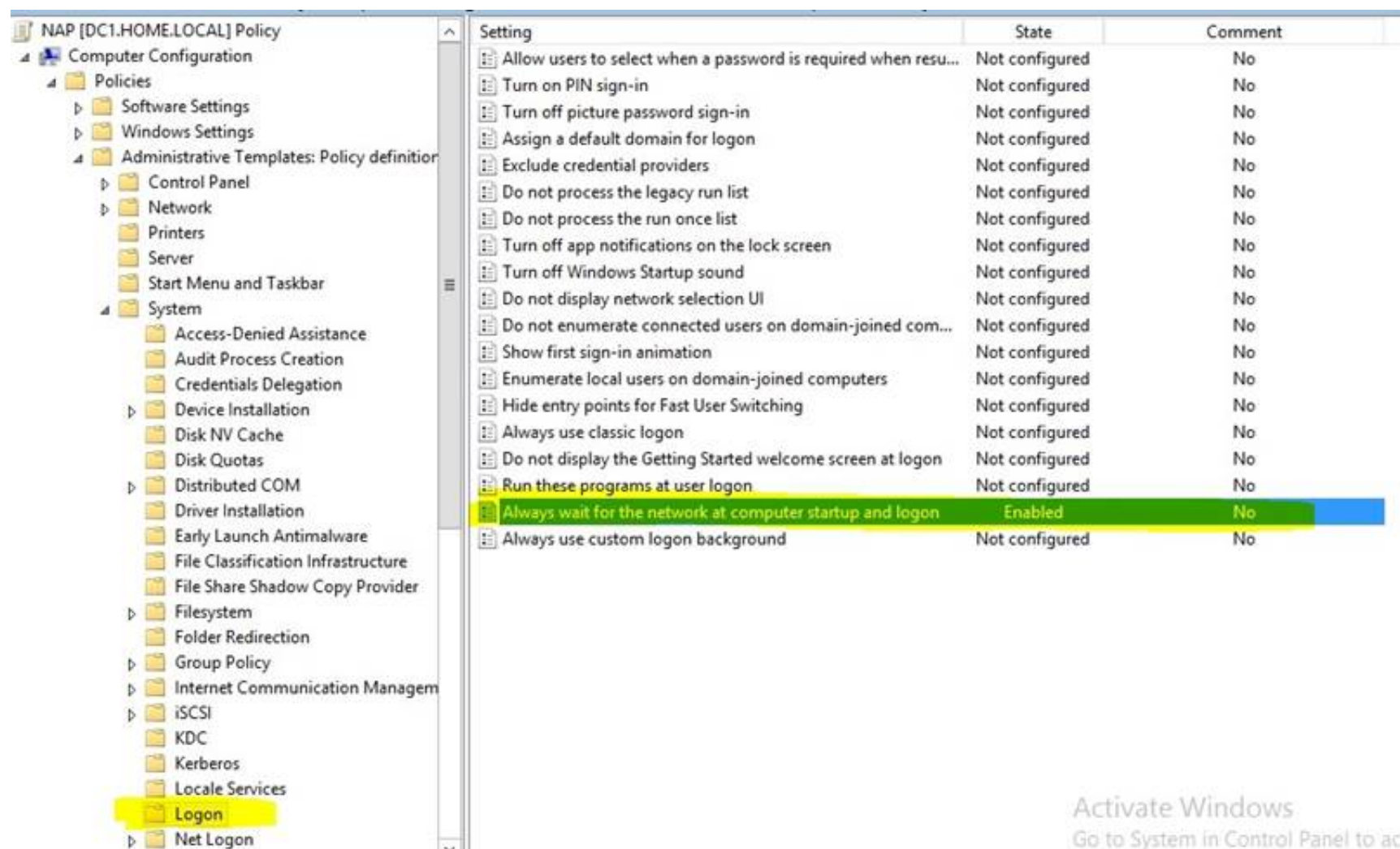
If you disable this policy or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously.

This policy appears in the Computer Configuration and User Configuration folders. The policy set in Computer Configuration takes precedence over the policy set in User

Configuration.

By default, the Fast Logon Optimization feature is set for both domain and workgroup members. This setting causes policy to be applied asynchronously when the computer starts and the user logs on. The result is similar to a background refresh. The advantage is that it can reduce the amount of time it takes for the logon dialog box to appear and the amount of time it takes for the desktop to become available to the user. Of course, it also means that the user may log on and start working before the absolute latest policy settings have been applied to the system.

Depending on your environment, you may want to disable Fast Logon Optimization. You can do this with Group Policy, using the Always wait for the network at computer startup and logon policy setting.



References:

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

NEW QUESTION 113

- (Topic 1)

Your network contains an Active Directory domain named adatum.com. The domain contains a member server named Server1 and 10 web servers. All of the web servers are

in an organizational unit (OU) named WebServers_OU. All of the servers run Windows Server 2012 R2.

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

What should you do?

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

Answer: A

Explanation:

Source-initiated subscriptions allow you to define a subscription on an event collector computer without defining the event source computers, and then multiple remote event source computers can be set up (using a group policy setting) to forward events to the event collector computer. This differs from a collector initiated subscription because in the collector initiated subscription model, the event collector must define all the event sources in the event subscription.

1. Run the following command from an elevated privilege command prompt on the Windows Server domain controller to configure Windows Remote Management: winrm qc -q.

2. Start group policy by running the following command:
%SYSTEMROOT%\System32\gpedit. msc.

3. Under the Computer Configuration node, expand the Administrative Templates node, then expand the Windows Components node, then select the Event Forwarding node.

4. Right-click the SubscriptionManager setting, and select Properties. Enable the SubscriptionManager setting, and click the Show button to add a server address to the setting. Add at least one setting that specifies the event collector computer. The SubscriptionManager Properties window contains an Explain tab that describes the syntax for the setting.

5. After the SubscriptionManager setting has been added, run the following command to ensure the policy is applied: gpupdate /force.

If you want to configure a source computer-initiated subscription, you need to configure the following group policies on the computers that will act as the event forwarders:

* (A) Configure Target Subscription Manager This policy enables you to set the location of the collector computer.

NEW QUESTION 117

HOTSPOT - (Topic 1)

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

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

You remove Servers from the network.

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

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

Server1

Server2

Server1

```
set-wsusserver synchronization -syncfrommu
set-wsusserver synchronization -useservername server1
set-wsusserver synchronization -useservername server2
wsusutil.exe movecontent \\server1\c$
wsusutil.exe movecontent \\server2\c$
```

Server2

```
set-wsusserver synchronization -syncfrommu
set-wsusserver synchronization -useservername server1
set-wsusserver synchronization -useservername server2
wsusutil.exe movecontent \\server1\c$
wsusutil.exe movecontent \\server2\c$
```

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Set-WsusServerSynchronization-SyncFromMU [-UpdateServer<IUpdateServer>] [- Confirm] [-WhatIf] [<CommonParameters>]

Set-WsusServerSynchronization-UssServerName<String> [-PortNumber<Int32>] [- Replica] [-UpdateServer<IUpdateServer>] [-UseSsl] [-Confirm] [-WhatIf] [<CommonParameters>]

The Set-WsusServerSynchronizationcmdlet sets whether the Windows Server Update Services (WSUS) server synchronizes from Microsoft Update or an upstream server. This cmdlet allows the user to specify settings such as the upstream server name, the port number, and whether or not to use Secure Sockets Layer (SSL).

References:

<http://technet.microsoft.com/en-us/library/hh826163.aspx>

<http://technet.microsoft.com/en-us/library/cc708480%28v=ws.10%29.aspx>

NEW QUESTION 118

HOTSPOT - (Topic 1)

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

You need to audit successful and failed attempts to read data from USB drives on the servers.

Which two objects should you configure? To answer, select the appropriate two objects in the answer area.

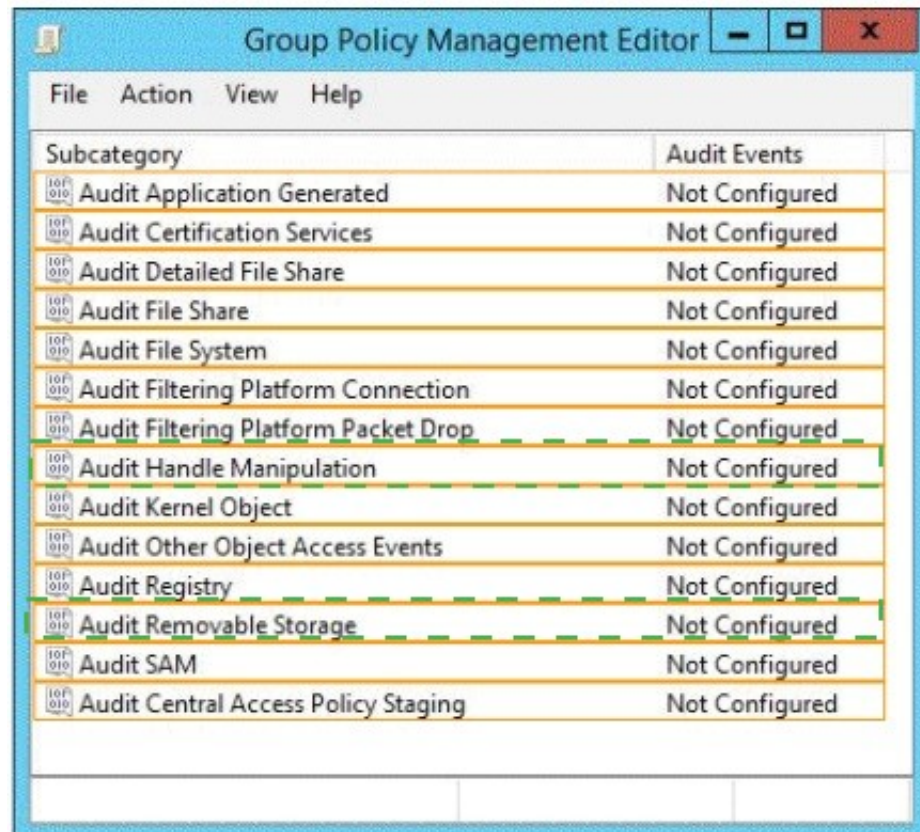
Group Policy Management Editor

Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Not Configured
Audit File Share	Not Configured
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

- A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 121

- (Topic 1)

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

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

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

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

Answer: E

Explanation:

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

NEW QUESTION 125

- (Topic 2)

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

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

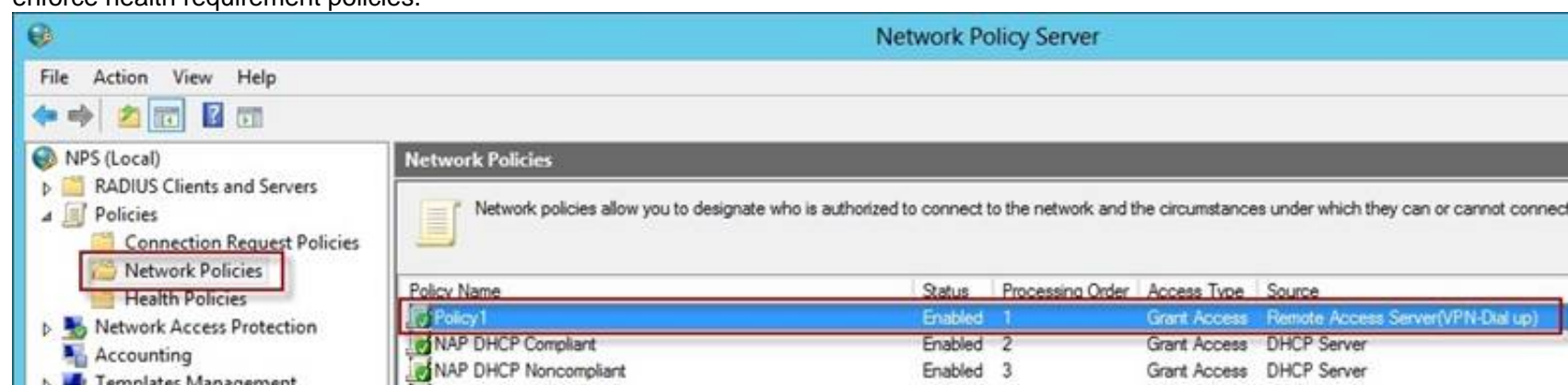
Answer: A

Explanation:

Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances

under which they can or cannot connect.

Network policies can be viewed as rules. Each rule has a set of conditions and settings. Configure your VPN server to use Network Access Protection (NAP) to enforce health requirement policies.



References:

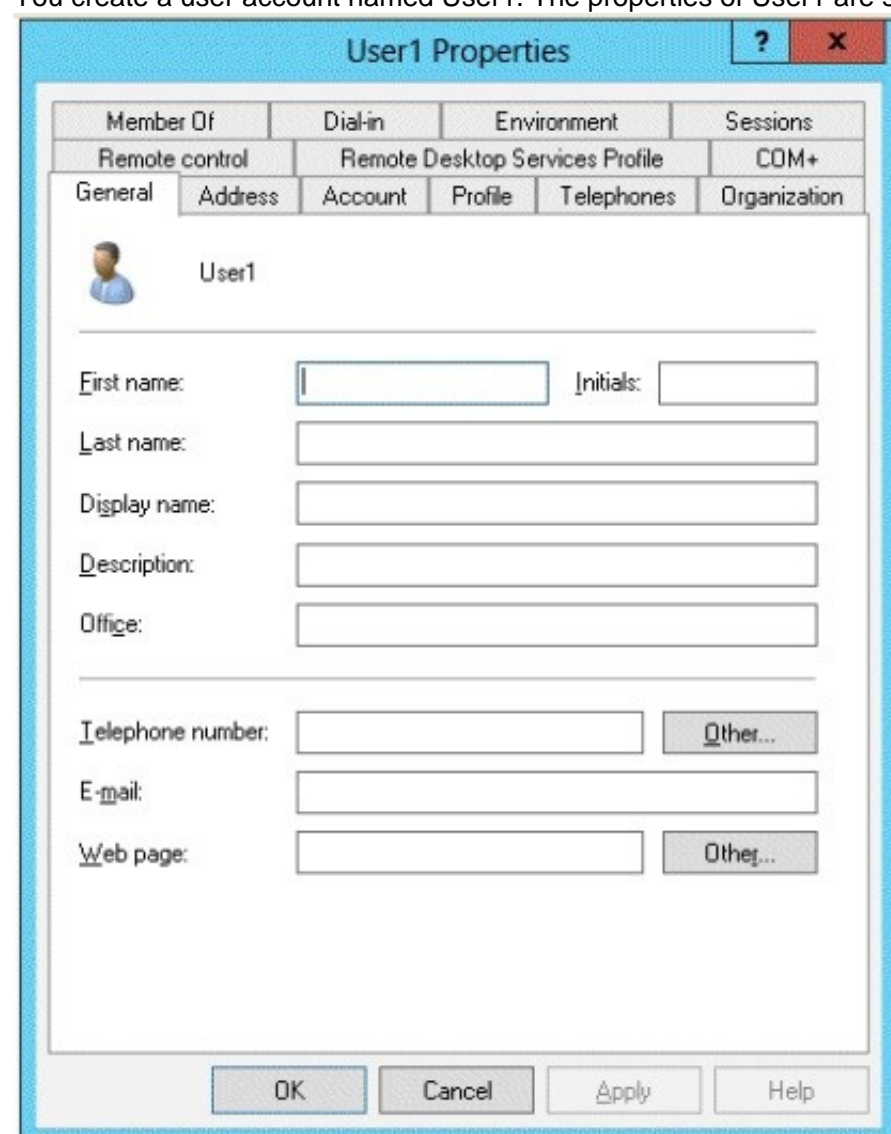
<http://technet.microsoft.com/en-us/library/hh831683.aspx>
<http://technet.microsoft.com/en-us/library/cc754107.aspx>
<http://technet.microsoft.com/en-us/library/dd314165%28v=ws.10%29.aspx>
<http://technet.microsoft.com/en-us/windowsserver/dd448603.aspx>
[http://technet.microsoft.com/en-us/library/dd314165\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/libr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

NEW QUESTION 126

- (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.

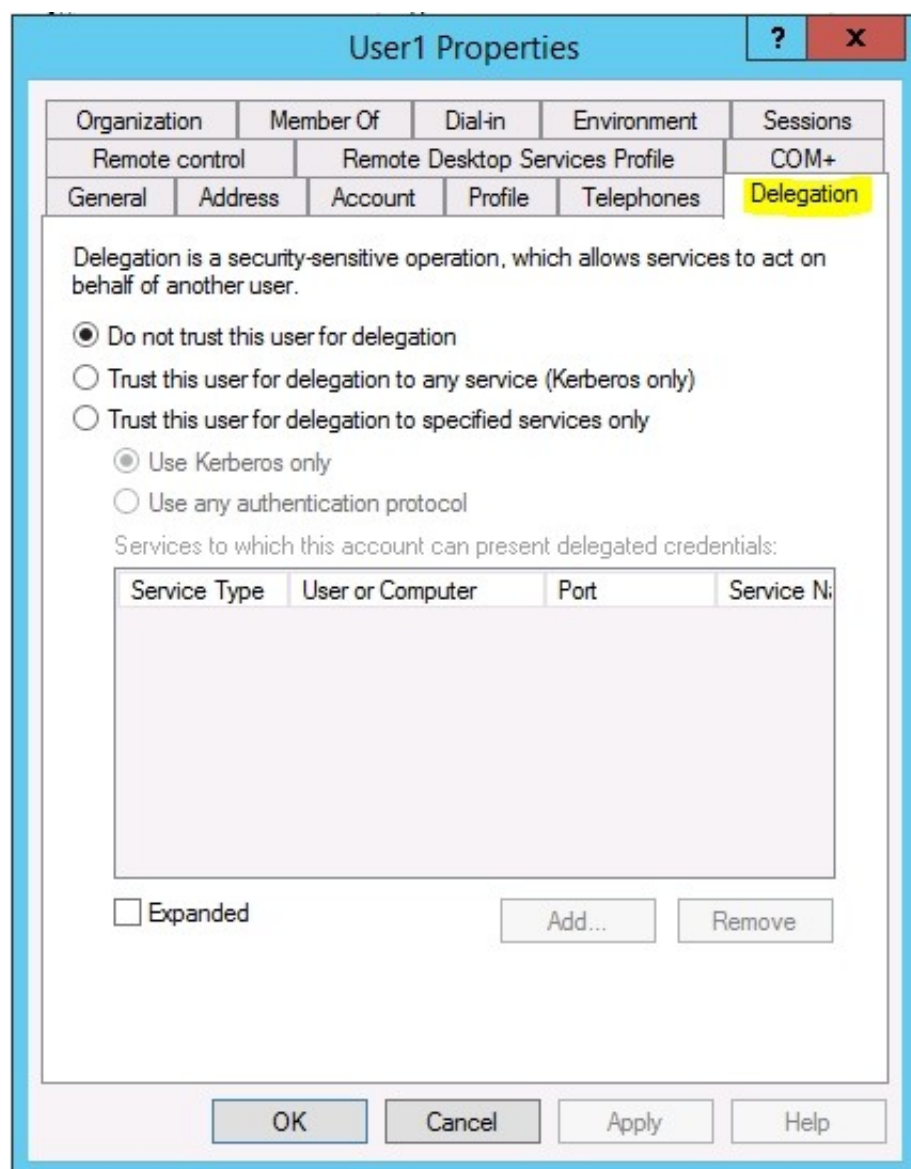
Answer: C

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 127

HOTSPOT - (Topic 2)

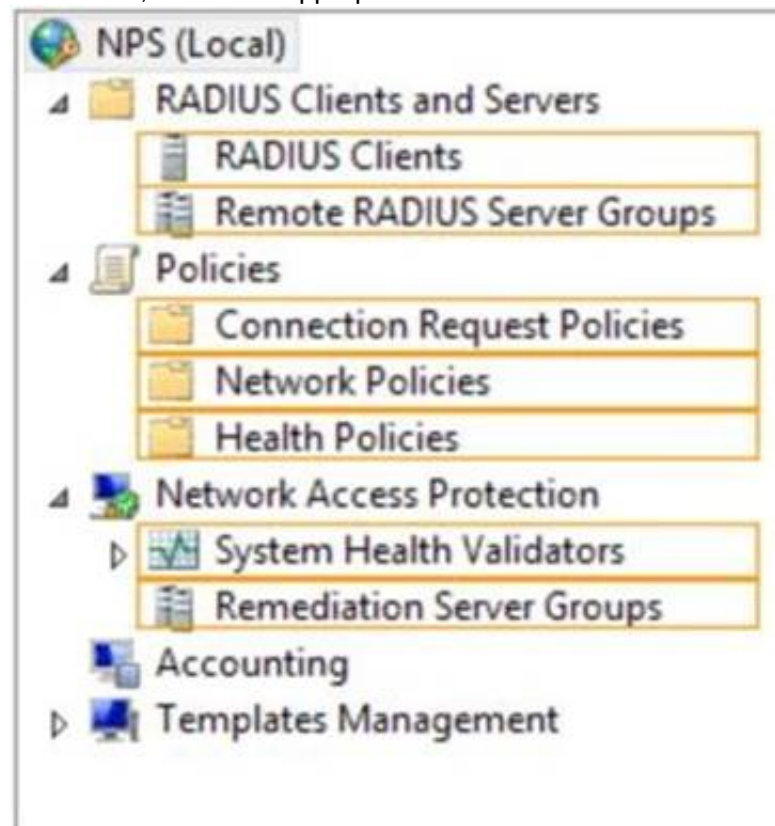
Your network contains a RADIUS server named Admin1.

You install a new server named Server2 that runs Windows Server 2012 R2 and has Network Policy Server (NPS) installed.

You need to ensure that all accounting requests for Server2 are forwarded to Admin1. On Server2, you create a new remote RADIUS server group named Group1 that contains Admin1.

What should you configure next on Server2?

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Connection request policies are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User Service

(RADIUS) servers perform the authentication and authorization of connection requests that the server running Network Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS servers are used for RADIUS accounting.

NEW QUESTION 130

- (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.

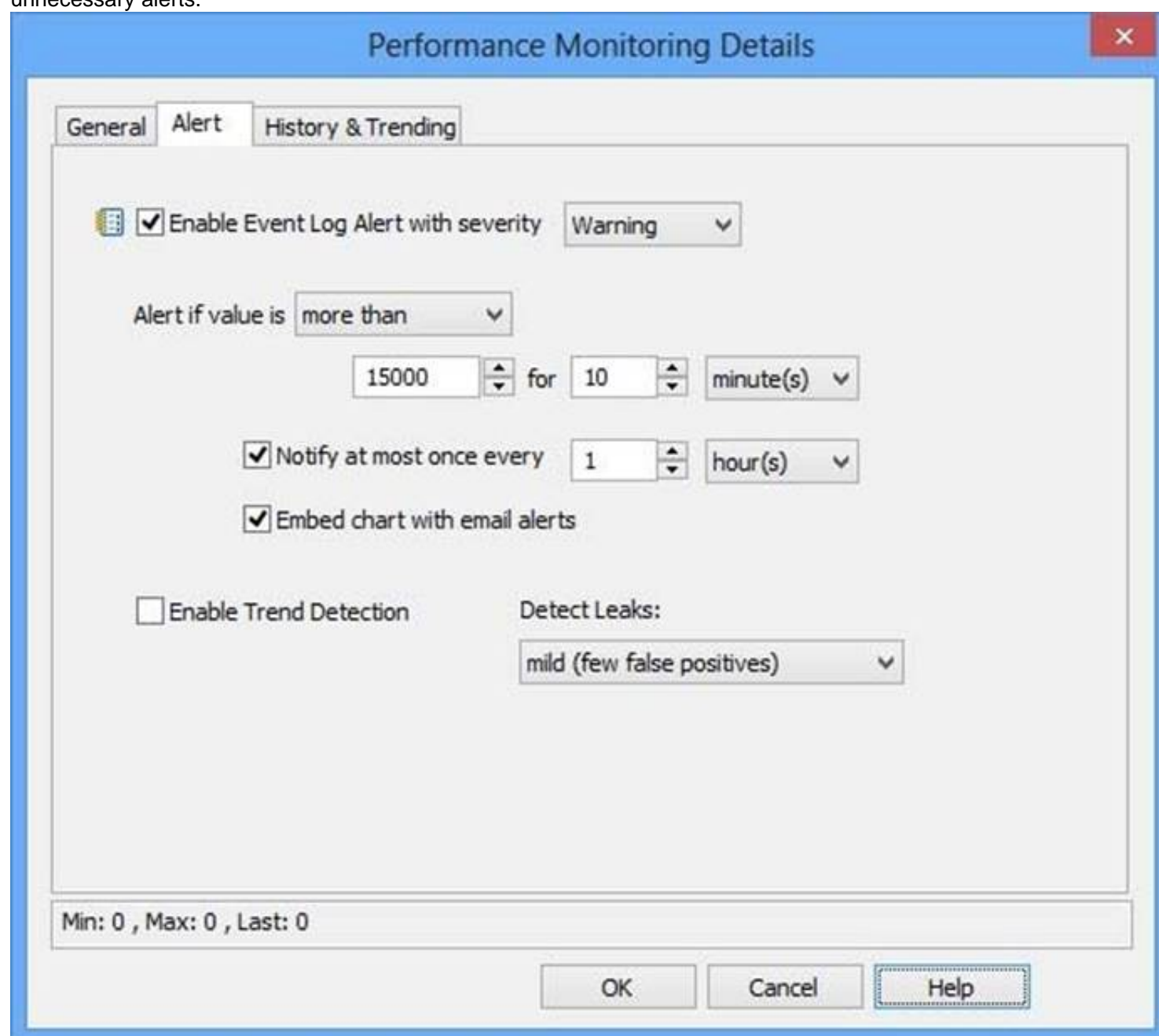
Which type of data collector should you create?

- 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.



NEW QUESTION 133

- (Topic 2)

Your network has a router named Router1 that provides access to the Internet. You have a server named Server1 that runs Windows Server 2012 R2. Server1 to use Router1 as the default gateway.

A new router named Router2 is added to the network. Router2 provides access to the Internet. The IP address of the internal interface on Router2 is 10.1.14.2S4. You need to configure Server1 to use Router2 to connect to the Internet if Router1 fails. What should you do on Server1?

- A. Add a route for 10.1.14.0/24 that uses 10.1.14.254 as the gateway and set the metric to 1.
- B. Add 10.1.14.254 as a gateway and set the metric to 1.
- C. Add a route for 10.1.14.0/24 that uses 10.1.14.254 as the gateway and set the metric to 500.
- D. Add 10.1.14.254 as a gateway and set the metric to 500.

Answer: C

Explanation:

To configure the Automatic Metric feature:

1. In Control Panel, double-click Network Connections.
2. Right-click a network interface, and then click Properties.
3. Click Internet Protocol (TCP/IP), and then click Properties.
4. On the General tab, click Advanced.
5. To specify a metric, on the IP Settings tab, click to clear the Automatic metric check box, and then enter the metric that you want in the Interface Metric field.

To manually add routes for IPv4

Open the Command Prompt window by clicking the Start button Picture of the Start button. In the search box, type Command Prompt, and then, in the list of results, click Command Prompt.

At the command prompt, type route -p add [destination] [mask <netmask>] [gateway] [metric <metric>] [if <interface>].

NEW QUESTION 134

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2.

You have a Password Settings object (PSOs) named PSO1.

You need to view the settings of PSO1. Which tool should you use?

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

Answer: B

Explanation:

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

NEW QUESTION 136

- (Topic 2)

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

Server1 has the Windows Server updates Services server role installed and is configured to download updates from the Microsoft Update servers.

You need to ensure that Server1 downloads express installation files from the Microsoft Update servers.

What should you do from the Update Services console?

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

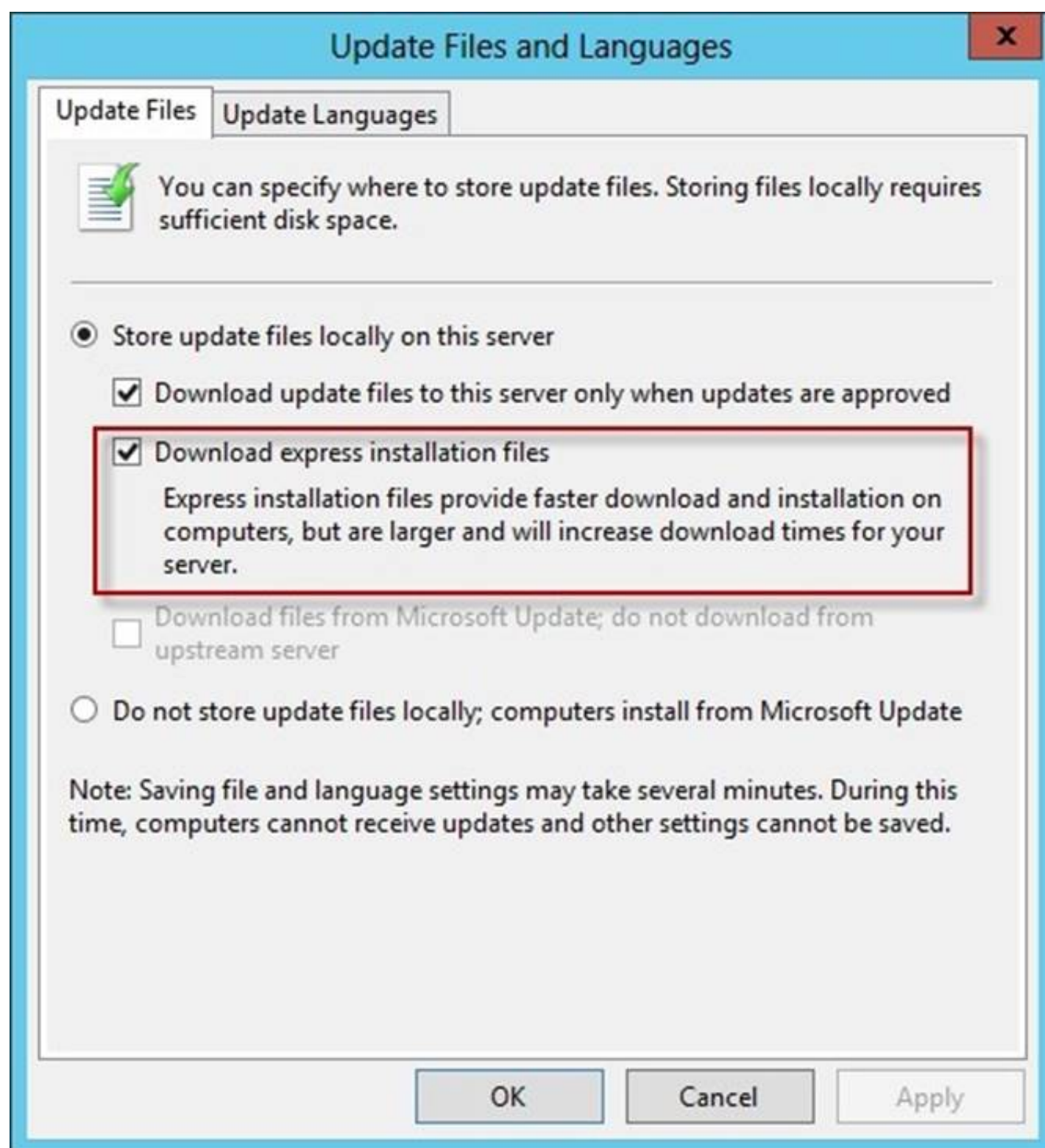
Answer: A

Explanation:

To specify whether express installation files are downloaded during synchronization In the left pane of the WSUS Administration console, click Options.

In Update Files and Languages, click the Update Files tab.

If you want to download express installation files, select the Download express installation files check box. If you do not want to download express installation files, clear the check box.



Reference:

<http://technet.microsoft.com/en-us/library/cc708431.aspx>

<http://technet.microsoft.com/en-us/library/cc708431.aspx>

NEW QUESTION 139

- (Topic 2)

Your network contains a single Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that hosts the primary DNS zone for contoso.com.

All servers dynamically register their host names.

You install three new Web servers that host identical copies of your company's intranet website. The servers are configured as shown in the following table.

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

You need to use DNS records to load balance name resolution queries for intranet.contoso.com between the three Web servers.

What is the minimum number of DNS records that you should create manually?

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

Answer: B

Explanation:

To create DNS Host (A) Records for all internal pool servers

1. Click Start, click All Programs, click Administrative Tools, and then click DNS.
2. In DNS Manager, click the DNS Server that manages your records to expand it.
3. Click Forward Lookup Zones to expand it.
4. Right-click the DNS domain that you need to add records to, and then click New Host (A or AAAA).
5. In the Name box, type the name of the host record (the domain name will be automatically appended).
6. In the IP Address box, type the IP address of the individual Front End Server and then select Create associated pointer (PTR) record or Allow any authenticated user to update DNS records with the same owner name, if applicable.
7. Continue creating records for all member Front End Servers that will participate in DNS Load Balancing.

For example, if you had a pool named pool1.contoso.com and three Front End Servers, you would create the following DNS entries:

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

erence:

<http://technet.microsoft.com/en-us/library/cc772506.aspx>

<http://technet.microsoft.com/en-us/library/gg398251.aspx>

NEW QUESTION 144

HOTSPOT - (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a member server that runs Windows Server 2012 R2 and has the Windows Deployment Services (WDS) server role installed.

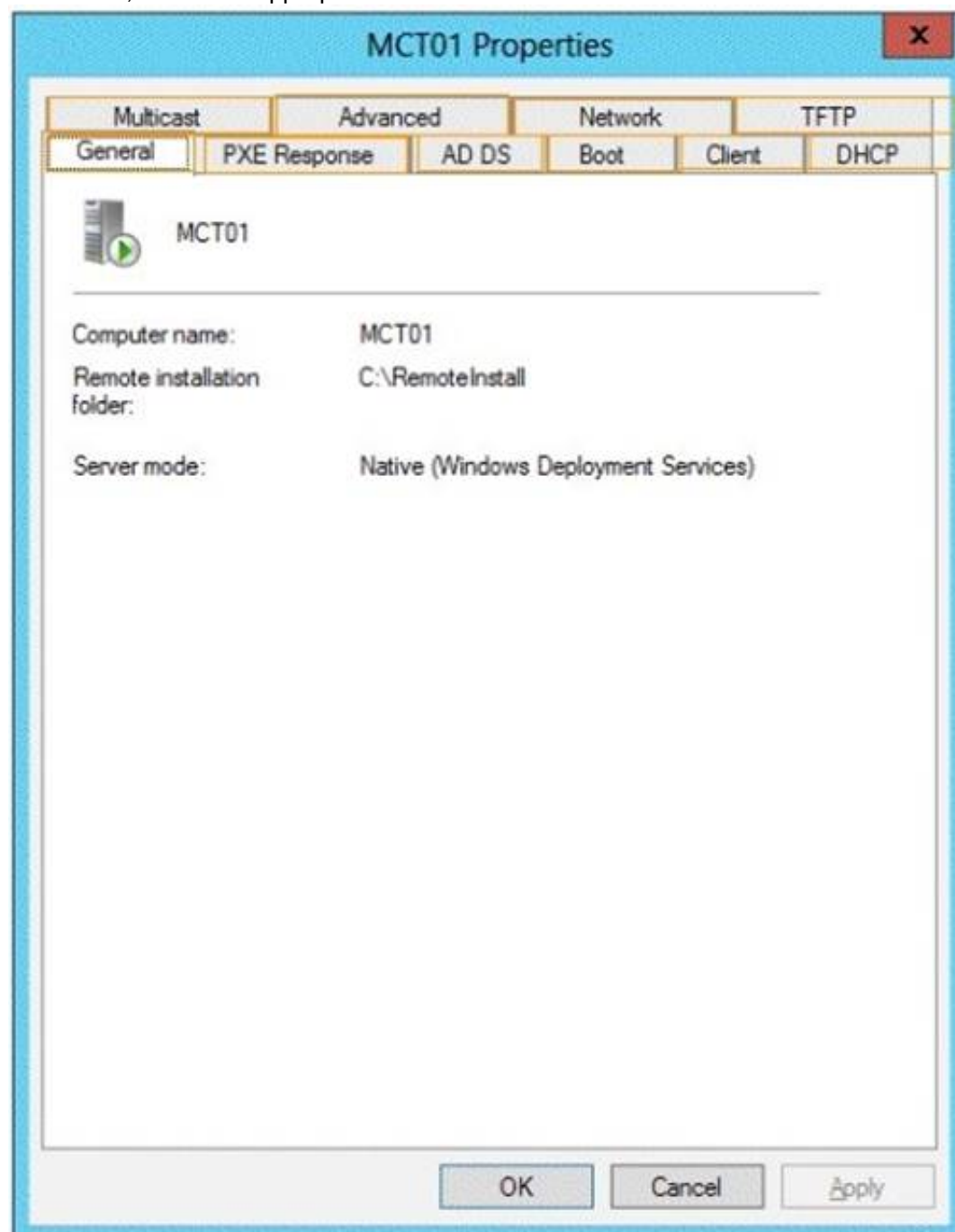
You create a new multicast session in WDS and connect 50 client computers to the session.

When you open the Windows Deployment Services console, you discover that all of the computers are listed as pending devices.

You need to ensure that any of the computers on the network can join a multicast transmission without requiring administrator approval.

What should you configure?

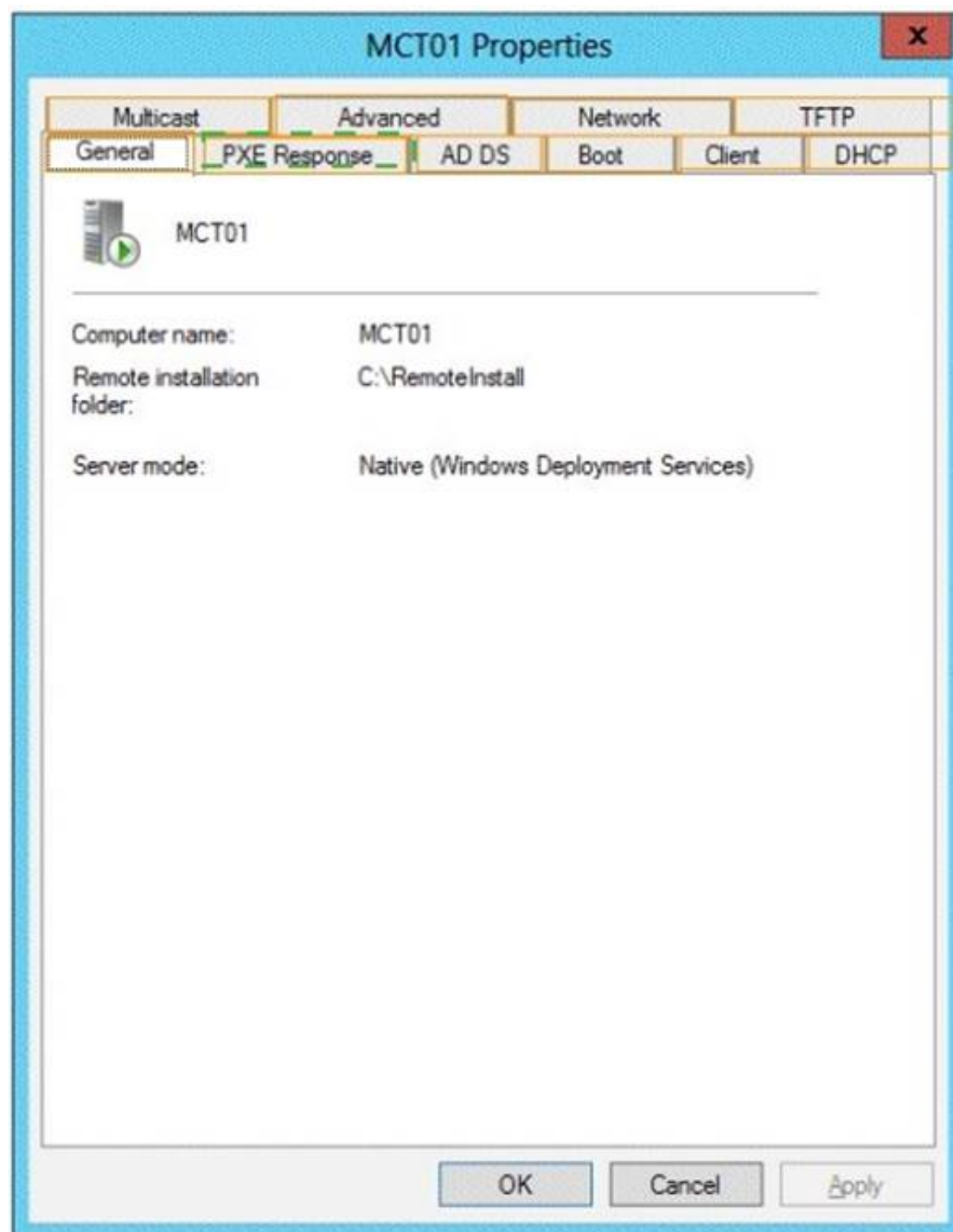
To answer, select the appropriate tab in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 147

HOTSPOT - (Topic 2)

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

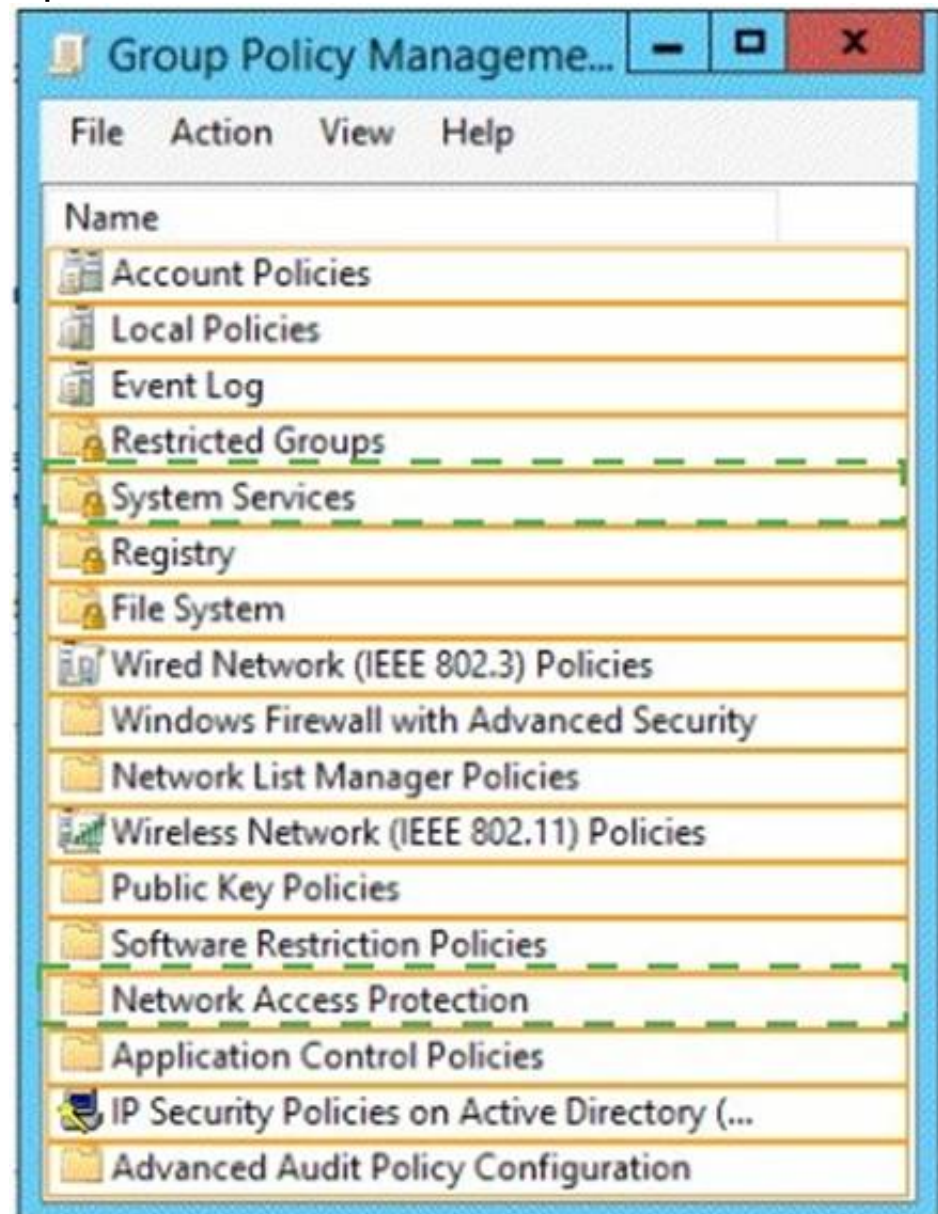
To answer, select the appropriate two settings in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 148

- (Topic 2)

You have a failover cluster that contains five nodes. All of the nodes run Windows Server 2012 R2. All of the nodes have BitLocker Drive Encryption (BitLocker) enabled.

You enable BitLocker on a Cluster Shared Volume (CSV).

You need to ensure that all of the cluster nodes can access the CSV. Which cmdlet should you run next?

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

Answer: B

Explanation:

4. Add an Active Directory Security Identifier (SID) to the CSV disk using the Cluster Name Object (CNO) The Active Directory protector is a domain security identifier (SID) based protector for protecting clustered volumes held within the Active Directory infrastructure. It can be bound to a user account, machine account or group. When an unlock request is made for a protected volume, the BitLocker service interrupts the request and uses the BitLocker protect/unprotect APIs to unlock or deny the request. For the cluster service to selfmanage

BitLocker enabled disk volumes, an administrator must add the Cluster Name Object (CNO), which is the Active Directory identity associated with the Cluster Network name, as a BitLocker protector to the target disk volumes.

Add-BitLockerKeyProtector <drive letter or CSV mount point> - ADAccountOrGroupProtector – ADAccountOrGroup \$cno

NEW QUESTION 153

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.

You mount an Active Directory snapshot on DC1.

You need to expose the snapshot as an LDAP server. Which tool should you use?

- A. Ldp
- B. ADSI Edit
- C. Dsmain
- D. Ntdsutil

Answer: C

Explanation:

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

```
Administrator: Command Prompt - dsamain -dbpath c:\$SNAP_201212101208_...
C:\Windows\system32>ntdsutil
ntdsutil: act inst ntds
Active instance set to "ntds".
ntdsutil: snap
snapshot: create
Creating snapshot...
Snapshot set {062d937f-9cdd-4286-8938-9c29ce83c8a6} generated successfully.
snapshot: list all
1: 2012/12/10:11:21 <283eb2bf-0d60-46b2-8aec-3b33c5f02204>
2:    <b23a00fc-ad43-469c-bf74-1973a0eca377>

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

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

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

snapshot: mount {062d937f-9cdd-4286-8938-9c29ce83c8a6}
Snapshot {d41683c7-ae91-48fc-a639-1e9b82138bf4} mounted as C:\$SNAP_201212101208_
_VOLUMEC$\
snapshot: quit
ntdsutil: quit

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

Current value of VM Generation ID: 6680128214492828164

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

msDS-GenerationId attribute value:
6680128214492828164

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

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

NEW QUESTION 154

- (Topic 2)

Your company has a main office and a branch office. The main office is located in Seattle. The branch office is located in Montreal. Each office is configured as an Active Directory site.

The network contains an Active Directory domain named adatum.com. The Seattle office contains a file server named Server1. The Montreal office contains a file server named Server2.

The servers run Windows Server 2012 R2 and have the File and Storage Services server role, the DFS Namespaces role service, and the DFS Replication role service installed.

Server1 and Server2 each have a share named Share1 that is replicated by using DFS Replication.

You need to ensure that users connect to the replicated folder in their respective office when they connect to \\contoso.com\Share1.

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

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

Answer: BCE

Explanation:

To share a replicated folder and publish it to a DFS namespace Click Start, point to Administrative Tools, and then click DFS Management. In the console tree, under the Replication node, click the replication group that contains the replicated folder you want to share. In the details pane, on the Replicated Folders tab, right-click the replicated folder that you want to share, and then click Share and Publish in Namespace. In the Share and Publish Replicated Folder Wizard, click Share and publish the replicated folder in a namespace, and then follow the steps in the wizard.

Note that: If you do not have an existing namespace, you can create one in the Namespace Path page in the Share and Publish Replicated Folder Wizard. To create the namespace, in the Namespace Path page, click Browse, and then click New Namespace.

To create a namespace

Click Start, point to Administrative Tools, and then click DFS Management.

In the console tree, right-click the Namespaces node, and then click New Namespace. Follow the instructions in the New Namespace Wizard.

To create a stand-alone namespace on a failover cluster, specify the name of a clustered file server instance on the Namespace Server page of the New Namespace Wizard.

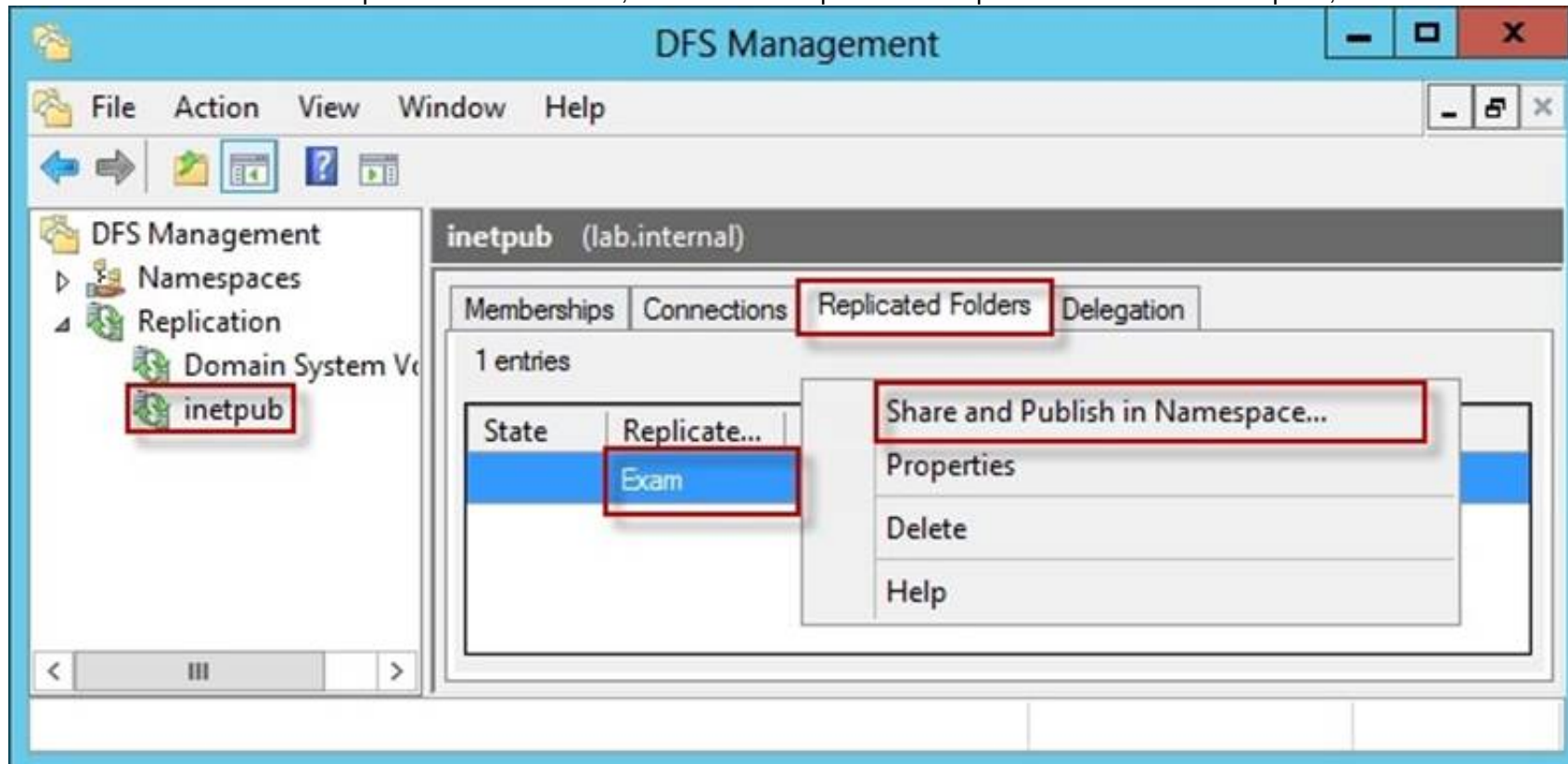
Important

Do not attempt to create a domain-based namespace using the Windows Server 2008 mode unless the forest functional level is Windows Server 2003 or higher.

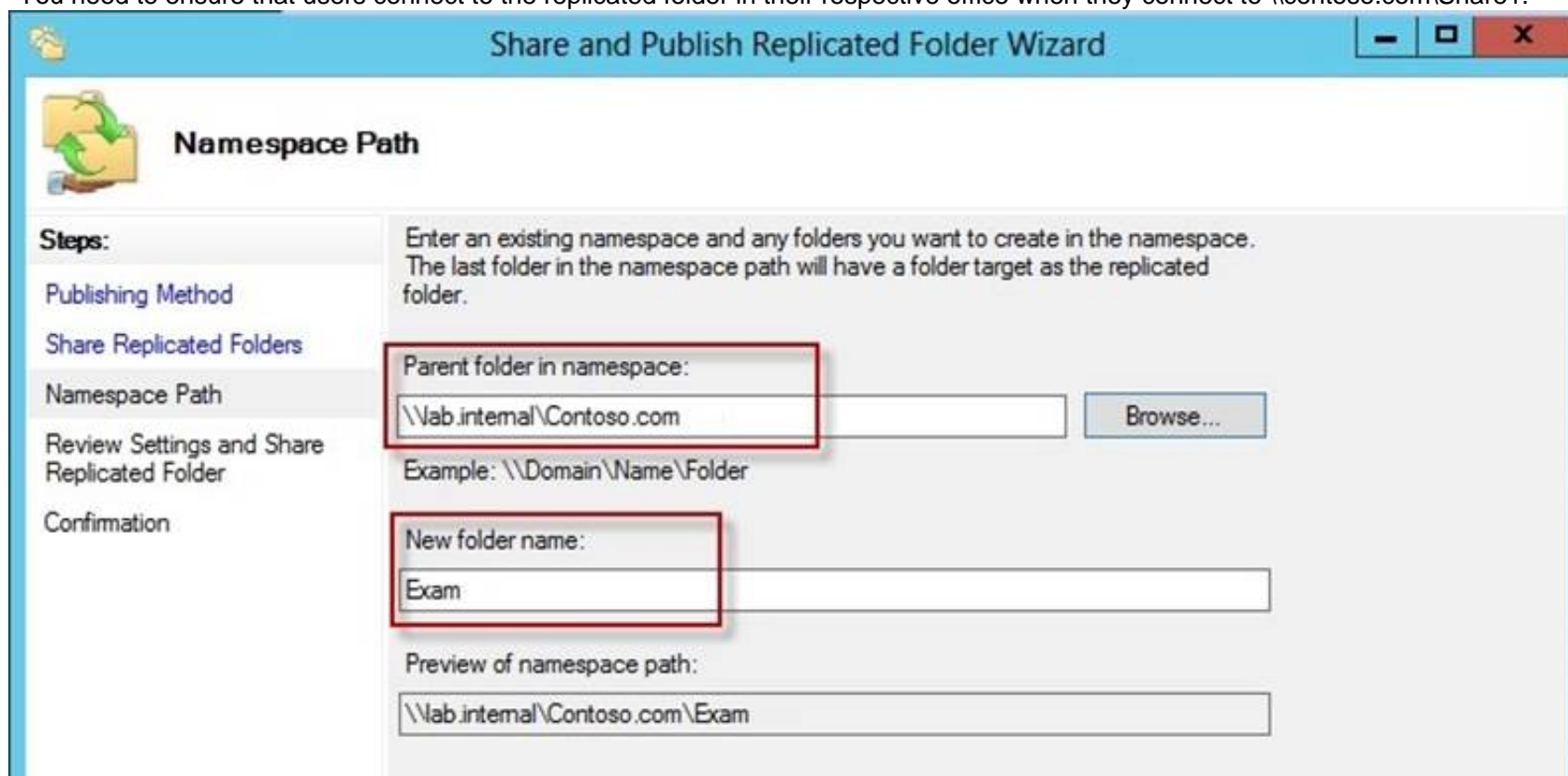
Doing so can result in a namespace for which you cannot delete DFS folders, yielding the following error message: "The folder cannot be deleted. Cannot complete this function."

To share a replicated folder and publish it to a DFS namespace

1. Click Start, point to Administrative Tools, and then click DFS Management.
2. In the console tree, under the Replication node, click the replication group that contains the replicated folder you want to share.
3. In the details pane, on the Replicated Folders tab, right-click the replicated folder that you want to share, and then click Share and Publish in Namespace.
4. In the Share and Publish Replicated Folder Wizard, click Share and publish the replicated folder in a namespace, and then follow the steps in the wizard.



"You need to ensure that users connect to the replicated folder in their respective office when they connect to \\contoso.com\Share1."



inetpub Properties

General Referrals Advanced

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

Cache duration (in seconds): 1800

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

☒ Exclude targets outside of the client's site

Effective referral ordering:
Exclude targets outside of the client's site

☒ Clients fail back to preferred targets

Effective failback mode for clients:
Enabled

OK Cancel Apply

Reference:

<http://technet.microsoft.com/en-us/library/cc731531.aspx>
<http://technet.microsoft.com/en-us/library/cc772778%28v=ws.10%29.aspx>
<http://technet.microsoft.com/en-us/library/cc732414.aspx>
<http://technet.microsoft.com/en-us/library/cc772379.aspx>
<http://technet.microsoft.com/en-us/library/cc732863%28v=ws.10%29.aspx>
<http://technet.microsoft.com/en-us/library/cc725830.aspx>
<http://technet.microsoft.com/en-us/library/cc771978.aspx>

NEW QUESTION 159

- (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 161

- (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?

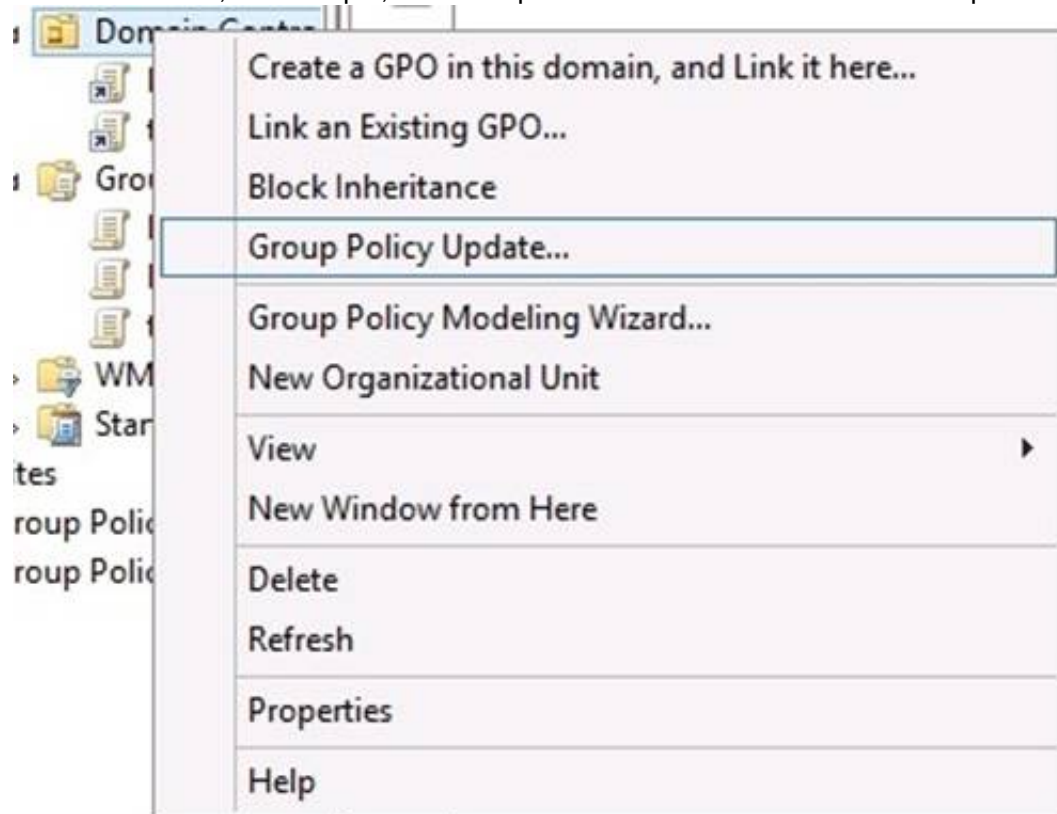
- A. The Secedit command
- B. Group Policy Management Console (GPMC)
- C. Server Manager
- D. The Gpupdate command

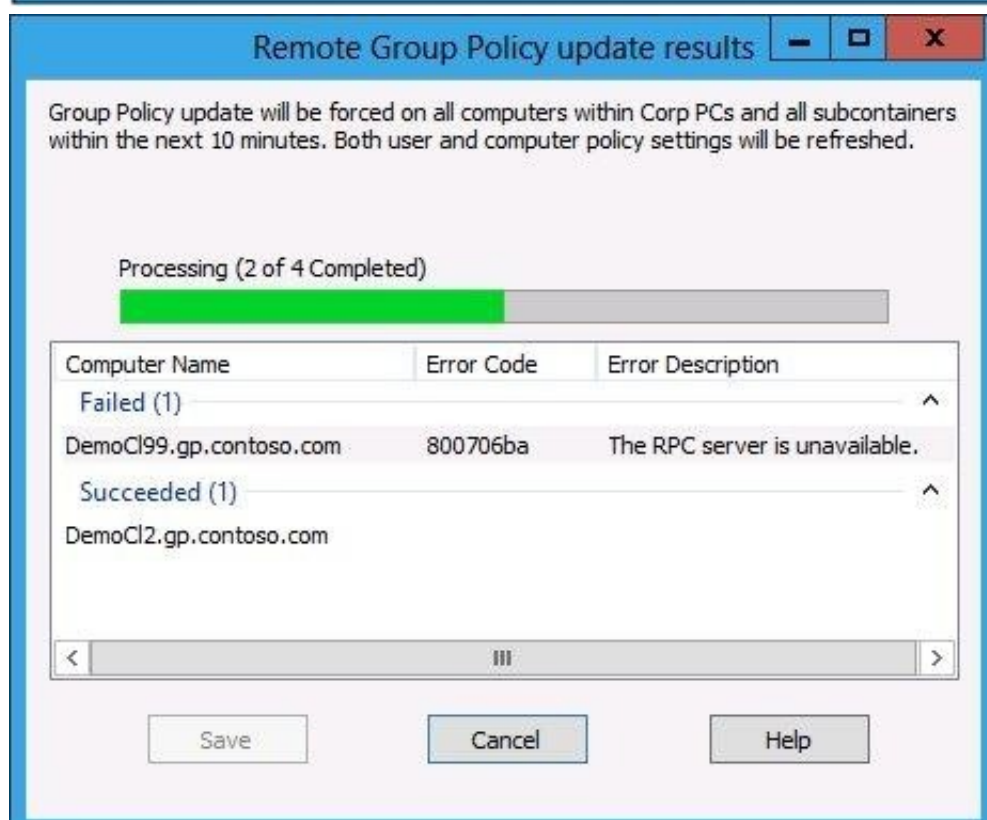
Answer: B

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 165

- (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. The Invoke-GpUpdate cmdlet
- C. Group Policy Object Editor
- D. Server Manager

Answer: B

Explanation:

Invoke-GPUpdate

Schedule a remote Group Policy refresh (gpupdate) on the specified computer. Applies To: Windows Server 2012 R2

The Invoke-GPUpdate cmdlet refreshes Group Policy settings, including security settings that are set on remote computers by scheduling the running of the Gpupdate command on a remote computer. You can combine this cmdlet in a scripted fashion to schedule the Gpupdate command on a group of computers.

The refresh can be scheduled to immediately start a refresh of policy settings or wait for a specified period of time, up to a maximum of 31 days. To avoid putting a load on the network, the refresh times will be offset by a random delay.

Note:

Group Policy is a complicated infrastructure that enables you to apply policy settings to remotely configure a computer and user experience within a domain. When the Resultant Set of Policy settings does not conform to your expectations, a best practice is to first verify that the computer or user has received the latest policy settings. In previous versions of Windows, this was accomplished by having the user run GpUpdate.exe on their computer. With Windows Server 2012 R2 and Windows 8, you can remotely refresh Group Policy settings for all computers in an organizational unit (OU) from one central location by using the Group Policy Management Console (GPMC). Or you can use the Invoke-GPUpdate Windows PowerShell cmdlet to refresh Group Policy for a set of computers, including computers that are not within the OU structure—for example, if the computers are located in the default computers container.

The remote Group Policy refresh updates all Group Policy settings, including security settings that are set on a group of remote computers, by using the

functionality that is added to the context menu for an OU in the Group Policy Management Console (GPMC). When you select an OU to remotely refresh the Group Policy settings on all the computers in that OU, the following operations happen:

- ? An Active Directory query returns a list of all computers that belong to that OU.
- ? For each computer that belongs to the selected OU, a WMI call retrieves the list of signed in users.
- ? A remote scheduled task is created to run GPUpdate.exe /force for each signed in user and once for the computer Group Policy refresh. The task is scheduled to run with a random delay of up to 10 minutes to decrease the load on the network traffic. This random delay cannot be configured when you use the GPMC, but you can configure the random delay for the scheduled task or set the scheduled task to run immediately when you use the Invoke-GPUpdate cmdlet.

Reference: Force a Remote Group Policy Refresh (GPUpdate)

NEW QUESTION 166

- (Topic 2)

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

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

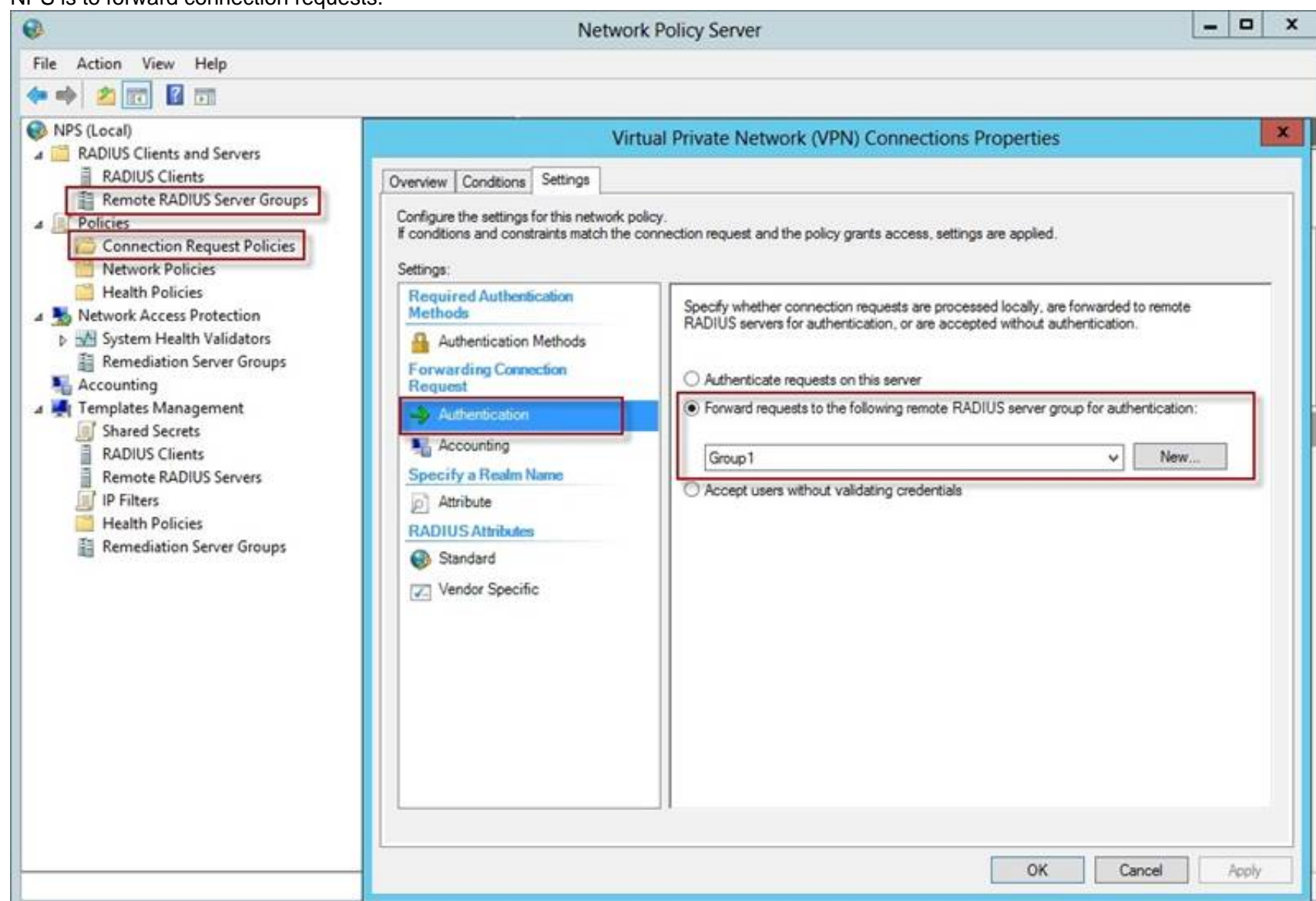
Answer: BC

Explanation:

To configure NPS as a RADIUS proxy, you must create a connection request policy that contains all of the information required for NPS to evaluate which messages to forward and where to send the messages.

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

When you configure a remote RADIUS server group in NPS and you configure a connection request policy with the group, you are designating the location where NPS is to forward connection requests.



References:

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

NEW QUESTION 169

- (Topic 2)

You have a server that runs Windows Server 2012 R2.

You have an offline image named Windows2012.vhd that contains an installation of Windows Server 2012 R2.

You plan to apply several updates to Windows2012.vhd. You need to mount Wmdows2012.vhd to D:\Mount. Which tool should you use?

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

Answer: D

Explanation:

You can use the Deployment Image Servicing and Management (DISM) tool to mount a Windows image from a WIM or VHD file. Mounting an image maps the contents of the image to a directory so that you can service the image using DISM without booting into the image. You can also perform common file operations, such as copying, pasting, and editing on a mounted image.

To apply packages and updates to a Windows Embedded Standard 7 image, we recommend creating a configuration set and then using Deployment Imaging Servicing and Management (DISM) to install that configuration set. Although DISM can be used to install individual updates to an image, this method carries some additional risks and is not recommended.

NEW QUESTION 170

- (Topic 2)

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

The network contains several group Managed Service Accounts that are used by four member servers.

You need to ensure that if a group Managed Service Account resets a password of a domain user account, an audit entry is created.

You create a Group Policy object (GPO) named GPO1. What should you do next?

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

Answer: A

Explanation:

Audit User Account Management

This security policy setting determines whether the operating system generates audit events when the following user account management tasks are performed:

? A user account is created, changed, deleted, renamed, disabled, enabled, locked out, or unlocked.

? A user account password is set or changed.

? Security identifier (SID) history is added to a user account.

? The Directory Services Restore Mode password is set.

? Permissions on accounts that are members of administrators groups are changed.

? Credential Manager credentials are backed up or restored.

This policy setting is essential for tracking events that involve provisioning and managing user accounts.

NEW QUESTION 172

- (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?

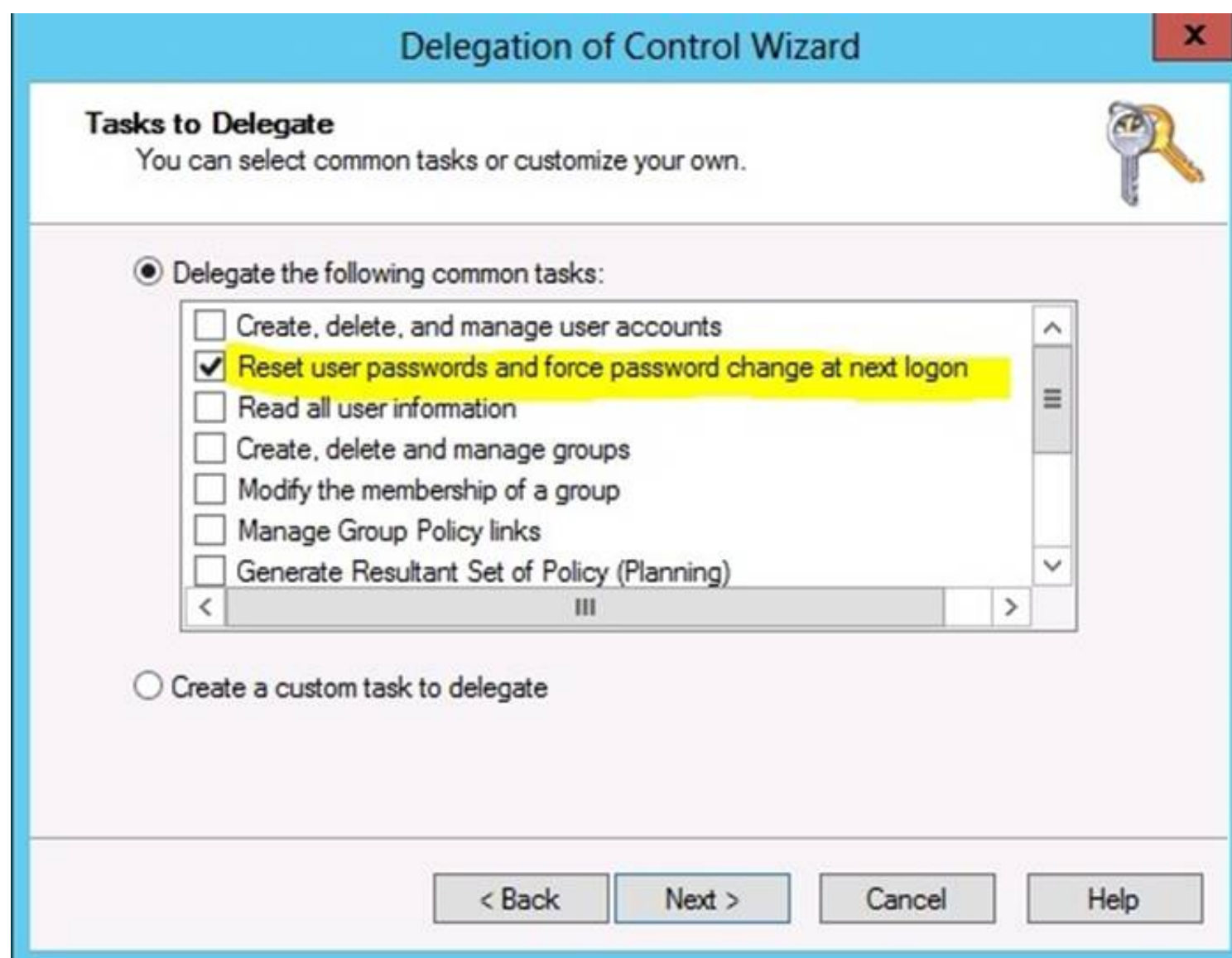
- A. Run the Set-ADAccountPasswordcmdlet and specify the -identity parameter.
- B. Right-click the Sales OU and select Delegate Control.
- C. Right-click the IT OU and select Delegate Control.
- D. Run the Set-ADFineGrainedPasswordPolicycmdlet and specify the -identity parameter.

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 177

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.

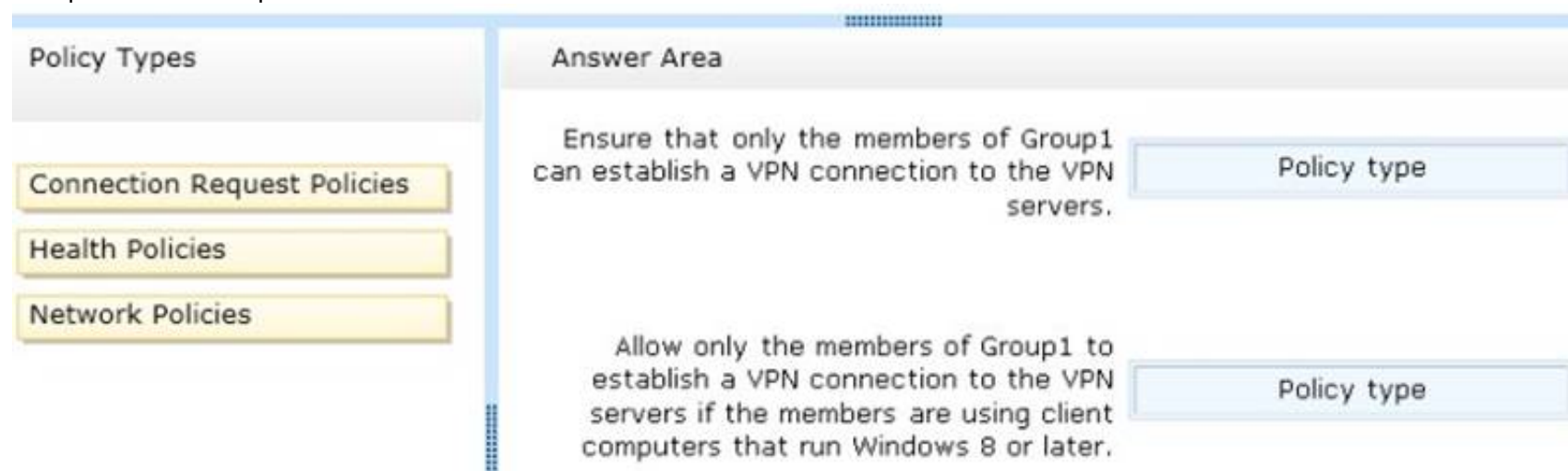
You need to configure Network Policy and Access Services (NPAS) to meet the following requirements:

? 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.

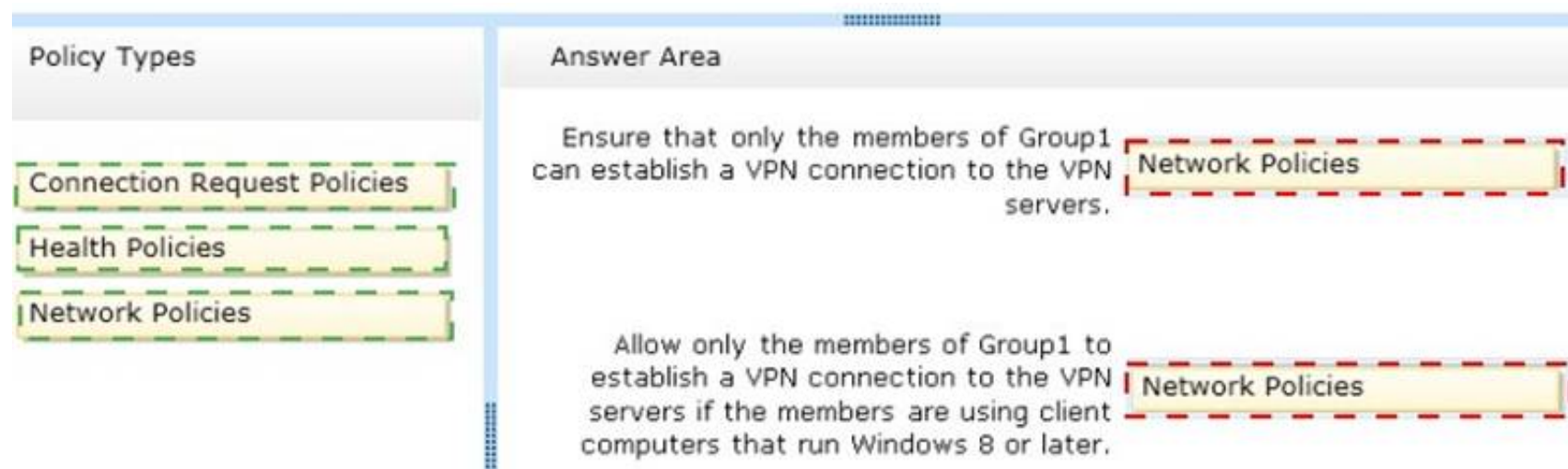


A. Mastered

B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 181

- (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.

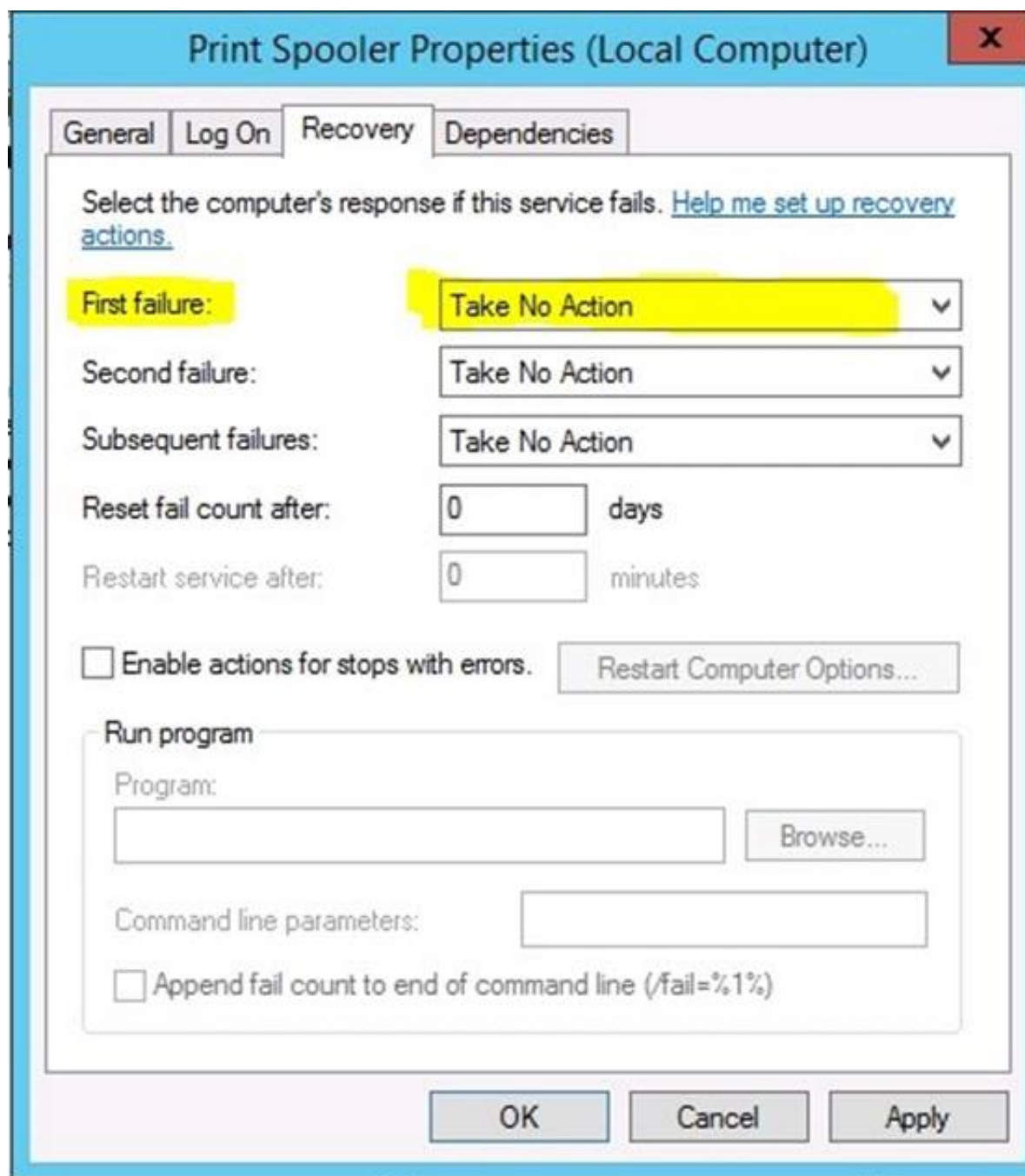
Windows Server 2012 Failover Cluster introduces a new capability for Hyper-V virtual machines (VMs), which is a basic monitoring of a service within the VM which causes the VM to be rebooted should the monitored service fail three times. For this feature to work the following must be configured:

? 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).

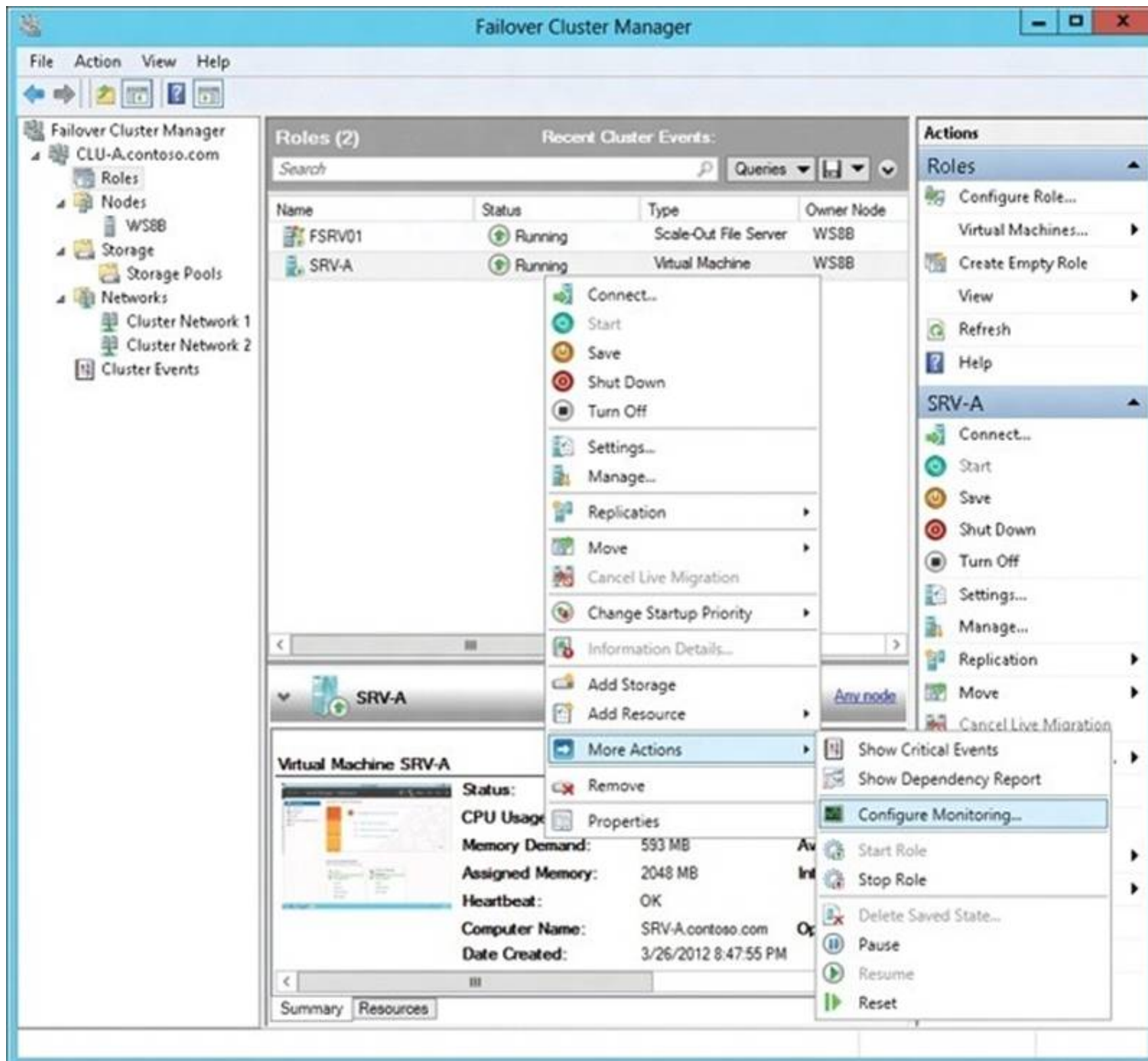


Within the guest VM, ensure the Virtual Machine Monitoring firewall exception is enabled for the Domain network by using the Windows Firewall with Advanced Security application or by using the Windows PowerShell command below: `Set-NetFirewallRule -DisplayGroup "Virtual Machine Monitoring" -Enabled True`.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

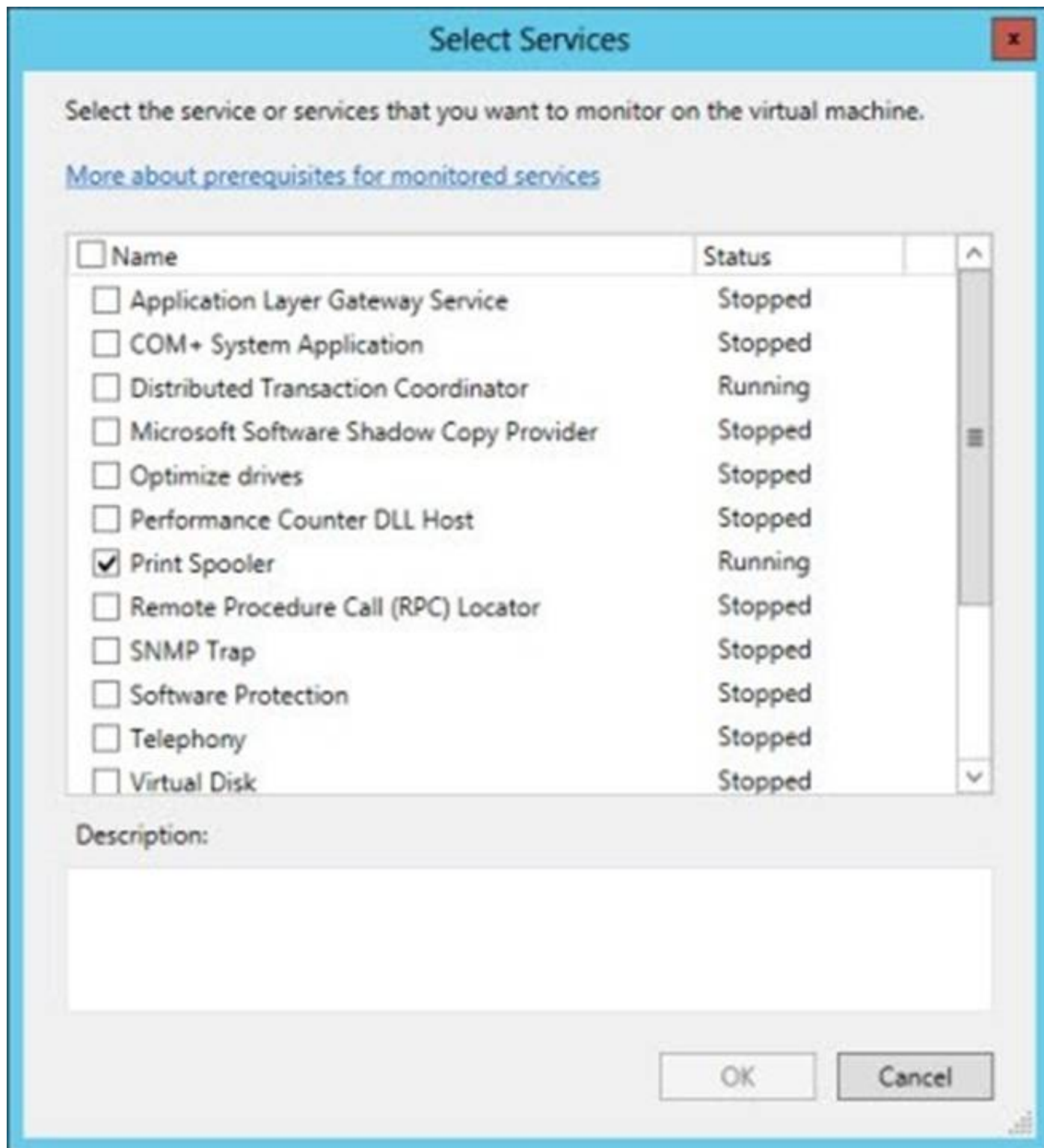
? Launch the Failover Cluster Manager tool.

? 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 182

- (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.

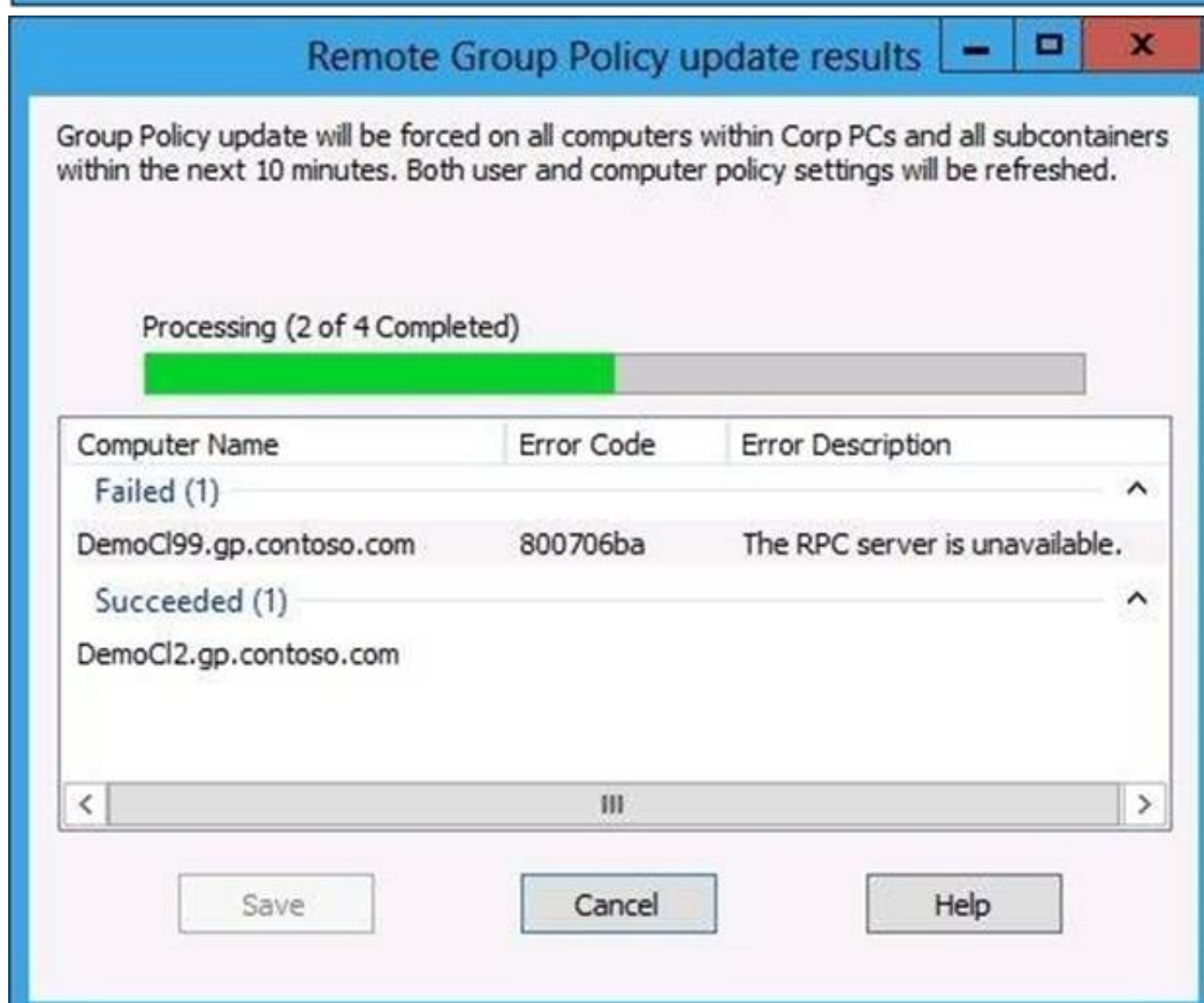
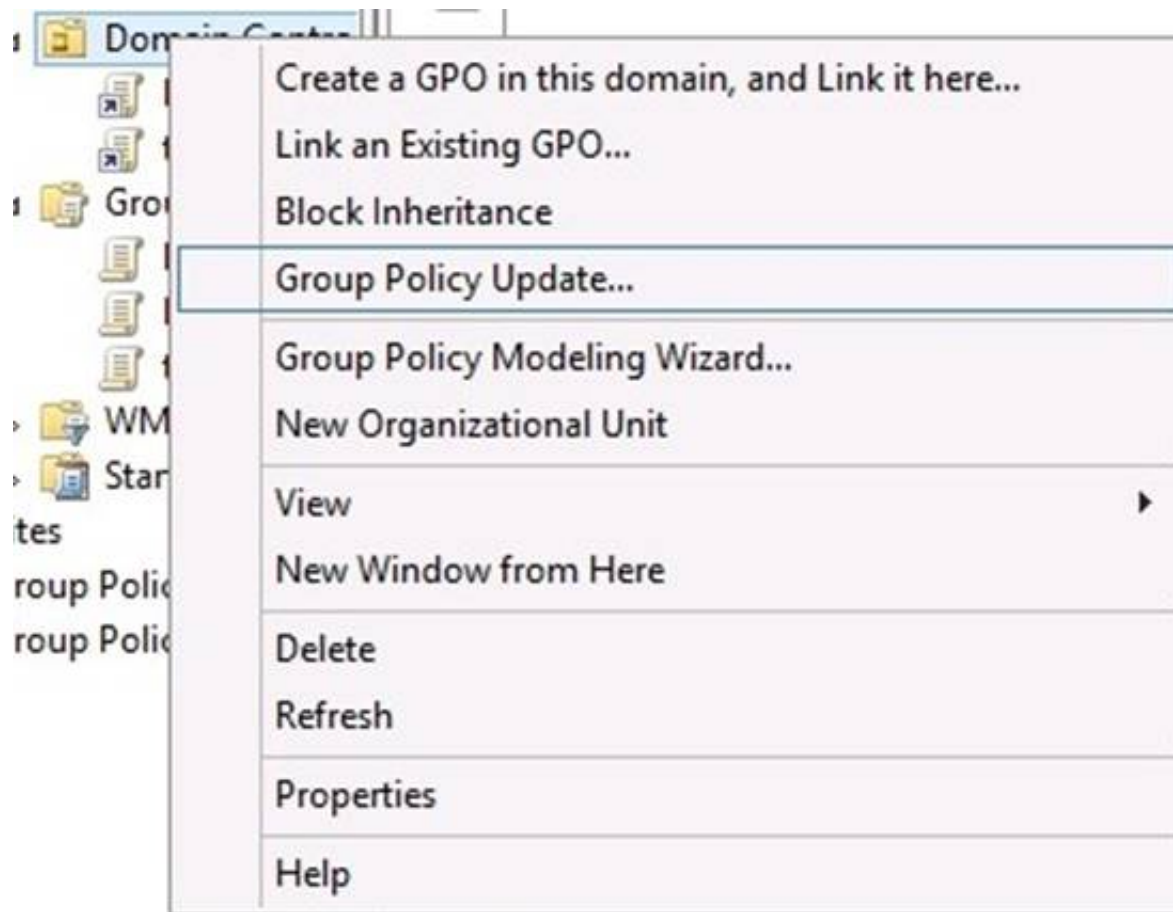
Which tool should you use?

- A. Server Manager
- B. Active Directory Users and Computers
- C. The Gpupdate command
- D. Group Policy Management Console (GPMC)

Answer: D

Explanation:

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.



References:

<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 185

- (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.

Each time a user receives an access-denied message after attempting to access a folder on Server1, an email notification is sent to a distribution list named DL1.

You create a folder named Folder1 on Server1, and then you configure custom NTFS permissions for Folder 1.

You need to ensure that when a user receives an access-denied message while attempting to access Folder1, an email notification is sent to a distribution list named DL2. The solution must not prevent DL1 from receiving notifications about other access-denied messages.

What should you do?

- A. From File Explorer, modify the Classification tab of Folder1.
- B. From the File Server Resource Manager console, modify the Email Notifications settings.
- C. From the File Server Resource Manager console, set a folder management property.
- D. From File Explorer, modify the Customize tab of Folder1.

Answer: C

Explanation:

When using the email model each of the file shares, you can determine whether access requests to each file share will be received by the administrator, a distribution list that represents the file share owners, or both.

You can use the File Server Resource Manager console to configure the owner distribution list by editing the management properties of the classification properties.

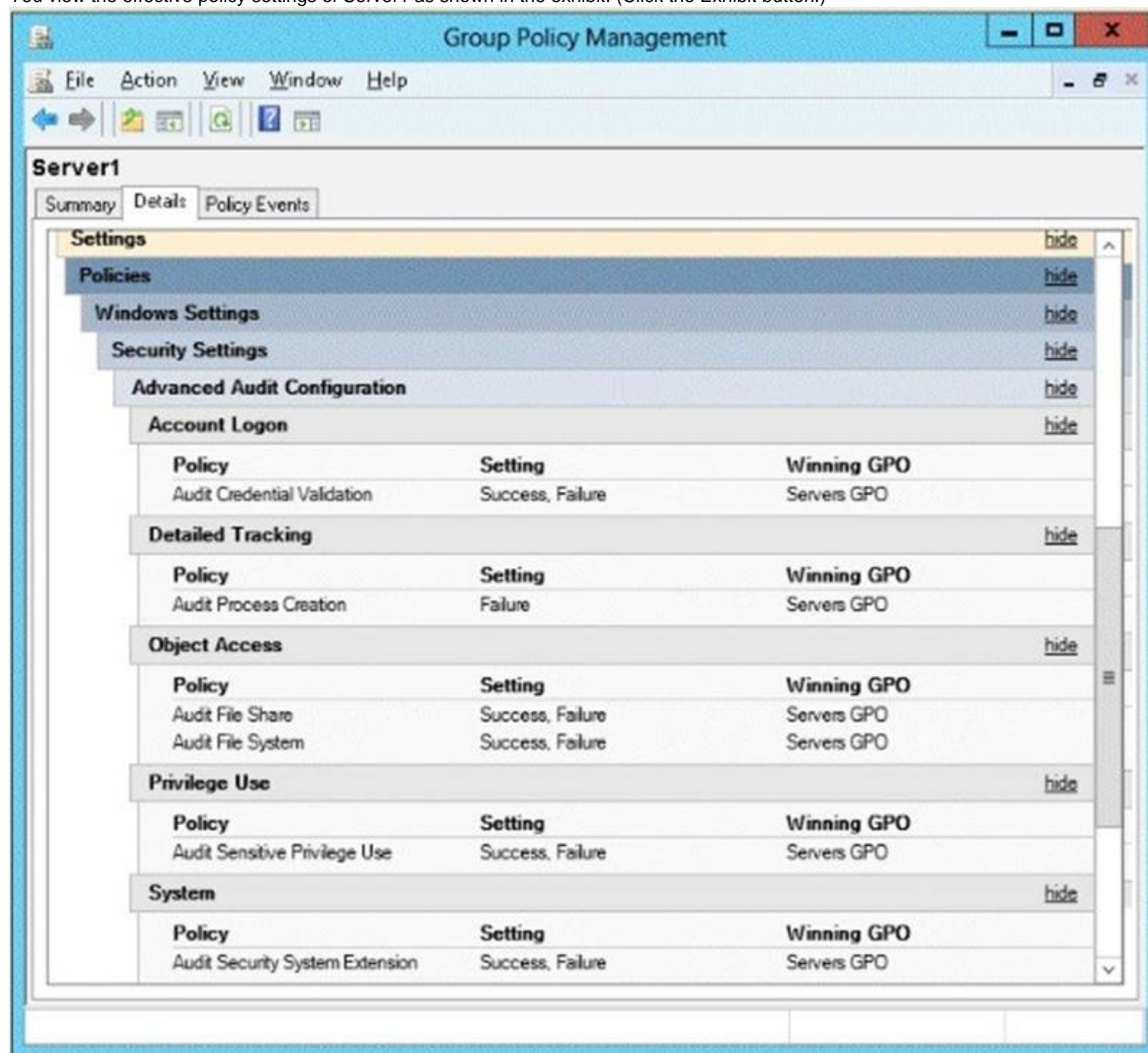
Reference: http://technet.microsoft.com/en-us/library/jj574182.aspx#BKMK_12

NEW QUESTION 188

- (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.)



On Server1, you have a folder named C:\Share1 that is shared as Share1. Share1 contains confidential data. A group named Group1 has full control of the content in Share1.

You need to ensure that an entry is added to the event log whenever a member of Group1 deletes a file in Share1.

What should you configure?

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

Answer: D

Explanation:

You can use Computer Management to track all connections to shared resources on a Windows Server 2008 R2 system.

Whenever a user or computer connects to a shared resource, Windows Server 2008 R2 lists a connection in the Sessions node.

File access, modification and deletion can only be tracked, if the object access auditing is enabled you can see the entries in the event log.

To view connections to shared resources, type net session at a command prompt or follow these steps:

? In Computer Management, connect to the computer on which you created the shared resource.

? In the console tree, expand System Tools, expand Shared Folders, and then select Sessions. You can now view connections to shares for users and computers.

To enable folder permission auditing, you can follow the below steps:

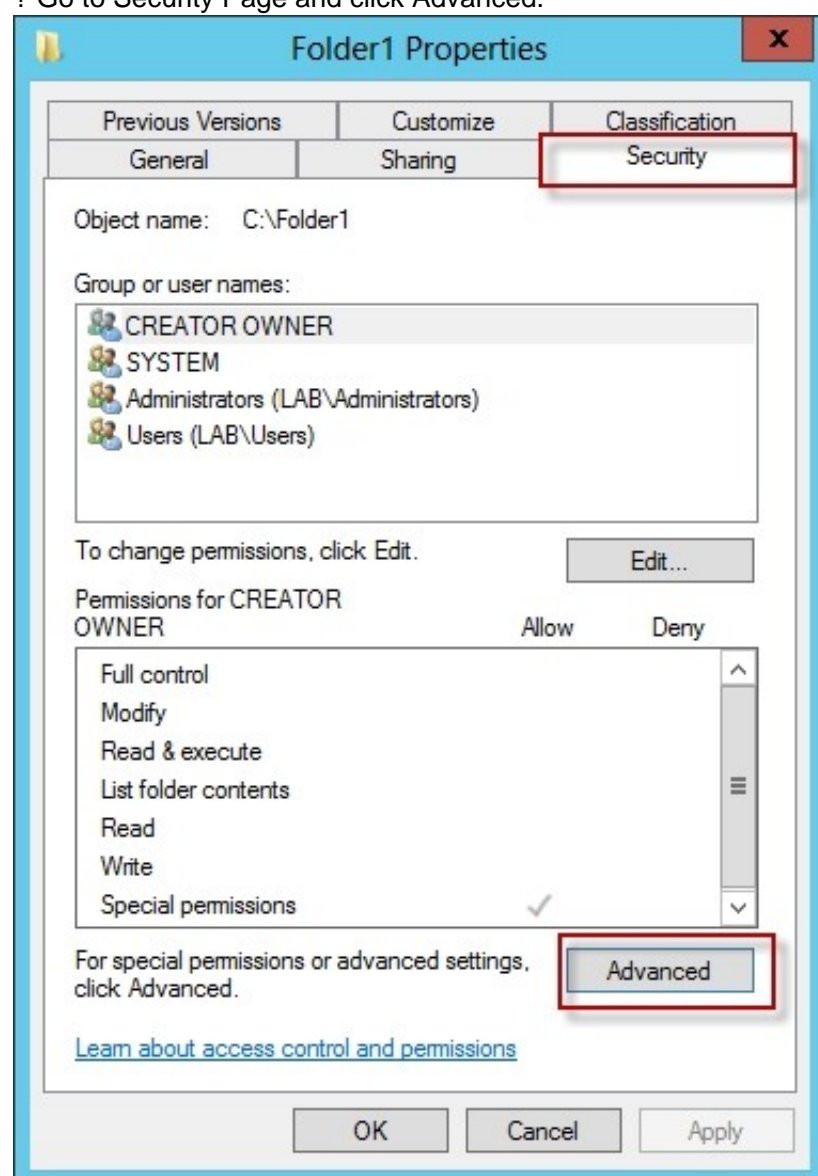
? Click start and run "secpol. msc" without quotes.

? Open the Local Policies\Audit Policy

? Enable the Audit object access for "Success" and "Failure".

? Go to target files and folders, right click the folder and select properties.

? Go to Security Page and click Advanced.



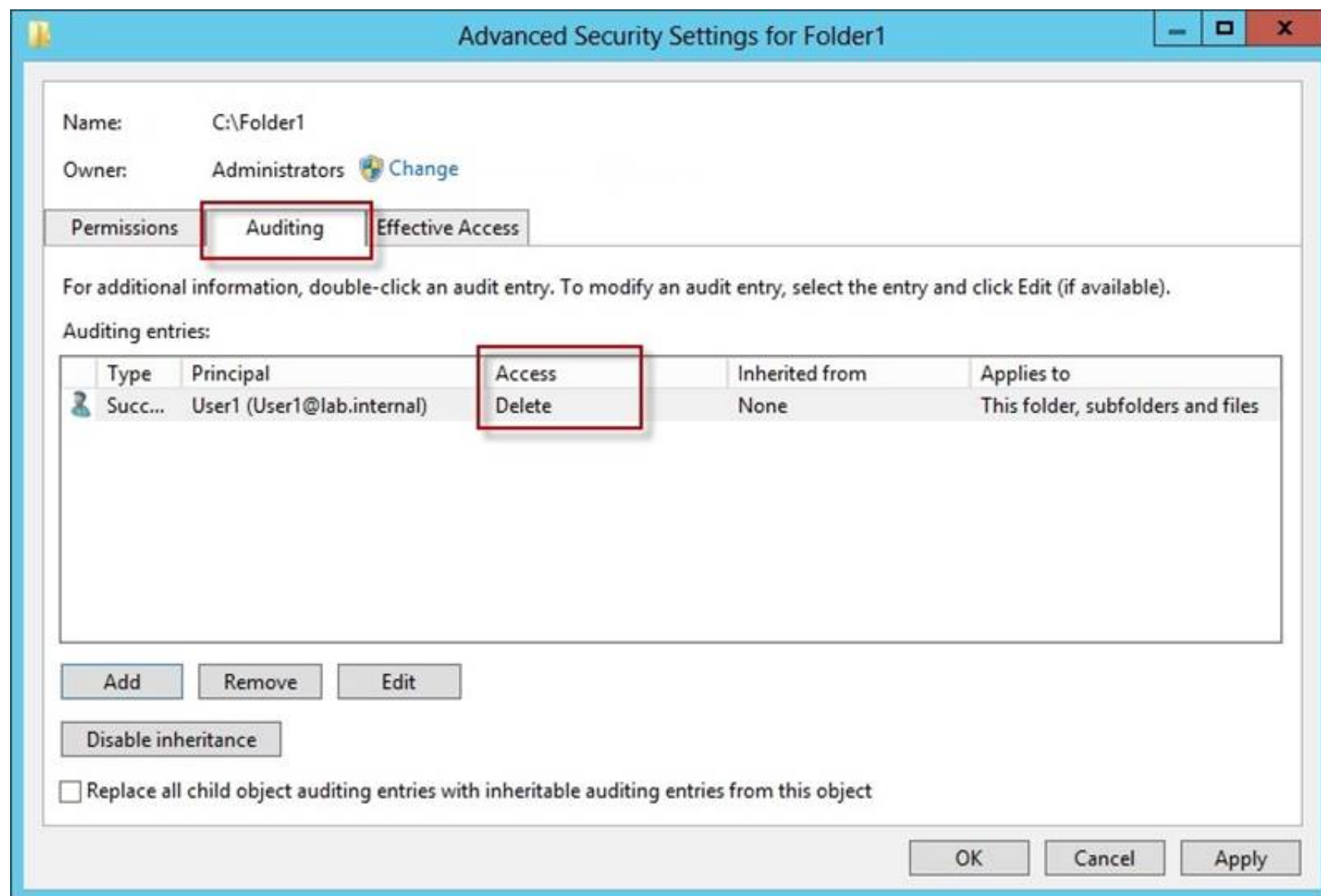
? Click Auditing and Edit.

? Click add, type everyone in the Select User, Computer, or Group.

? Choose Apply onto: This folder, subfolders and files.

? Tick on the box "Change permissions"

? Click OK.



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

References:

<http://social.technet.microsoft.com/Forums/en-US/winservergen/thread/13779c78-0c73-4477-8014-f2eb10f3f10f/>

[http://technet.microsoft.com/en-us/library/cc753927\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc753927(v=ws.10).aspx)

<http://social.technet.microsoft.com/Forums/en-US/winservergen/thread/13779c78-0c73-4477-8014-f2eb10f3f10f/>

<http://support.microsoft.com/kb/300549>

<http://www.windowsitpro.com/article/permissions/auditing-folder-permission-changes> <http://www.windowsitpro.com/article/permissions/auditing-permission-changes-on-a-folder>

NEW QUESTION 191

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 70-411 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 70-411 Product From:

<https://www.2passeasy.com/dumps/70-411/>

Money Back Guarantee

70-411 Practice Exam Features:

- * 70-411 Questions and Answers Updated Frequently
- * 70-411 Practice Questions Verified by Expert Senior Certified Staff
- * 70-411 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 70-411 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year