70-411.microsoft

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

https://vceplus.com/

Sections
1. Volume A
2. Volume B

Exam A

QUESTION 1
Your network contains an Active Directory domain named adatum.com.

A network administrator creates a Group Policy central store.

After the central store is created, you discover that when you create new Group Policy objects (GPOs), the GPOs do not contain any Administrative Templates.

You need to ensure that the Administrative Templates appear in new GPOs.

What should you do?

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

Correct Answer: C
Section: Volume A
Explanation

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

QUESTION 2
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains 500 client computers that run Windows 8 Enterprise.

You implement a Group Policy central store.

You have an application named App1. App1 requires that a custom registry setting be deployed to all of the computers.

You need to deploy the custom registry setting. The solution must minimize administrator effort.

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

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
▪ Open the Group Policy Management Console. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click Edit. ▪
In the console tree under Computer Configuration or User Configuration, expand the Preferences folder, and then expand the Windows Settings folder. ▪
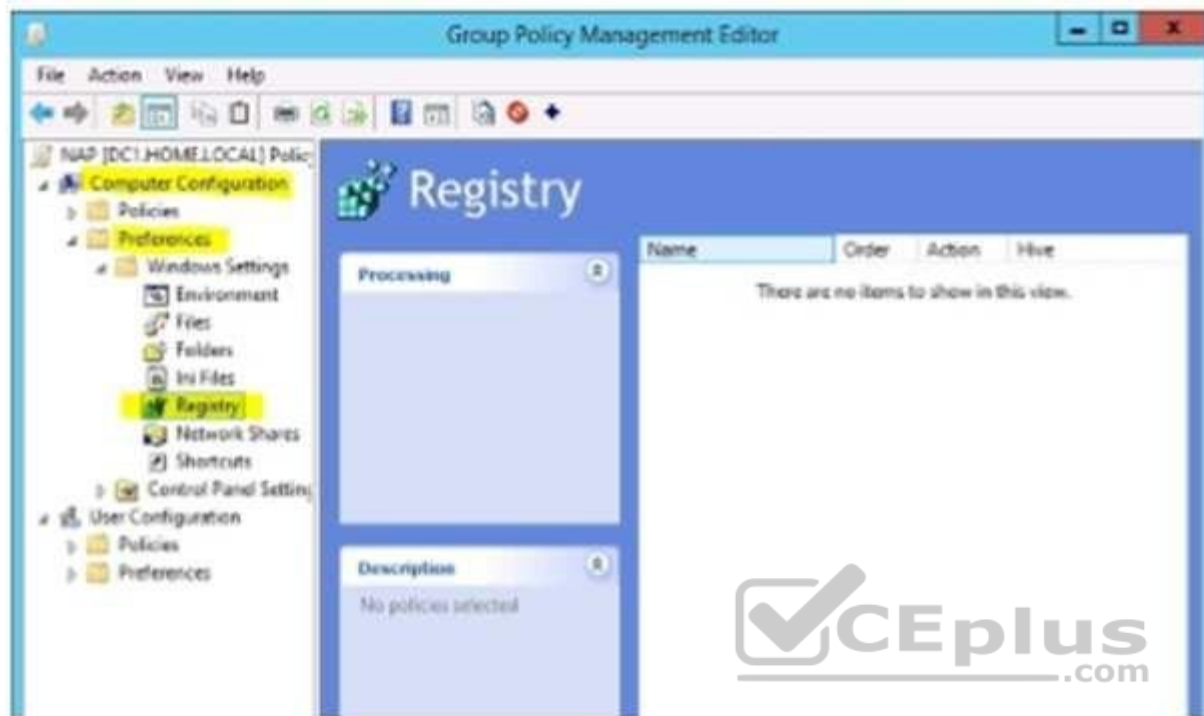Right-click the Registry node, point to New, and select Registry Item.

Group Policy preferences provide the means to simplify deployment and standardize configurations. They add to Group Policy a centralized system for deploying preferences (that is, settings that users can change later).
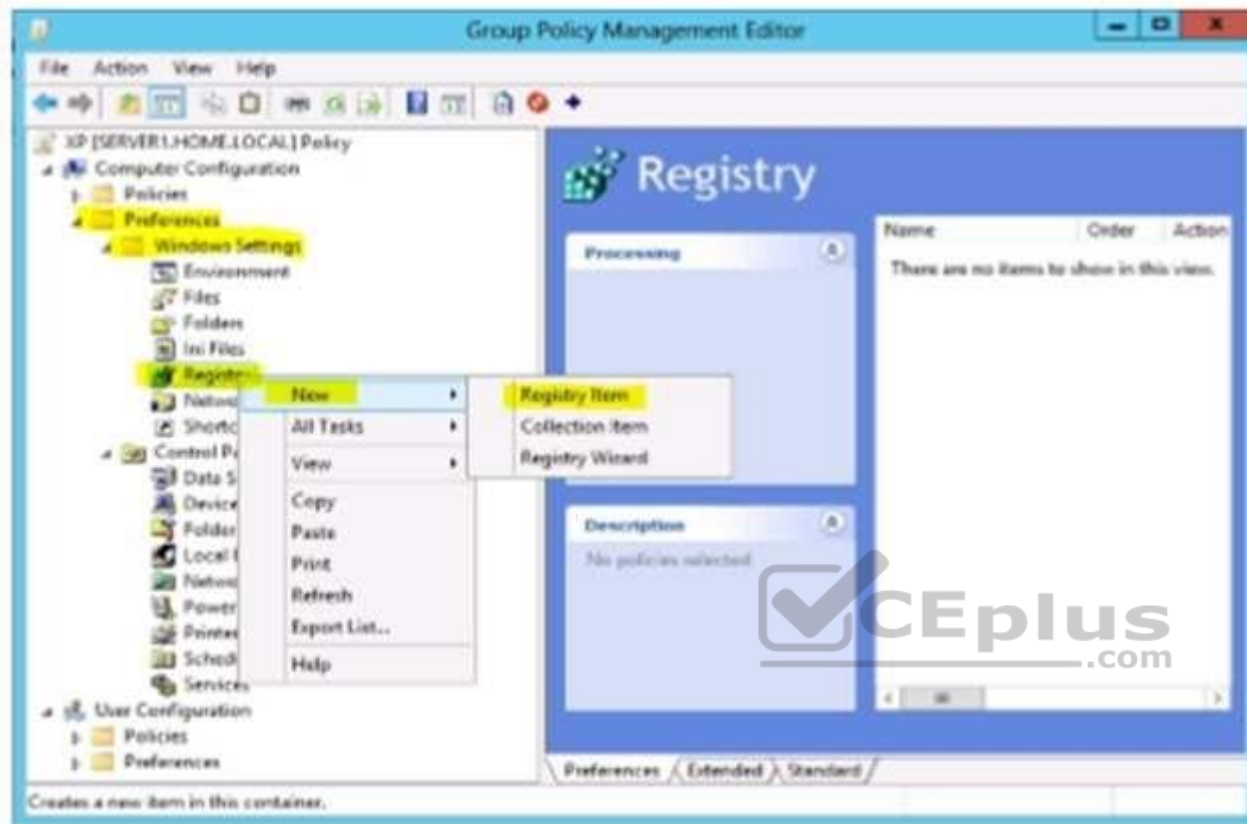
You can also use Group Policy preferences to configure applications that are not Group Policy- aware. By using Group Policy preferences, you can change or delete almost any registry setting, file or folder, shortcut, and more. You are not limited by the contents of Administrative Template files. The Group Policy Management
Editor (GPME) includes Group Policy preferences.

References:
http://technet.microsoft.com/en-us/library/gg699429.aspx
http://www.unidesk.com/blog/gpos-set-custom-registry-entries-virtual-desktops-disabling-machine-password

QUESTION 3

Your network contains two Active Directory forests named contoso.com and dev.contoso.com. The contoso.com forest contains a domain controller named DC1. The dev.contoso.com forest contains a domain controller named DC2. Each domain contains an organizational unit (OU) named OU1.

Dev.contoso.com has a Group Policy object (GPO) named GPO1. GPO1 contains 200 settings, including several settings that have network paths. GPO1 is linked to OU1.

You need to copy GPO1 from dev.contoso.com to contoso.com.

What should you do first on DC2?

A. From the Group Policy Management console, right-click GPO1 and select Copy.

B. Run the mtedit.exe command and specify the /Domaintcontoso.com /DC: DC 1 parameter.

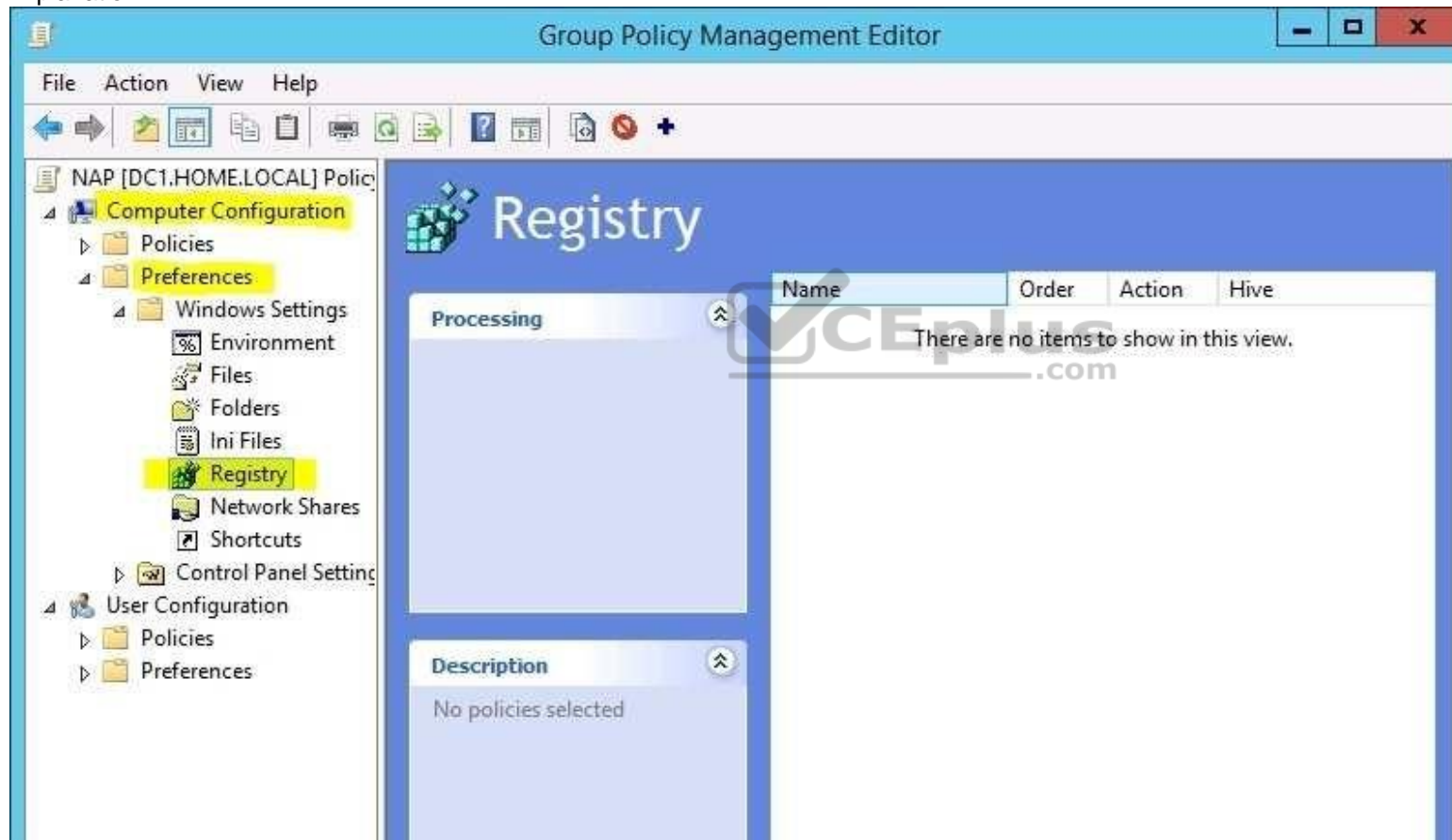C. Run the Save-NetGpocmdlet.
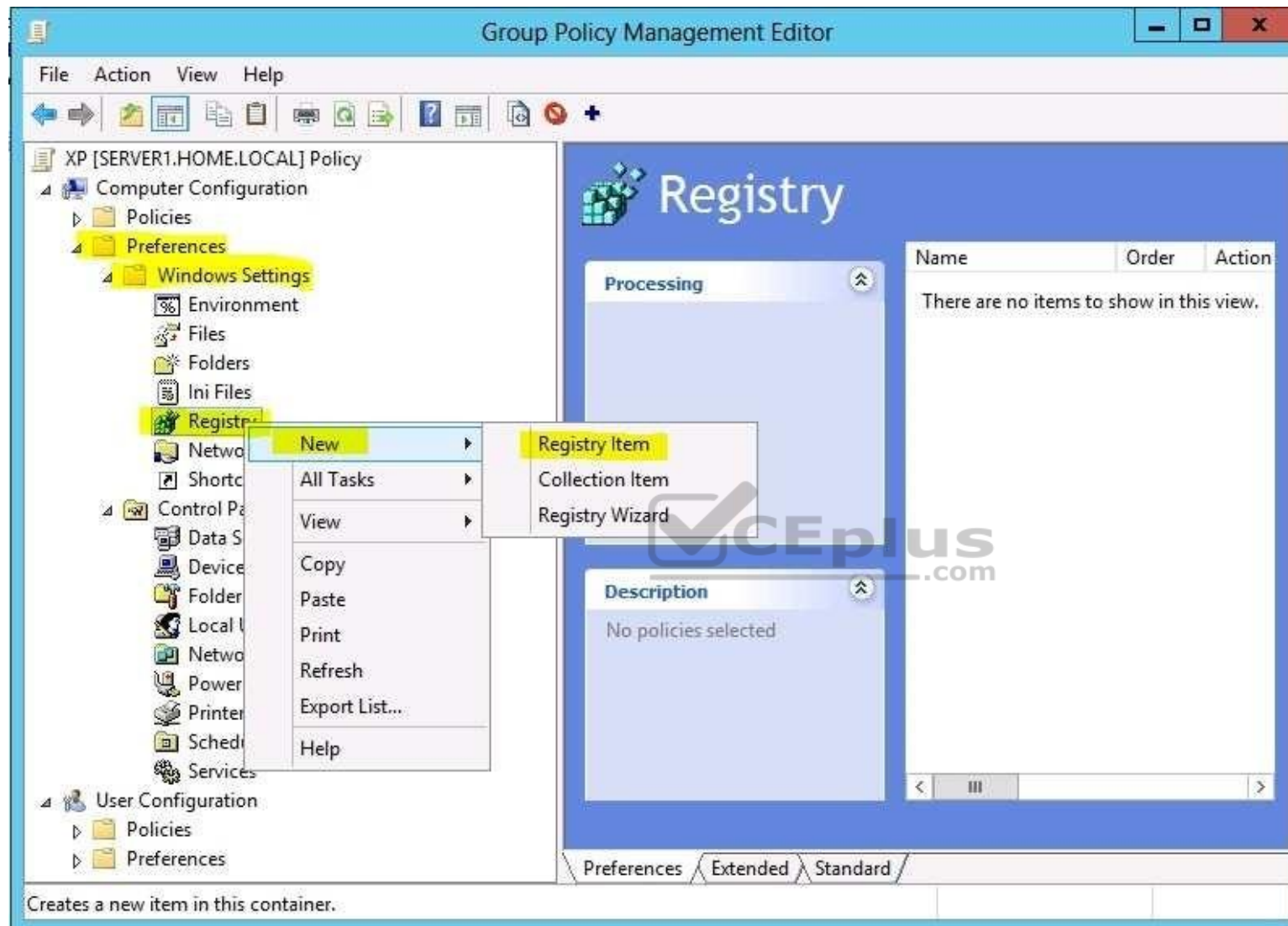
D. Run the Backup-Gpocmdlet.

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
Explanation:

To copy a Group Policy object:
In the GPMC console tree, right-click the GPO that you want to copy, and then click Copy.
To create a copy of the GPO in the same domain as the source GPO, right-click Group Policy objects, click Paste, specify permissions for the new GPO in the Copy GPO box, and then click OK.
For copy operations to another domain, you may need to specify a migration table.

The Migration Table Editor (MTE) is provided with Group Policy Management Console (GPMC) to facilitate the editing of migration tables. Migration tables are used for copying or importing Group Policy objects (GPOs) from one domain to another, in cases where the GPOs include domain-specific information that must be updated during copy or import.
Source WS2008R2: Backup the existing GPOs from the GPMC, you need to ensure that the "Group Policy Objects" container is selected for the "Backup Up All" option to be available.

Copy a Group Policy Object with the Group Policy Management Console (GPMC)
You can copy a Group Policy object (GPO) either by using the drag-and-drop method or right-click method.
Applies To: Windows 8, Windows Server 2008 R2, Windows Server 2012

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

QUESTION 4
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

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
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.

QUESTION 5
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.

Correct Answer: B
Section: Volume A
Explanation

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

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

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

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

QUESTION 6

HOTSPOT

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

Server1 and Server2 are configured as replica servers that use Server3 as an upstream server.
You remove Servers from the network.

You need to ensure that WSUS on Server2 retrieves updates from Server1. The solution must ensure that Server1 and Server2 have the latest updates from Microsoft.
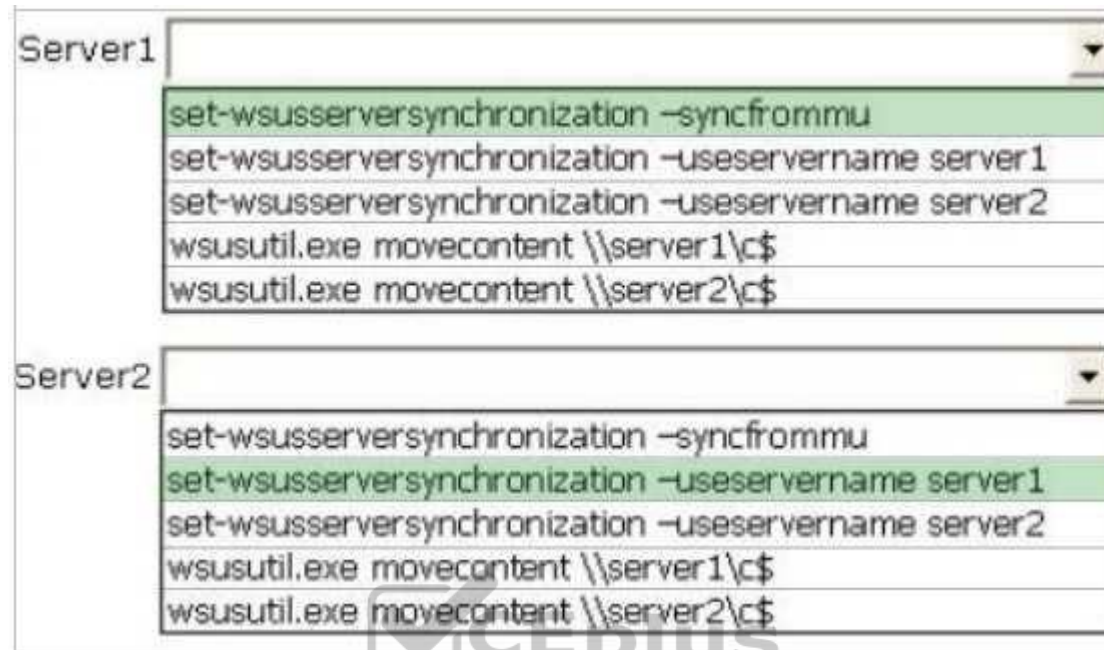
Which command should you run on each server? To answer, select the appropriate command to run on each server in the answer area.

Hot Area:

Server1	▼
set-wsusserversynchronization –syncfrommu	
set-wsusserversynchronization –useservername server1	
set-wsusserversynchronization –useservername server2	
wsusutil.exe movecontent \\server1\c$	
wsusutil.exe movecontent \\server2\c$	

Server2	▼
set-wsusserversynchronization –syncfrommu	
set-wsusserversynchronization –useservername server1	
set-wsusserversynchronization –useservername server2	
wsusutil.exe movecontent \\server1\c$	
wsusutil.exe movecontent \\server2\c$	

Correct Answer:

Server1: set-wsusserversynchronization –syncfrommu

Server2: set-wsusserversynchronization –useservername server1

Section: Volume A
Explanation

Explanation/Reference:
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

QUESTION 7
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. 00000000000000000000020CF306SD087
E. 00000000-0000-0000-0000-C41S0BB6C618

Correct Answer: CD
Section: Volume A
Explanation

Explanation/Reference:
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"

QUESTION 8
You have Windows Server 2012 R2 installation media that contains a file named Install.wim. You need to identify the permissions of the mounted images in Install.wim.

What should you do?

A. Run dism.exe and specify the /get-mountedwiminfo parameter.

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

Correct Answer: A

Section: Volume A

Explanation

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

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

QUESTION 9
You have a server named Server1 that runs Windows Server 2012 R2. You create a Data Collector Set (DCS) named DCS1.

You need to configure DCS1 to log data to D:\logs.

What should you do?

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

Correct Answer: A
Section: Volume A
Explanation
Explanation/Reference:
Explanation:
The Root Directory will contain data collected by the Data Collector Set. Change this setting if you want to store your Data Collector Set data in a different location than the default. Browse to and select the directory, or type the directory name.

To view or modify the properties of a Data Collector Set after it has been created, you can:
* Select the Open properties for this data collector set check box at the end of the Data Collector Set Creation Wizard.
* Right-click the name of a Data Collector Set, either in the MMC scope tree or in the console window, and click Properties in the context menu.

Directory tab:
In addition to defining a root directory for storing Data Collector Set data, you can specify a single Subdirectory or create a Subdirectory name format by clicking the arrow to the right of the text entry field.

QUESTION 10
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 subscription. From a Group Policy object (GPO), configure the Configure target Subscription Manager setting.
B. On Server1, create a source computer initiated subscription. From a Group Policy object (GPO), configure the Configure forwarder resource usage setting.
C. On Server1, create a collector initiated subscription. From a Group Policy object (GPO), configure the Configure forwarder resource usage setting.
D. On Server1, create a collector initiated subscription. From a Group Policy object (GPO), configure the Configure target Subscription Manager setting.

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
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.
▪ Run the following command from an elevated privilege command prompt on the Windows Server domain controller to configure Windows Remote Management: winrm qc -q.
▪ Start group policy by running the following command: %SYSTEMROOT%\System32\gpedit.msc.
▪ Under the Computer Configuration node, expand the Administrative Templates node, then expand the Windows Components node, then select the Event Forwarding node.

▪ 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.
▪ 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.

QUESTION 11
Your network contains a Hyper-V host named Hyperv1. Hyperv1 runs Windows Server 2012 R2.

Hyperv1 hosts four virtual machines named VM1, VM2, VM3, and VM4. All of the virtual machines run Windows Server 2008 R2 Service Pack 1 (SP1).

You need to view the amount of memory resources and processor resources that VM4 currently uses.

Which tool should you use on Hyperv1?

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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
Explanation:
Hyper-V Performance Monitoring Tool
Know which resource is consuming more CPU. Find out if CPUs are running at full capacity or if they are being underutilized. Metrics tracked include Total CPU utilization, Guest CPU utilization, Hypervisor CPU utilization, idle CPU utilization, etc.

WSRM is deprecated starting with Windows Server 2012
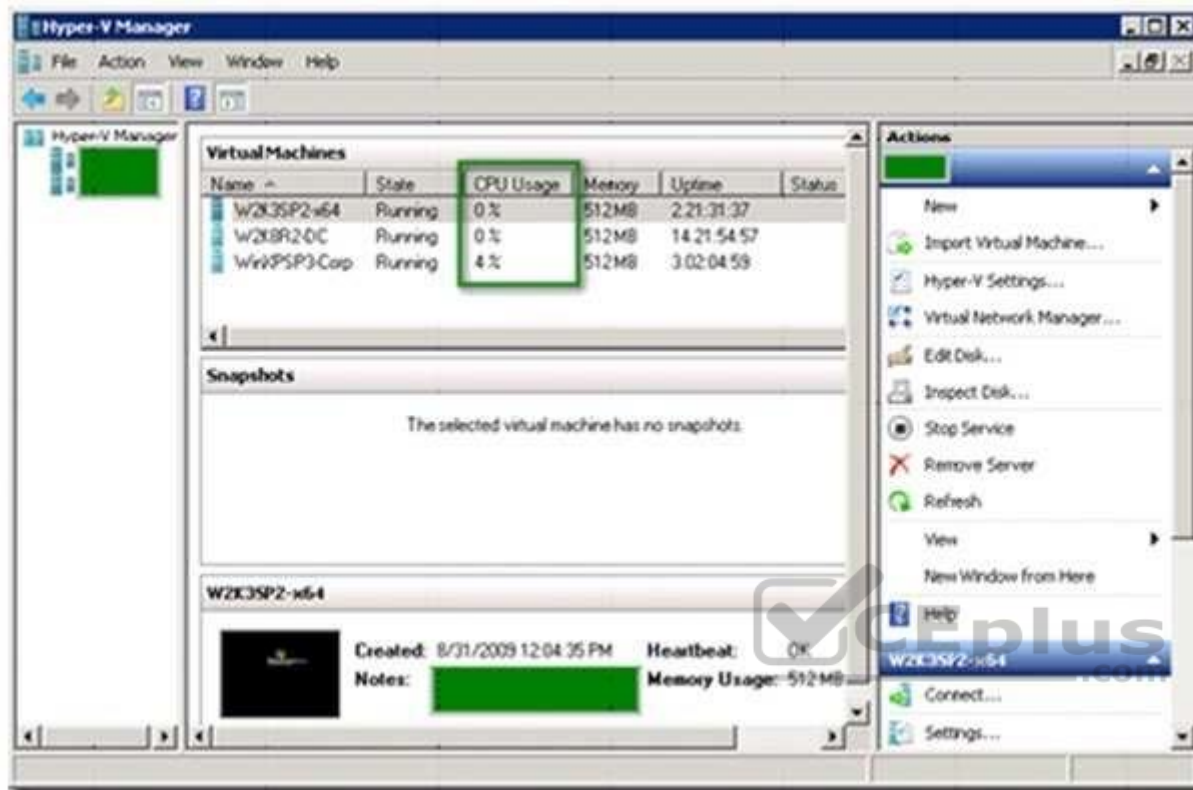
QUESTION 12

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 runs Windows Server 2012 R2 and has the Hyper-V server role installed.

Server1 hosts 10 virtual machines. A virtual machine named VM1 runs Windows Server 2012 R2 and hosts a processor-intensive application named App1.

Users report that App1 responds more slowly than expected.

You need to monitor the processor usage on VM1 to identify whether changes must be made to the hardware settings of VM1.

Which performance object should you monitor on Server1?

A. Processor

B. Hyper-V Hypervisor Virtual Processor C. Hyper-V Hypervisor Logical Processor
D. Hyper-V Hypervisor Root Virtual Processor
E. Process

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
Explanation:
In the simplest way of thinking the virtual processor time is cycled across the available logical processors in a round-robin type of fashion. Thus all the processing power gets used over time, and technically nothing ever sits idle.
To accurately measure the processor utilization of a guest operating system, use the "\Hyper-V Hypervisor Logical Processor (Total)\% Total Run Time" performance monitor counter on the Hyper-V host operating system.

QUESTION 13
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.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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

QUESTION 14
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2.

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

You need to generate an audit event whenever Admin1 is denied access to a file or folder.

What should you run?

A. **auditpol.exe /set /user:admin1 /failure:enable**

B. **auditpol.exe /set /user:admin1 /category:"detailed tracking" /failure:enable**

C. **auditpol.exe /resourcesacl /set /type:file /user:admin1 /failure**

D. **auditpol.exe /resourcesacl /set /type:key /user: admin1 /failure /access:ga**

Correct Answer: C
Section: Volume A

Explanation

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

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

Syntax

auditpol /resourceSACL
[/set /type: <resource> [/success] [/failure] /user: <user> [/access: <access flags>]]
[/remove/type: <resource>/user: <user> [/type: <resource>]]
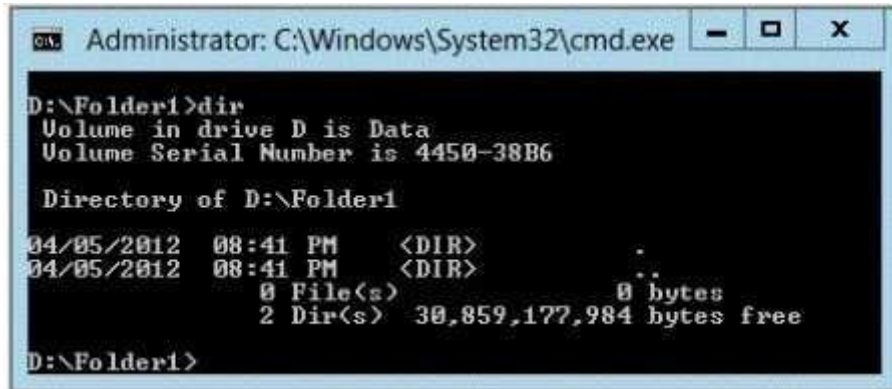[/clear [/type: <resource>]]
[/view [/user: <user>] [/type: <resource>]]

References:
http://technet.microsoft.com/en-us/library/ff625687(v=ws.10).aspx http://technet.microsoft.com/en-
us/library/ff625687.aspx **QUESTION 15**
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.)
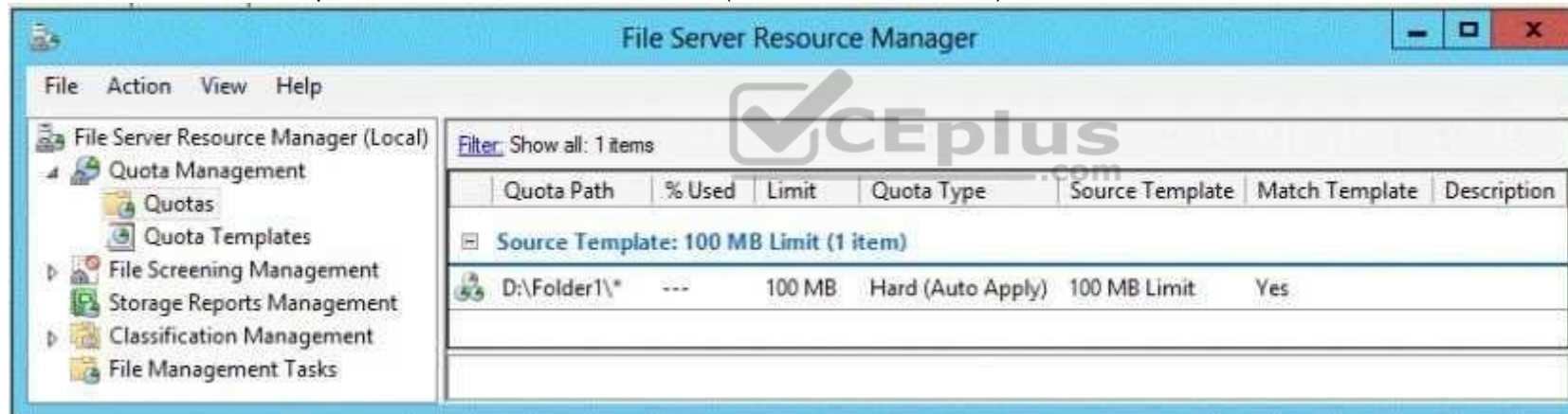
You run the dir command as shown in the Dir exhibit. (Click the Exhibit button.)

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

 Directory of D:\Folder1

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

D:\Folder1>
```

You need to ensure that D:\Folder1 can only consume 100 MB of disk space.

What should you do?

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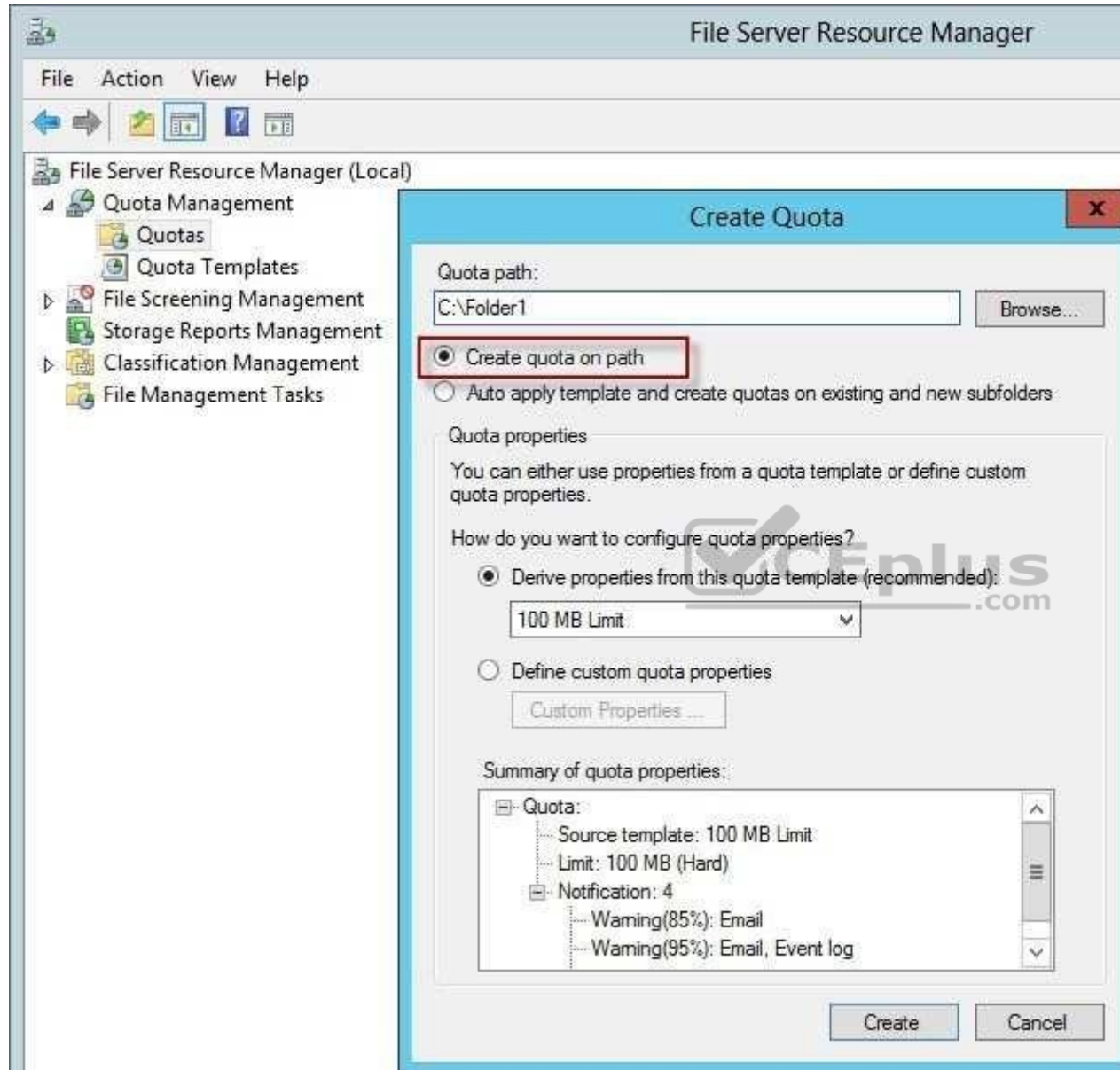D. From the properties of drive D, enable quota management.

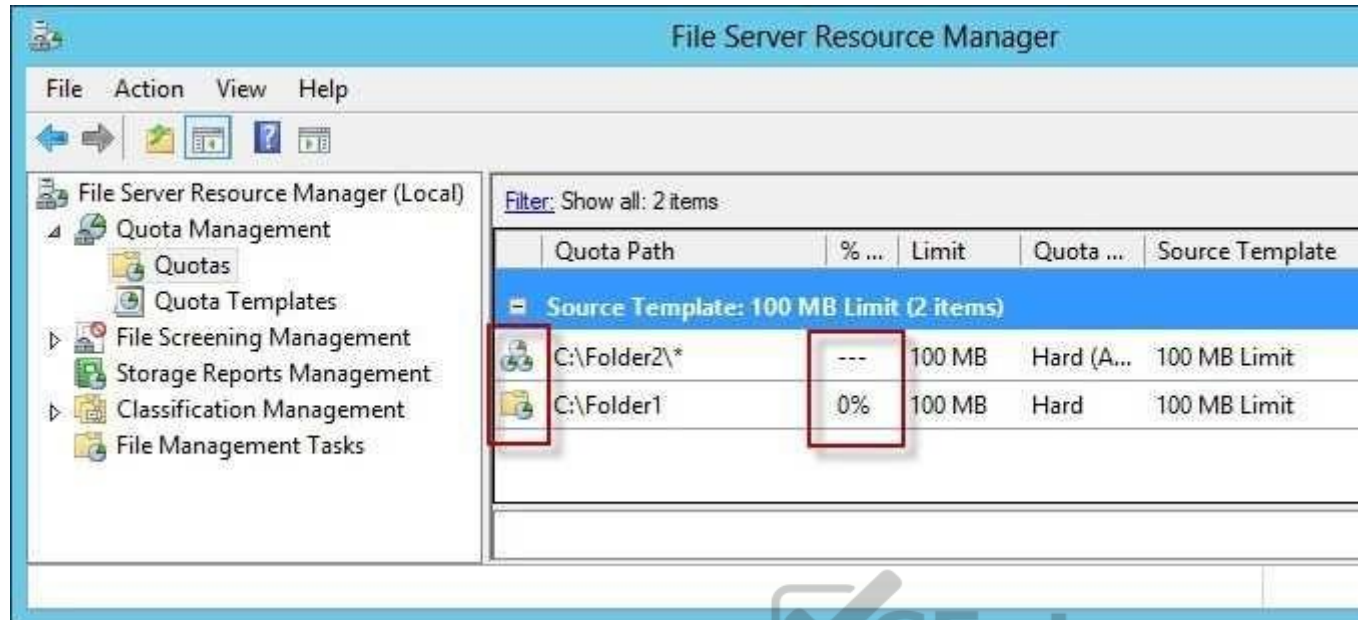**Correct Answer:** A
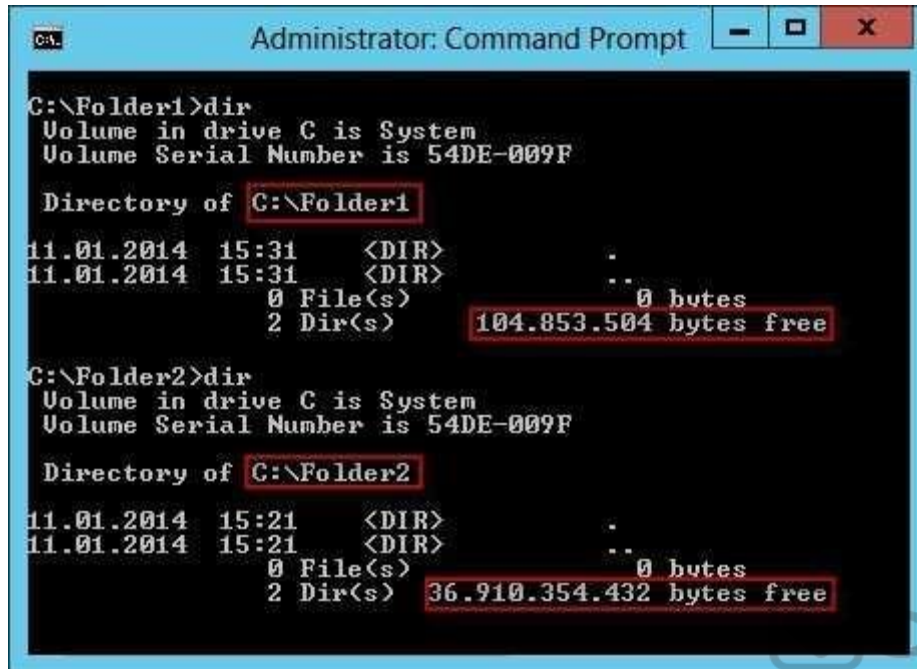**Section: Volume A**

Explanation

Explanation/Reference:
Explanation:
▪ In Quota Management, click the Quota Templates node.
▪ In the Results pane, select the template on which you will base your new quota.
▪ 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. ▪ Under Quota path, type or browse to the folder that the quota will apply to.
▪ 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.
▪ 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.
▪ Click Create. Create a new Quota on path, without using the auto apply template and create quota on existing and new subfolders.

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

QUESTION 16
Your company has a main office and two branch offices. The main office is located in New York. The branch offices are located in Seattle and Chicago.

The network contains an Active Directory domain named contoso.com. An Active Directory site exists for each office. Active Directory site links exist between the main office and the branch offices. All servers run Windows Server 2012 R2.

The domain contains three file servers. The file servers are configured as shown in the following table.

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

You implement a Distributed File System (DFS) replication group named ReplGroup.

ReplGroup is used to replicate a folder on each file server. ReplGroup uses a hub and spoke topology. NYC-SVR1 is configured as the hub server.

You need to ensure that replication can occur if NYC-SVR1 fails.
What should you do? www.vceplus.com - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

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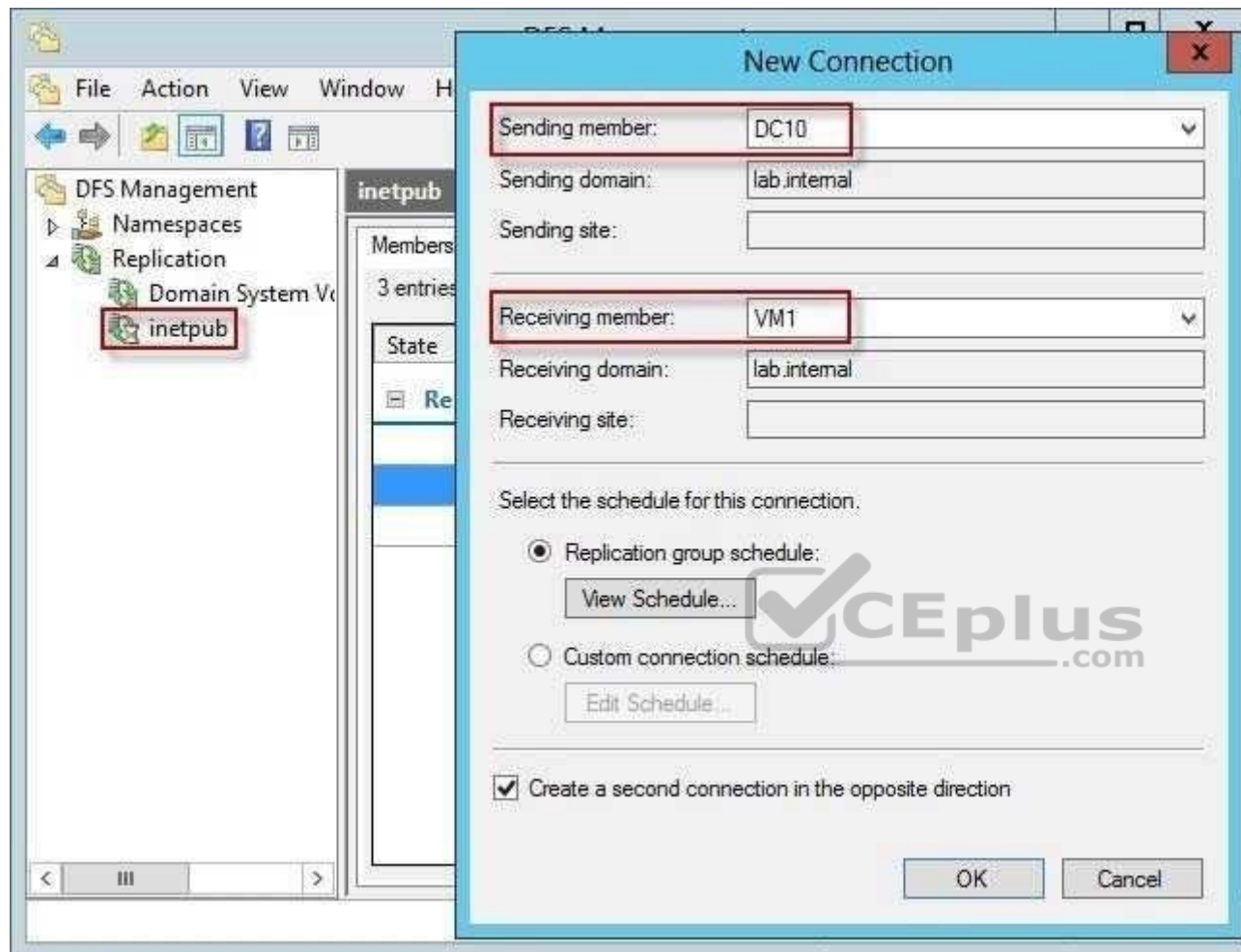D. Create a connection in Rep1Group.

Correct Answer: D
Section: Volume A
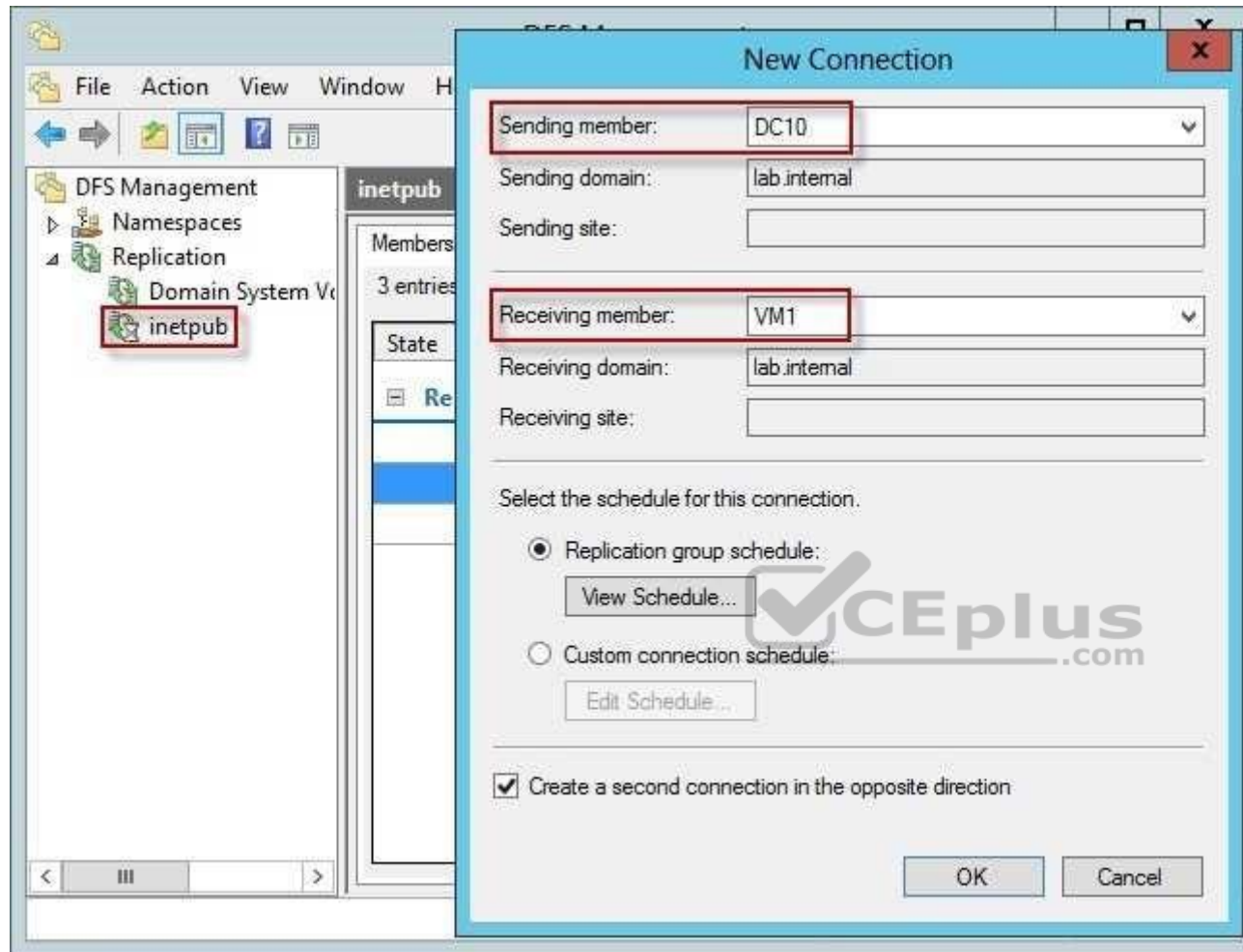**Explanation**

Explanation/Reference:
Explanation:

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

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

QUESTION 17
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
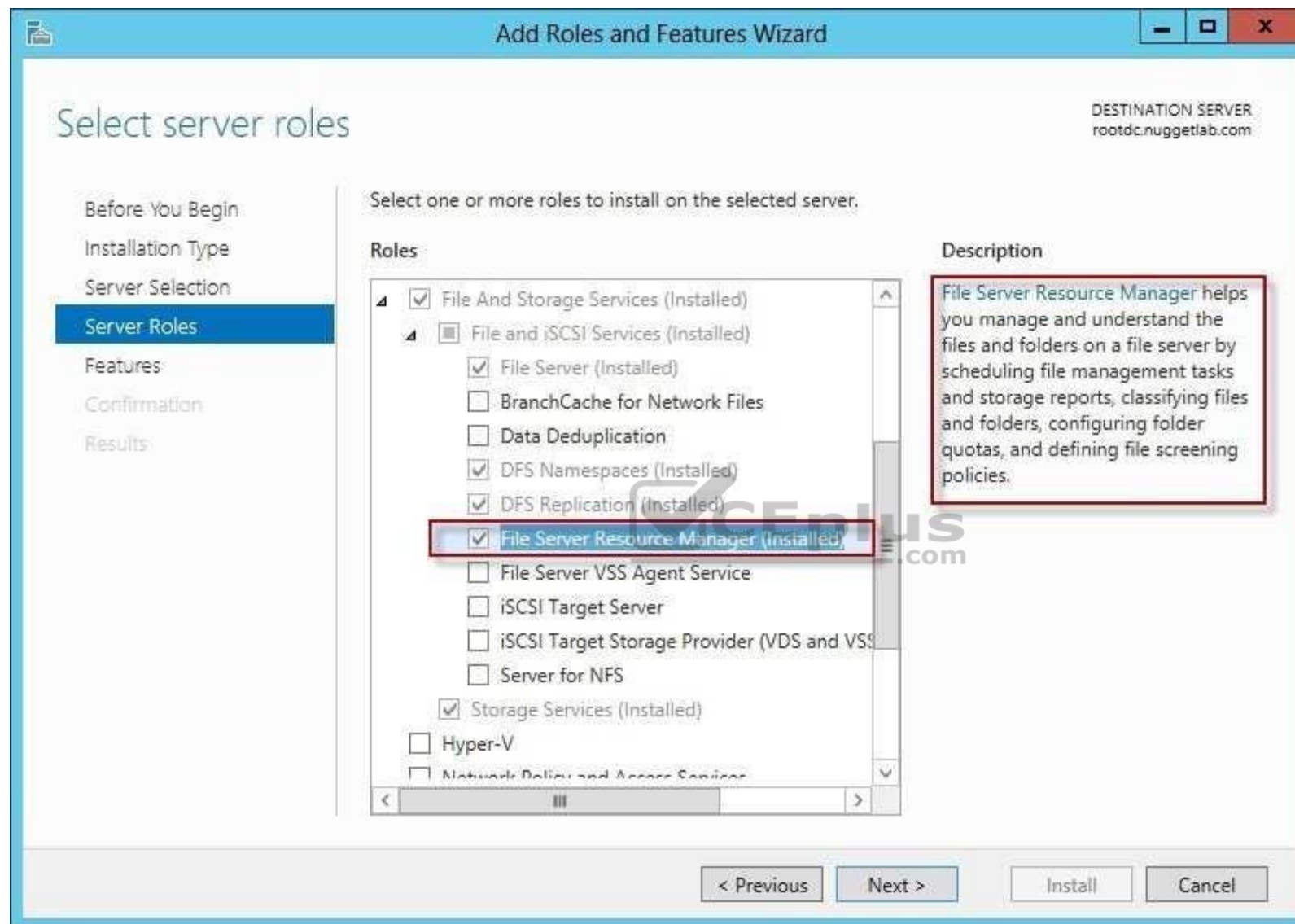D. The Enhanced Storage feature

Correct Answer: C
Section: Volume A

Explanation

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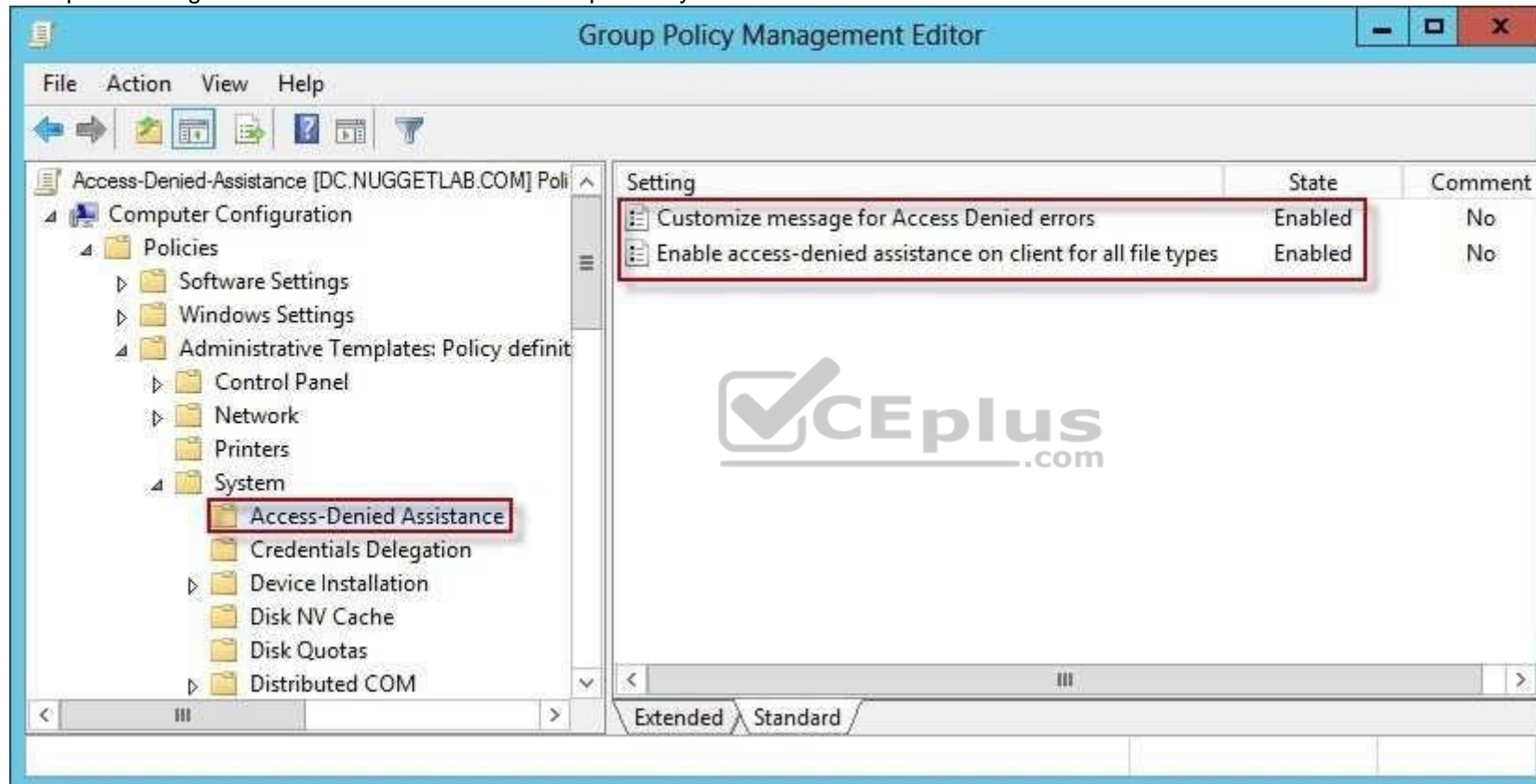
The Customize message for Access Denied errors policy, shown in the screenshot below, enables us to create the actual message box shown to users when they access a shared file to which their user account has no access.

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:
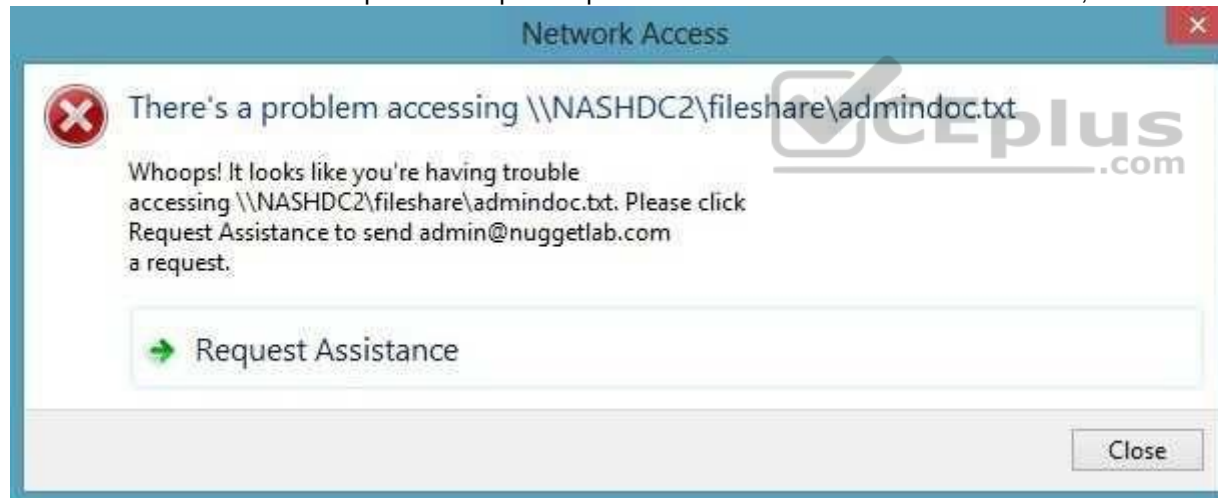
If the user clicks Request Assistance in the Network Access dialog box, they see a secondary message:
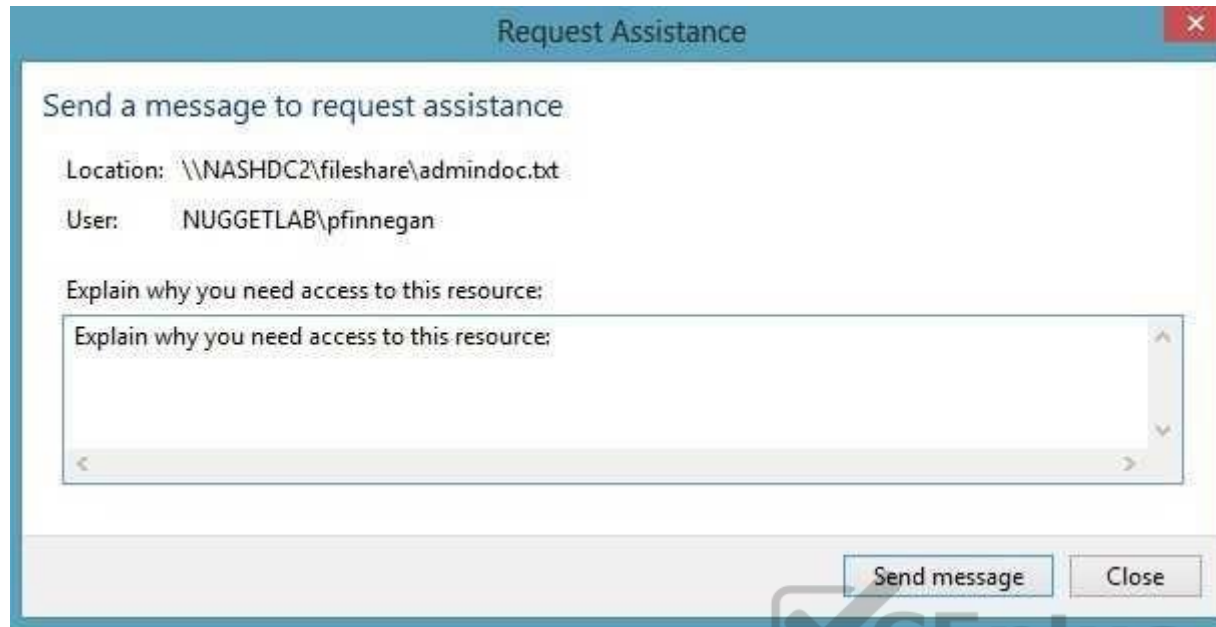
At the end of this process, the administrator(s) will receive an e-mail message that contains the key information they need in order to resolve the access problem: ▪ The user's Active Directory identity
▪ The full path to the problematic file
▪ A user-generated explanation of the problem

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/

QUESTION 18
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.

Correct Answer: A
Section: Volume A
Explanation

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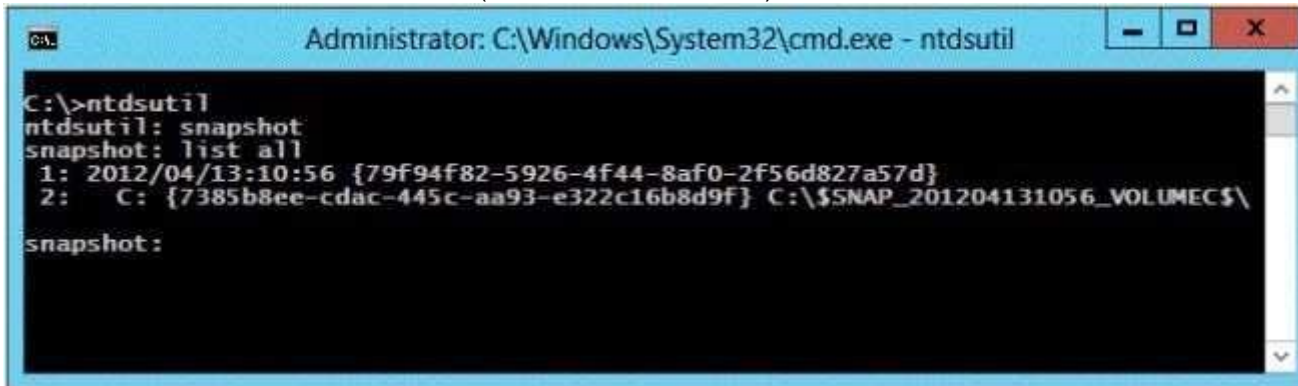
References: http://technet.microsoft.com/en-
us/library/jj574182.aspx#BKMK_12

QUESTION 19
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1.

You run ntdsutil as shown in the exhibit. (Click the Exhibit button.)


```
Administrator: C:\Windows\System32\cmd.exe - ntdsutil

C:\>ntdsutil
ntdsutil: snapshot
snapshot: list all
 1: 2012/04/13:10:56 {79f94f82-5926-4f44-8af0-2f56d827a57d}
 2:    C: {7385b8ee-cdac-445c-aa93-e322c16b8d9f} C:\$SNAP_201204131056_VOLUMEC$\

snapshot:
```

You need to ensure that you can access the contents of the mounted snapshot.

What should you do?

A. From the snapshot context of ntdsutil, run **activate instance "NTDS"**.
B. From a command prompt, run **dsamain.exe -dbpath c:\$snap_201204131056_volumec$\windows\ntds\ntds.dit -1dapport 389**.
C. From the snapshot context of ntdsutil, run **mount {79f94f82-5926-4f44-8af0-2f56d827a57d}**.

D. From a command prompt, run **dsamain.exe -dbpath c:\$snap_201204131056_volumec$\windows\ntds\ntds.dit -1dapport 33389**.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
By default, only members of the Domain Admins group and the Enterprise Admins group are allowed to view the snapshots because they contain sensitive AD DS data. If you want to access snapshot data from an old domain or forest that has been deleted, you can allow nonadministrators to access the data when you run Dsamain.exe.
If you plan to view the snapshot data on a domain controller, specify ports that are different from the ports that the domain controller will use.
A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP port and UDP [7] port 389. The client then sends an operation request to the server, and the server sends responses in return. With some exceptions, the client does not need to wait for a response before sending the next request, and the server may send the responses in any order. All information is transmitted using Basic Encoding Rules (BER).

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

_
```

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

QUESTION 20
DRAG DROP
You are a network administrator of an Active Directory domain named contoso.com.
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Web Server (IIS) server role installed.

Server1 will host a web site at URL https://secure.contoso.com. The application pool identity account of the web site will be set to a domain user account named
AppPool1.

You need to configure the Service Principal Name (SPN) for the web site.

What should you run? To answer, drag the appropriate objects to the correct location. 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.

Select and Place:

Objects

-r

-s

AppPool1

http/contoso

https/contoso

http/secure.contoso.com

https/secure.contoso.com

Answer Area

setspn.exe

Object

Object

Object

Correct Answer:

Objects

-r

http/contoso

https/contoso

https/secure.contoso.com

Answer Area

setspn.exe

-s

http/secure.contoso.com

AppPool1

Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Note:
* -s <SPN>
Adds the specified SPN for the computer, after verifying that no duplicates exist.
Usage: setspn –s SPN accountname
For example, to register SPN "http/daserver" for computer "daserver1":
setspn -S http/daserver daserver1

Attn: with Windows 2008 option is-abut with Windows 2012 it started to show-s Definition of an SPN
An SPN is the name by which a client uniquely identifies an instance of a service. If you install multiple instances of a service on computers throughout a forest, each service instance must have its own SPN. A particular service instance can have multiple SPNs if there are multiple names that clients might use for authentication. For example, an SPN always includes the name of the host computer on which the service instance is running. Therefore, a service instance might register an SPN for each name or alias of its host.

Adding SPNs
To add an SPN, use the setspn -s service/namehostname command at a command prompt, where service/name is the SPN that you want to add and hostname is the actual host name of the computer object that you want to update. For example, if there is an Active Directory domain controller with the host name server1.contoso.com that requires an SPN for the Lightweight Directory Access Protocol (LDAP), type setspn -s ldap/server1.contoso.com server1, and then press ENTER to add the SPN.

The HTTP service class

The HTTP service class differs from the HTTP protocol. Both the HTTP protocol and the HTTPS protocol use the HTTP service class. The service class is the string that identifies the general class of service.

For example, the command may resemble the following command: setspn–
S HTTP/iis6server1. mydomain.com mydomain\appPool1

References:
http://support.microsoft.com/kb/929650/en-us http://technet.microsoft.com/en-
us/library/cc731241(v=ws.10).aspx

QUESTION 21
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2. DC1 is backed up daily. The domain has the Active Directory Recycle Bin enabled.

During routine maintenance, you delete 500 inactive user accounts and 100 inactive groups. One of the deleted groups is named Group1. Some of the deleted user accounts are members of some of the deleted groups.

For documentation purposes, you must provide a list of the members of Group1 before the group was deleted.

You need to identify the names of the users who were members of Group1 prior to its deletion.

You want to achieve this goal by using the minimum amount of administrative effort.

What should you do first?

A. Mount the most recent Active Directory backup.

B. Reactivate the tombstone of Group1.
C. Perform an authoritative restore of Group1.
D. Use the Recycle Bin to restore Group1.

Correct Answer: A
Section: Volume A

Explanation

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

QUESTION 22
Your network contains an Active Directory domain named contoso.com. The domain contains six domain controllers. The domain controllers are configured as shown in the following table.

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

The network contains a server named Server1 that has the Hyper-v server role installed. DC6 is a virtual machine that is hosted on Server1.

You need to ensure that you can clone DC6.

Which FSMO role should you transfer to DC2?

A. Rid master
B. Domain naming master

C. PDC emulator
D. Infrastructure master

Correct Answer: C
Section: Volume A

Explanation

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

References: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/introduction-to-active-directory-domain-services-ad-ds-virtualization-level-100

QUESTION 23
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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
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.

QUESTION 24

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

Correct Answer: E
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 25
Your network contains an Active Directory domain named contoso.com. The Active Directory Recycle bin is enabled for contoso.com.

A support technician accidentally deletes a user account named User1. You need to restore the User1 account.

Which tool should you use?

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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:

QUESTION 26
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.
F. Modify the i**sDeleted** attribute of Group1.
G. Apply a virtual machine snapshot to DC2.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Because removing user accounts from an Active Directory group will not send them to the Active Directory Recycle Bin, performing an authoritative restore is the best option.

QUESTION 27
Your network contains an Active Directory domain named contoso.com. The domain contains a read-only domain controller (RODC) named RODC1.

You create a global group named RODC_Admins.

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

What should you do?

A. From Active Directory Site and Services, configure the Security settings of the RODC1 server object.
B. From Active Directory Sites and Services, run the Delegation of Control Wizard.
C. From a command prompt, run the dsmgmt local roles command.
D. From a command prompt, run the dsadd computer command.

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
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.

QUESTION 28
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 domain. Run dsmod and specify the /server switch.

Correct Answer: B
Section: Volume A
Explanation

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

QUESTION 29
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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. Gpedit. msc
F. Import-GPO
G. Restore-GPO
H. Set-GPInheritanceI. Set-GPLink
J. Set-GPPermission

K. Gpupdate
L. Add-ADGroupMember

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
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

QUESTION 30
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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 contains a top-level organizational unit (OU) for each department. A group named Group1 contains members from each department.

You have a GPO named GPO1 that is linked to the domain.

You need to configure GPO1 to apply settings to Group1 only.

What should you use?

A. Dcgpofix
B. Get-GPOReport
C. Gpfixup
D. Gpresult
E. Gpedit. msc
F. Import-GPO
G. Restore-GPO
H. Set-GPInheritance
I. Set-GPLink

J. Set-GPPermission
K. Gpupdate
L. Add-ADGroupMember

Correct Answer: J
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Set-GPPermission grants a level of permissions to a security principal (user, security group, or computer) for one GPO or all the GPOs in a domain. You use the TargetName and TargetType parameters to specify a user, security group, or computer for which to set the permission level.

-Replace <SwitchParameter>
Specifies that the existing permission level for the group or user is removed before the new permission level is set. If a security principal is already granted

a permission level that is higher than the specified permission level and you do not use the Replace parameter, no change is made. Reference:

http://technet.microsoft.com/en-us/library/ee461038.aspx

QUESTION 31
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

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. Gpedit. msc F. Import-GPO
G. Restore-GPO
H. Set-GPInheritanceI. Set-GPLink
J. Set-GPPermission
K. Gpupdate
L. Add-ADGroupMember

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
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

QUESTION 32
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

Correct Answer: B
Section: Volume A
Explanation

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

Administrators (A built-in group)
After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group. The Administrators group has built-in capabilities that give its members full control over the system. The group is the default owner of any object that is created by a member of the group.
This example logs in as a test user who is not a domain user or an administrator on the server. This results in the error specifying that DA can only be configured by a user with local administrator permissions.

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

QUESTION 33
Your network contains an Active Directory domain named contoso.com.

You need to install and configure the Web Application Proxy role service.

What should you do?

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

Correct Answer: A
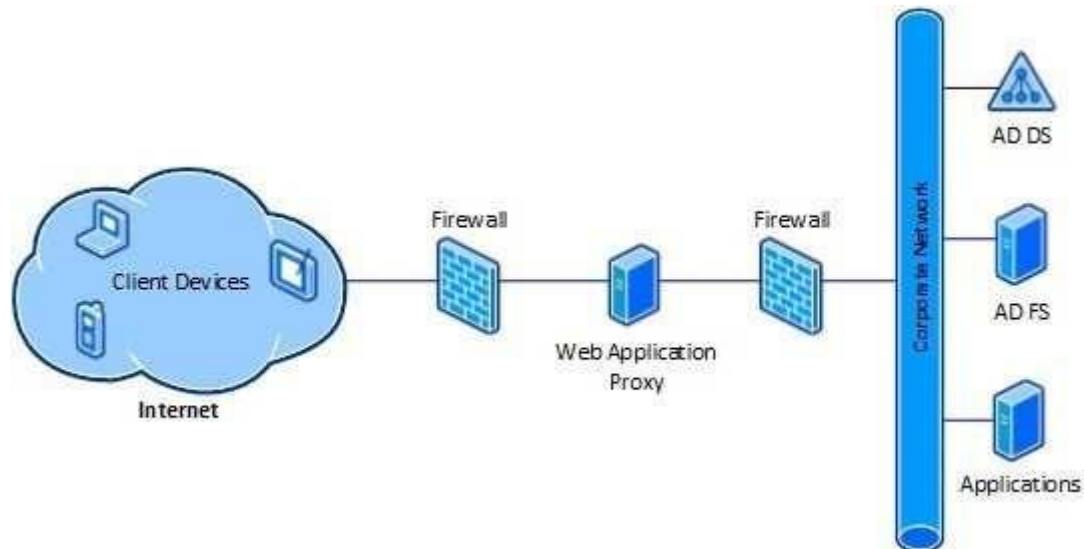**Section: Volume A**
Explanation
Explanation/Reference:
Explanation:
Web Application Proxy is a new Remote Access role service in Windows Server® 2012 R2.

QUESTION 34

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 is configured as a VPN server.

You need to configure Server1 to perform network address translation (NAT).

What should you do?

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

Correct Answer: D
Section: Volume A
Explanation
Explanation/Reference:
Explanation:
To configure an existing RRAS server to support both VPN remote access and NAT routing:
▪ Open Server Manager.
▪ Expand Roles, and then expand Network Policy and Access Services.
▪ Right-click Routing and Remote Access, and then click Properties.
▪ Select IPv4 Remote access Server or IPv6 Remote access server, or both.

QUESTION 35

You have a DNS server named DN51 that runs Windows Server 2012 R2.

On DNS1, you create a standard primary DNS zone named adatum.com.

You need to change the frequency that secondary name servers will replicate the zone from DNS1.

Which type of DNS record should you modify?

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

Correct Answer: B
Section: Volume A
Explanation

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

QUESTION 36
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.

Correct Answer: BE
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 37
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. All of the DNS servers in both of the domains run Windows Server 2012 R2.

The network contains two servers named Server1 and Server2. Server1 hosts an Active Directory- integrated zone for contoso.com. Server2 hosts an Active Directory-integrated zone for fabrikam.com. Server1 and Server2 connect to each other by using a WAN link.

Client computers that connect to Server1 for name resolution cannot resolve names in fabrikam.com.

You need to configure Server1 to support the resolution of names in fabnkam.com. The solution must ensure that users in contoso.com can resolve names in fabrikam.com if the WAN link fails.

What should you do on Server1?

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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
Explanation:
http://technet.microsoft.com/en-us/library/cc771898.aspx
When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone.
With secondary, you have ability to resolve records from the other domain even if its DNS servers are temporarily unavailable.
While secondary zones contain copies of all the resource records in the corresponding zone on the master name server, stub zones contain only three kinds of resource records:
▪ A copy of the SOA record for the zone.
▪ Copies of NS records for all name servers authoritative for the zone. ▪
Copies of A records for all name servers authoritative for the zone.

References:
http://www.windowsnetworking.com/articles-tutorials/windows-2003/DNS_Stub_Zones.html http://technet.microsoft.com/en-us/library/cc771898.aspx http://redmondmag.com/Articles/2004/01/01/The-Long-and-Short-of-Stub-Zones.aspx?Page=2

QUESTION 38
Your network contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2 and have the DNS Server server role installed.

On Server1, you create a standard primary zone named contoso.com.

You need to ensure that Server2 can host a secondary zone for contoso.com.

What should you do from Server1?

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

Correct Answer: A
Section: Volume A

Explanation

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

You must add a new Name Server. To add a name server to the list of authoritative servers for the zone, you must specify both the server's IP address and its DNS name. When entering names, click Resolve to resolve the name to its IP address prior to adding it to the list. Secondary zones cannot be AD-integrated under any circumstances.

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

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

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

We need to tell our primary DNS that it is ok for this secondary DNS to pull information from it. Otherwise replication will fail and you will get this big red X.


Head over to your primary DNS server, launch DNS manager, expand Forward Lookup Zones, navigate to your primary DNS zone, right-click on it and go to Properties.
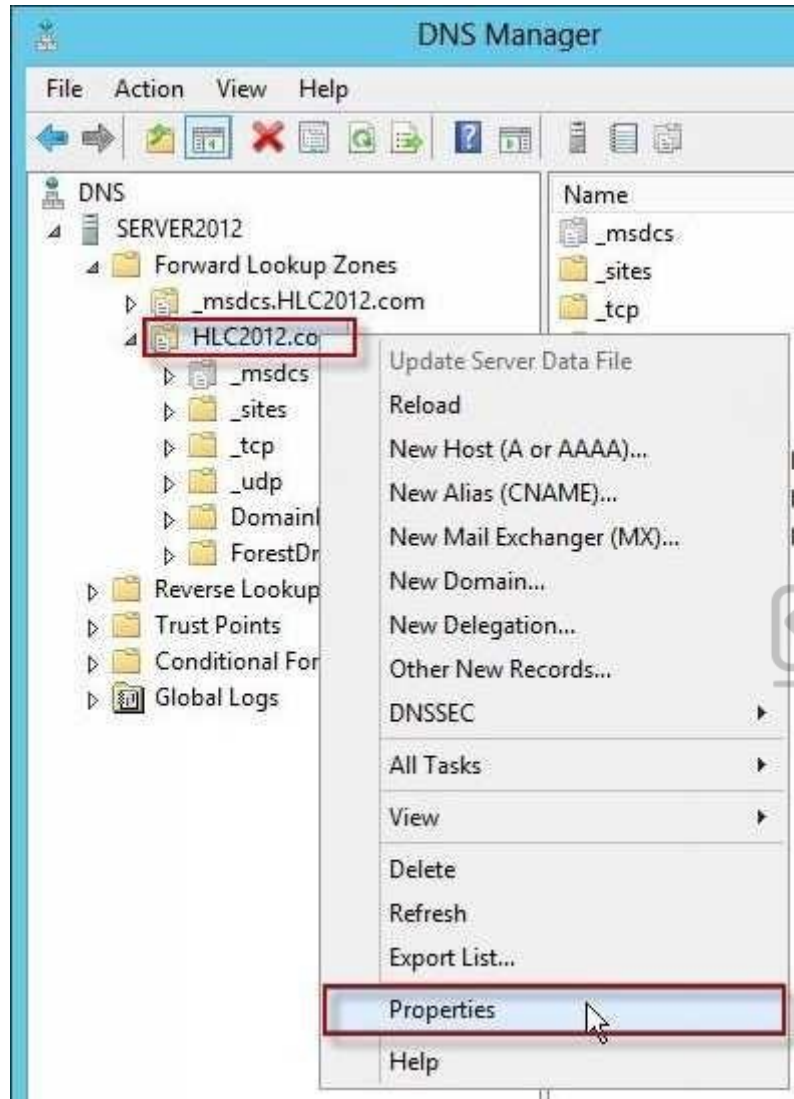
Go to "Zone Transfers" tab, by default, for security reasons, the "Allow zone transfers: " is un- checked to protect your DNS information. We need to allow zone transfers, if you value your DNS records, you do not want to select "To any server" but make sure you click on "Only to servers listed on the Name Servers tab".
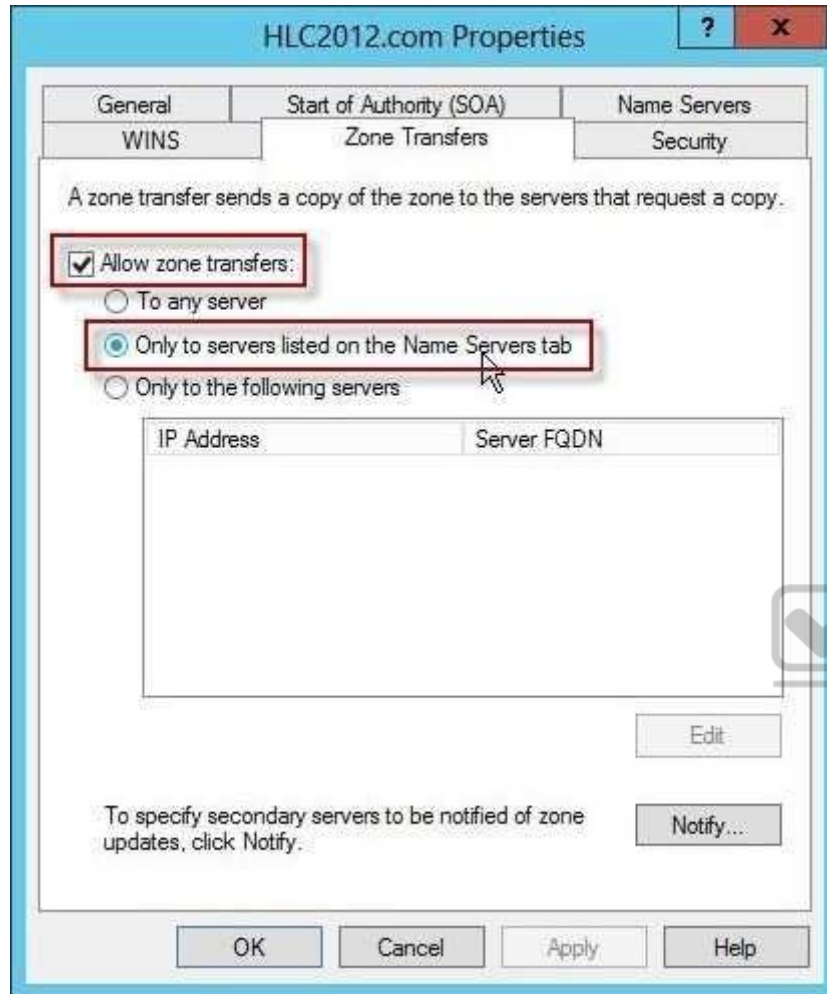
Head over to the "Name Servers" tab, click Add.
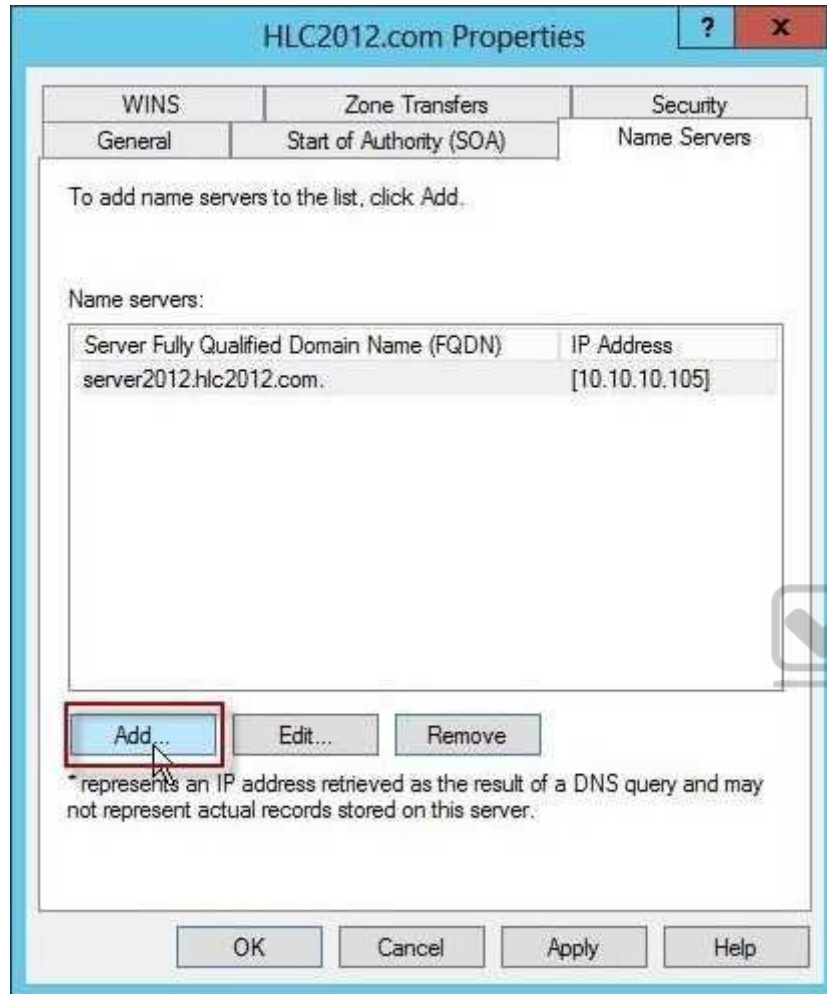
You will get "New Name Server Record" window, type in the name of your secondary DNS server. it is always better to validate by name not IP address to avoid future problems in case your IP addresses change. Once done, click OK.

You will see your secondary DNS server is now added to your name servers selection, click OK.
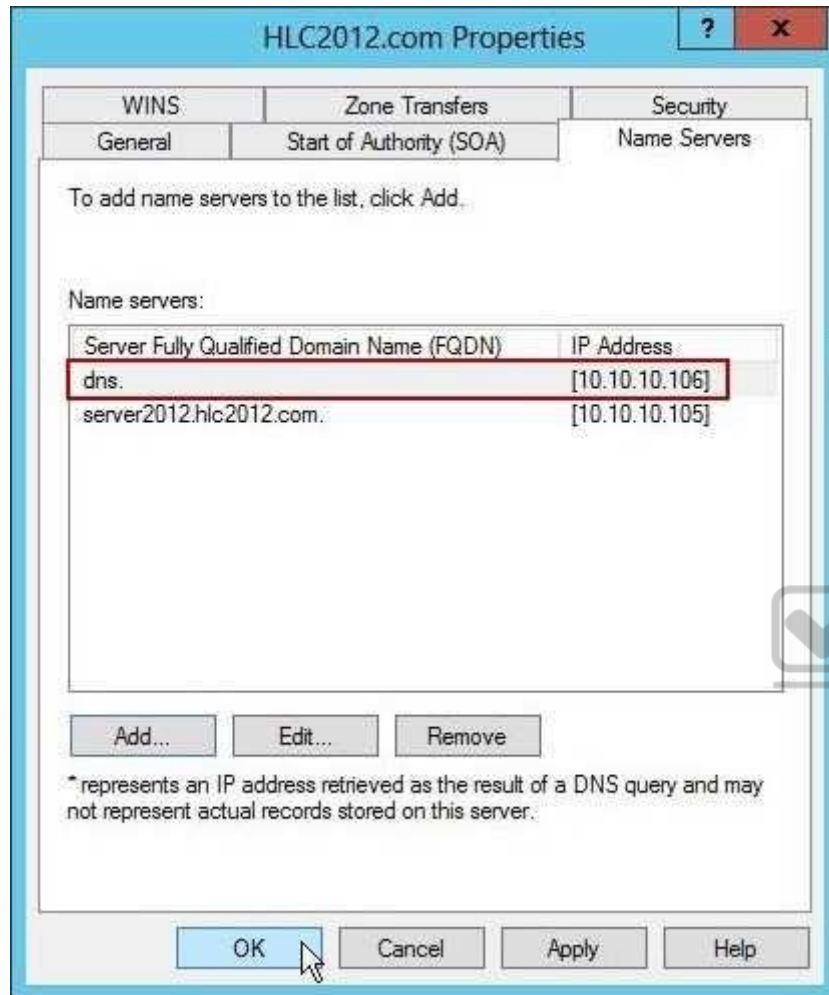
Now if you head back to your secondary DNS server and refresh, the big red X will go away and your primary zone data will populate.
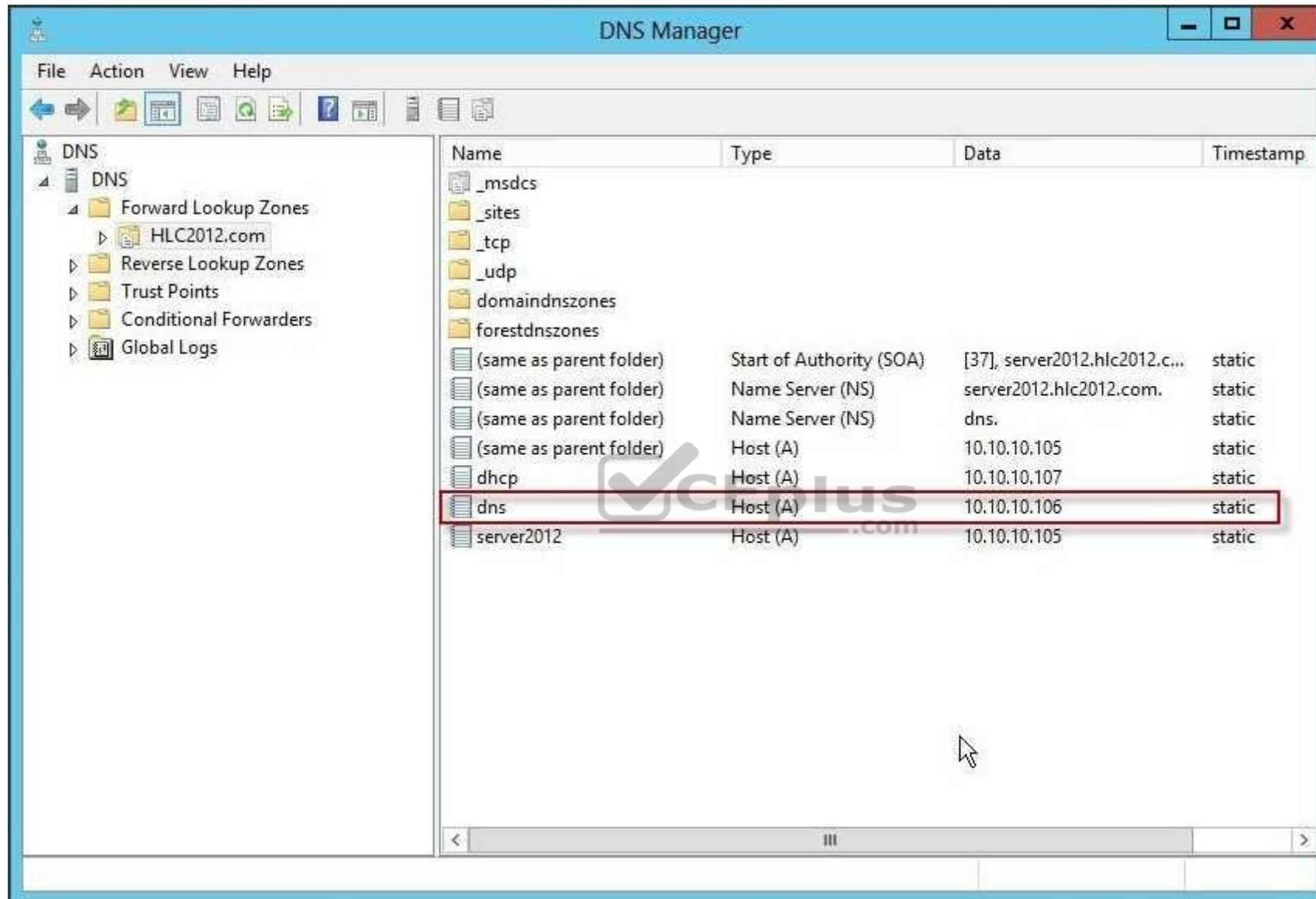
Your secondary DNS is fully setup now. You cannot make any DNS changes from your secondary DNS. Secondary DNS is a read-only DNS, Any DNS changes have to be done from the primary DNS.

References:
http://technet.microsoft.com/en-us/library/cc816885(v=ws.10).aspx http://technet.microsoft.com/en-us/library/cc816814(v=ws.10).aspx http://technet.microsoft.com/en-us/library/cc770984.aspx

http://technet.microsoft.com/en-us/library/cc753500.aspx http://technet.microsoft.com/en-us/library/cc771640(v=ws.10).aspx http://technet.microsoft.com/en-us/library/ee649280(v=ws.10).aspx

QUESTION 39
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.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 40
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.

All client computers run Windows 8.1 Enterprise.

DC1 contains a Group Policy object (GPO) named GPO1.

You need to deploy a VPN connection to all users.

What should you configure from User Configuration in GPO1?

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

Correct Answer: D
**Section: Volume A**
Explanation

Explanation/Reference:
Explanation:
▪ Open the Group Policy Management Console. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click Edit.
▪ In the console tree under Computer Configuration or User Configuration, expand the Preferences folder, and then expand the Control Panel Settings folder. ▪
Right-click the Network Options node, point to New, and select VPN Connection.

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

Reference: http://technet.microsoft.com/en-us/library/cc772449.aspx
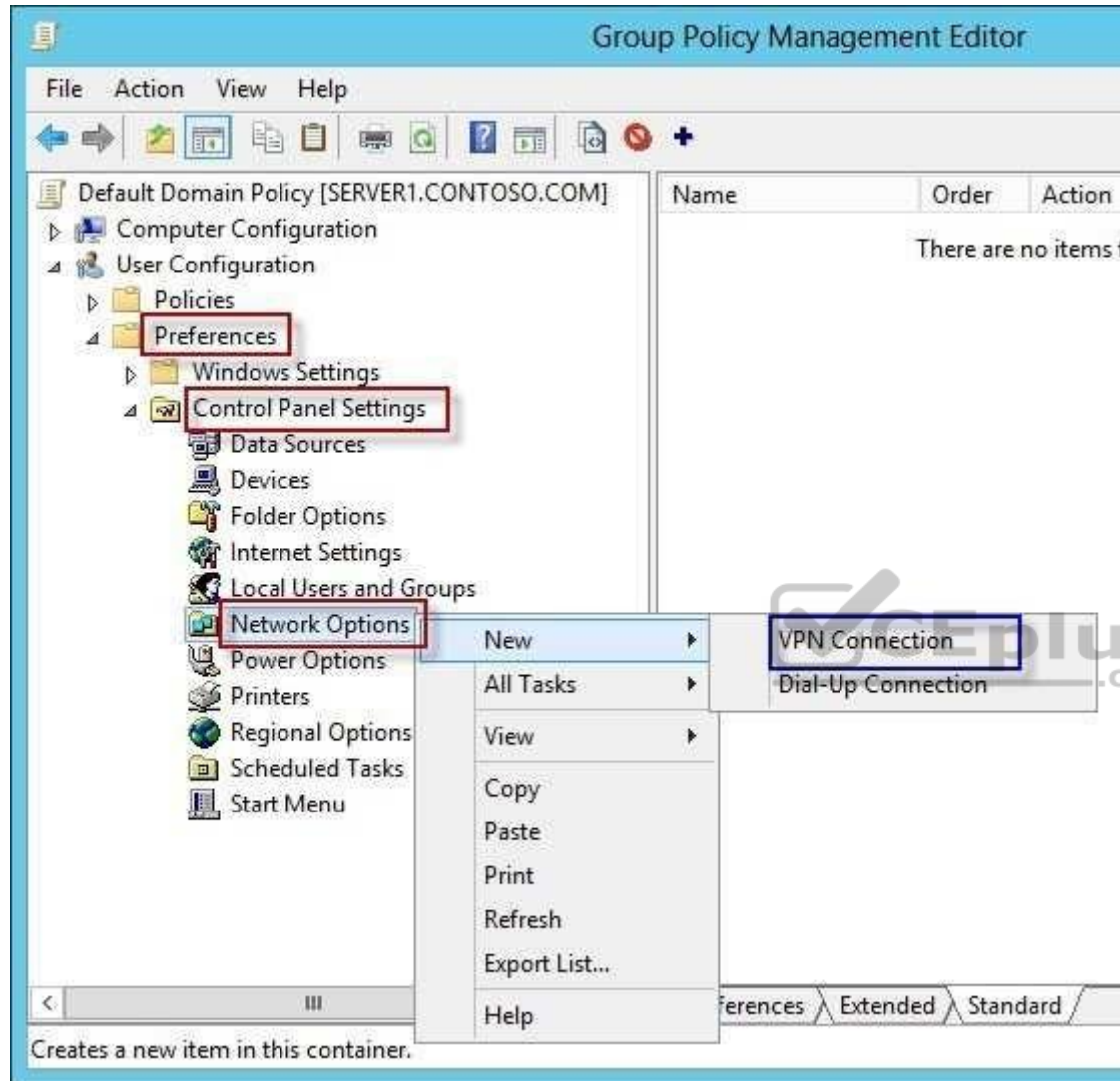
QUESTION 41
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 8.1.

The network contains a shared folder named FinancialData that contains five files.

You need to ensure that the FinancialData folder and its contents are copied to all of the client computers.

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

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

Correct Answer: DE
Section: Volume A

Explanation

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

QUESTION 42
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

Correct Answer: AD
Section: Volume A
Explanation

Explanation/Reference:
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/bb964258.aspx

QUESTION 43
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains 500 client computers that run Windows 8.1 Enterprise and Microsoft Office 2013.

You implement a Group Policy central store.

You need to modify the default Microsoft Office 2013 Save As location for all client computers.
The solution must minimize administrative effort.

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

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

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
Explanation:
Group Policy preferences provide the means to simplify deployment and standardize configurations. They add to Group Policy a centralized system for deploying preferences (that is, settings that users can change later). You can also use Group Policy preferences to configure applications that are not Group Policy-aware. By using Group Policy preferences, you can change or delete almost any registry setting, file or folder, shortcut, and more. You are not limited by the contents of Administrative Template files.

References: http://technet.microsoft.com/en-us/library/dn581922.aspx https://trekker.net/archives/set-the-default-save-location-to-computer-in-office-2013/

QUESTION 44
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

The domain contains 200 Group Policy objects (GPOs) and 100 WMI filters.

An administrator named Admin1 must be able to create new WMI filters and edit all of the existing WMI filters from the Group Policy Management Console (GPMC).

You need to delegate the required permissions to Admin1. The solution must minimize the number of permissions assigned to Admin1.

https://vceplus.com/ What should

you do?

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Users with Full control permissions can create and control all WMI filters in the domain, including WMI filters created by

others. Users with Creator owner permissions can create WMI filters, but can only control WMI filters that they create.

Reference: http://technet.microsoft.com/en-us/library/cc757429(v=ws.10).aspx

QUESTION 45
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
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

QUESTION 46
Your network contains an Active Directory domain named contoso.com. The domain contains six domain controllers named DC1, DC2, DC3, DC4, DC5, and DC6. Each domain controller has the DNS Server server role installed and hosts an Active Directory-integrated zone for contoso.com.

You plan to create a new Active Directory-integrated zone named litwareinc.com that will be used for testing.

You need to ensure that the new zone will be available only on DC5 and DCG.

What should you do first?

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
You can store Domain Name System (DNS) zones in the domain or application directory partitions of Active Directory Domain Services (AD DS). A partition is a data structure in AD DS that distinguishes data for different replication purposes. When you create an application directory partition for DNS, you can control the scope of replication for the zone that is stored in that partition.

QUESTION 47
Your network contains an Active Directory domain named contoso.com. The domain contains a server named NPS1 that has the Network Policy Server server role installed. All servers run Windows Server 2012 R2.

You install the Remote Access server role on 10 servers.

You need to ensure that all of the Remote Access servers use the same network policies.

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

A. Configure each Remote Access server to use the Routing and Remote Access service (RRAS) to authenticate connection requests.
B. On NPS1, create a remote RADIUS server group. Add all of the Remote Access servers to the remote RADIUS server group.
C. On NPS1, create a new connection request policy and add a Tunnel-Type and a Service-Type condition.
D. Configure each Remote Access server to use a RADIUS server named NPS1.
E. On NPS1, create a RADIUS client template and use the template to create RADIUS clients.

Correct Answer: CD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Connection request policies are sets of conditions and settings that allow network administrators to designate which 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.
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.

Reference: http://technet.microsoft.com/en-us/library/cc730866(v=ws.10).aspx

QUESTION 48
Your network contains a server named Server1 that has the Network Policy and Access Services server role installed.

All of the network access servers forward connection requests to Server1.

You create a new network policy on Server1.

You need to ensure that the new policy applies only to connection requests from the 192.168.0.0/24 subnet.

What should you do?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
RADIUS client properties
Following are the RADIUS client conditions that you can configure in network policy.
▪ Calling Station ID: Specifies the network access server telephone number that was dialed by the dial-up access client.
▪ Client Friendly Name: Specifies the name of the RADIUS client that forwarded the connection request to the NPS server.
▪ Client IPv4 Address: Specifies the Internet Protocol (IP) version 4 address of the RADIUS client that forwarded the connection request to the NPS server.
▪ Client IPv6 Address: Specifies the Internet Protocol (IP) version 6 address of the RADIUS client that forwarded the connection request to the NPS server.
▪ Client Vendor: Specifies the name of the vendor or manufacturer of the RADIUS client that sends connection requests to the NPS server. ▪
MS RAS Vendor: Specifies the vendor identification number of the network access server that is requesting authentication.

QUESTION 49
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed.

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

Which authentication method should you identify?

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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
802.1X uses EAP, EAP-TLS, EAP-MS-CHAP v2, and PEAP authentication methods:
▪ EAP (Extensible Authentication Protocol) uses an arbitrary authentication method, such as certificates, smart cards, or credentials.
▪ EAP-TLS (EAP-Transport Layer Security) is an EAP type that is used in certificate-based security environments, and it provides the strongest authentication and key determination method.
▪ EAP-MS-CHAP v2 (EAP-Microsoft Challenge Handshake Authentication Protocol version 2) is a mutual authentication method that supports password-based user or computer authentication.
▪ PEAP (Protected EAP) is an authentication method that uses TLS to enhance the security of other EAP authentication protocols.
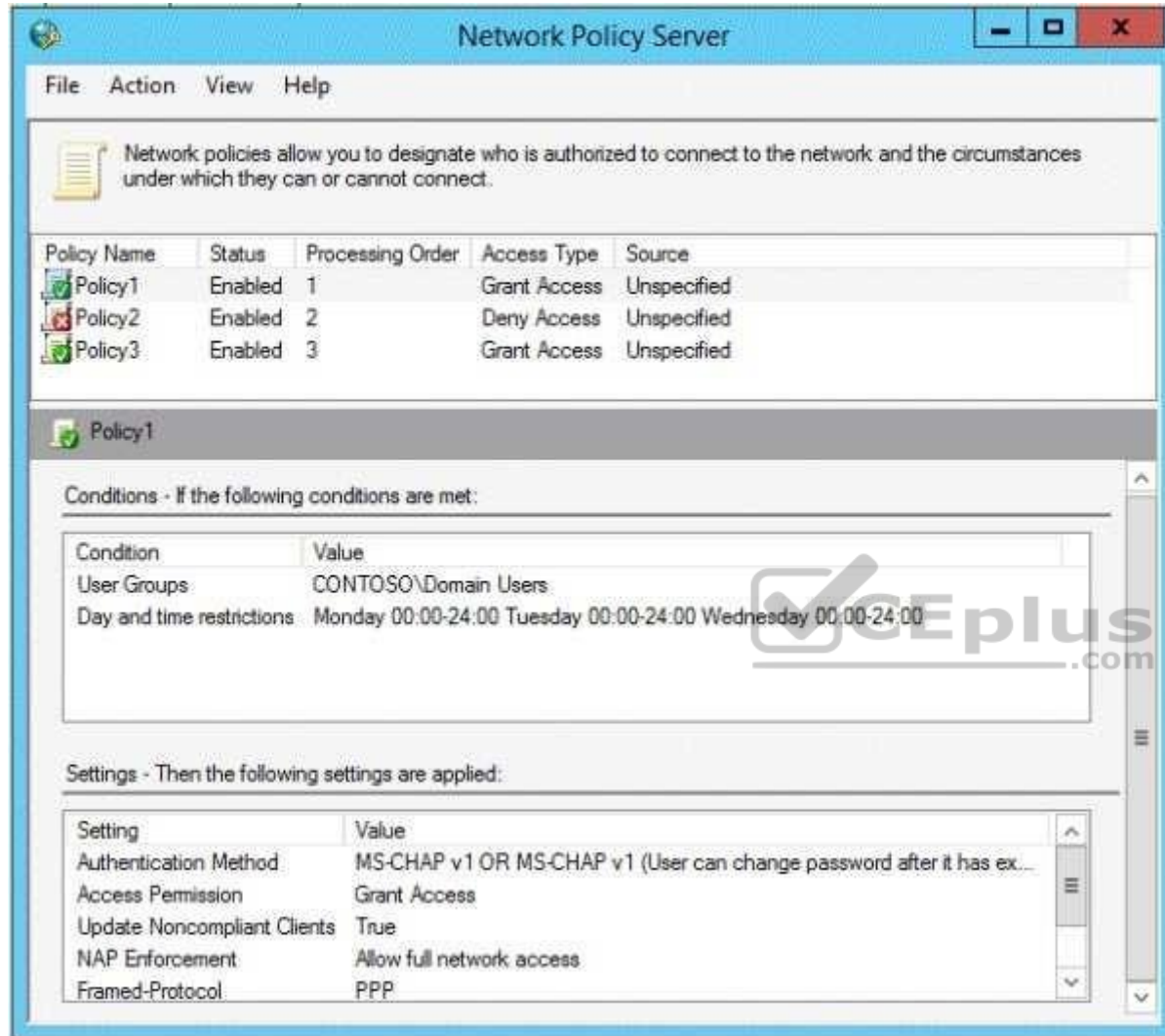
QUESTION 50
HOTSPOT
Your network contains an Active Directory named contoso.com.
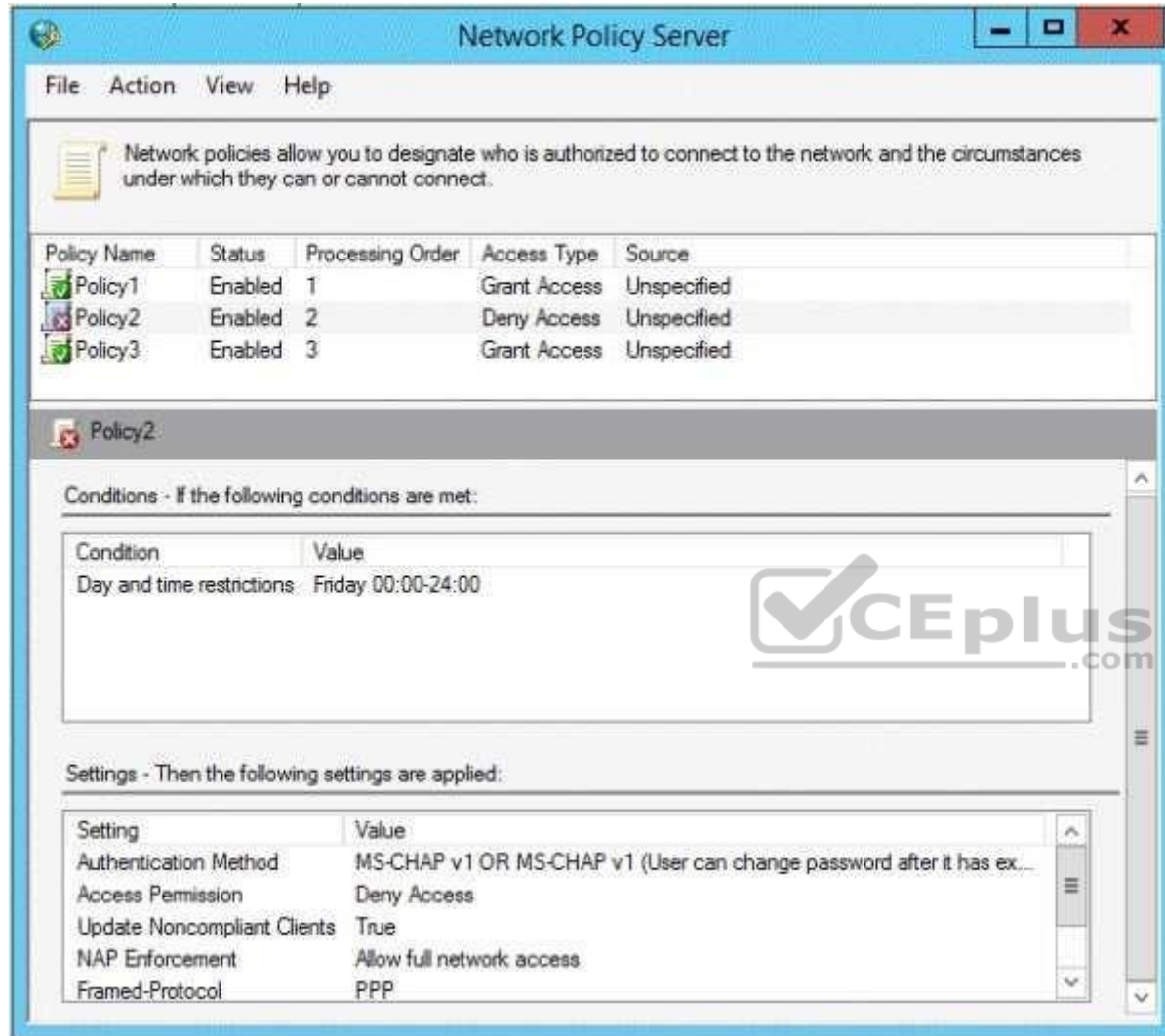
You have users named User1 and user2.

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

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

Network Policy Server

File Action View Help

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

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

Policy1

Conditions - If the following conditions are met:

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

Settings - Then the following settings are applied:

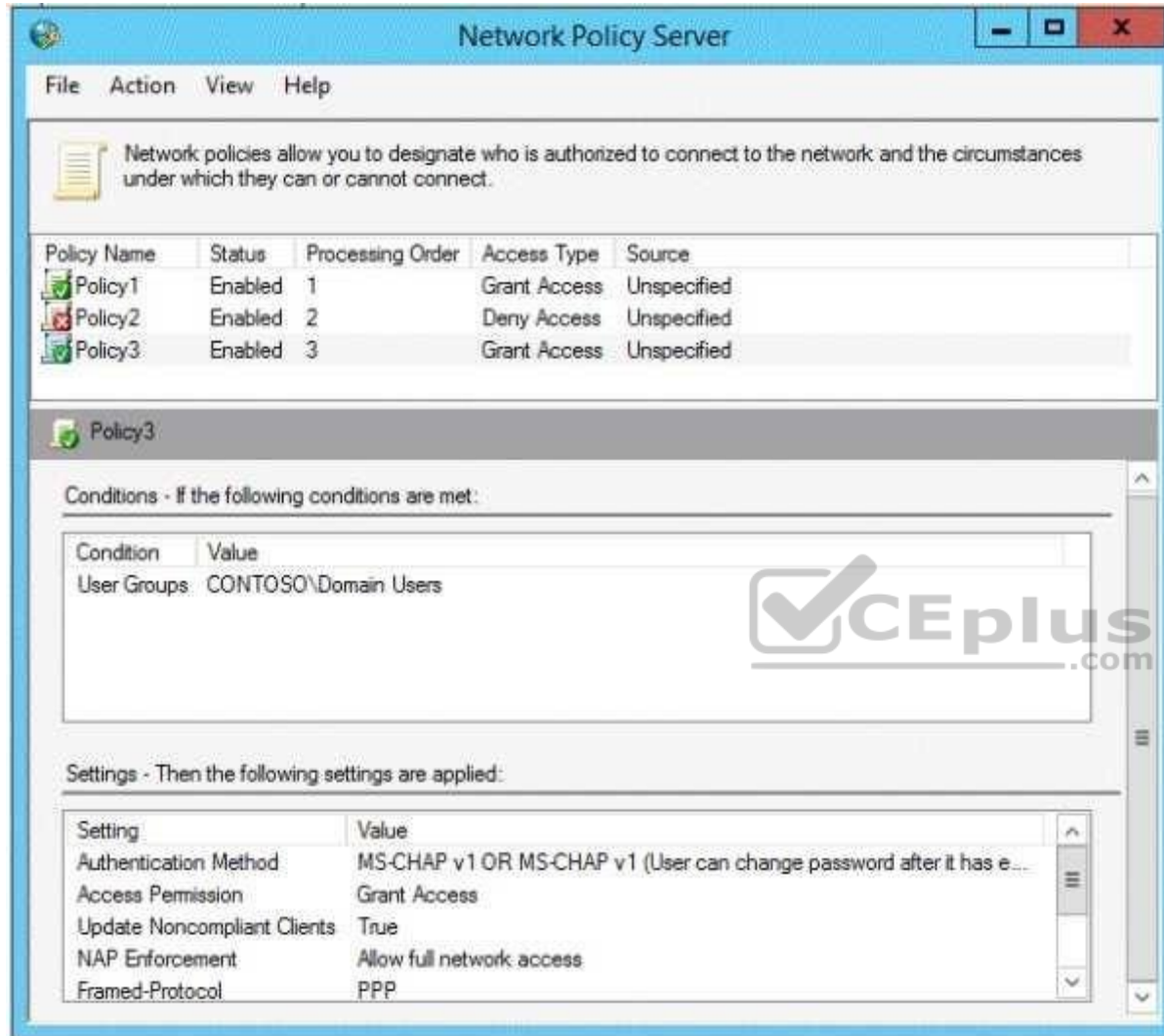| Setting	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has ex...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP

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

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

Network Policy Server

File Action View Help

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

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

Policy3

Conditions - If the following conditions are met:

Condition	Value
User Groups	CONTOSO\Domain Users

Settings - Then the following settings are applied:

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

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

Hot Area:

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

Correct Answer:

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

Section: Volume A
Explanation

Explanation/Reference:

QUESTION 51
DRAG DROP
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.

Select and Place:

Actions

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

Answer Area

Correct Answer:

Actions

Create a connection request policy
Create a remediation server group

Answer Area

Create a Windows Security Health Validator (WSHV) configuration
Create a health policy
Create a network policy

Section: Volume A
Explanation

Explanation/Reference:
Explanation:

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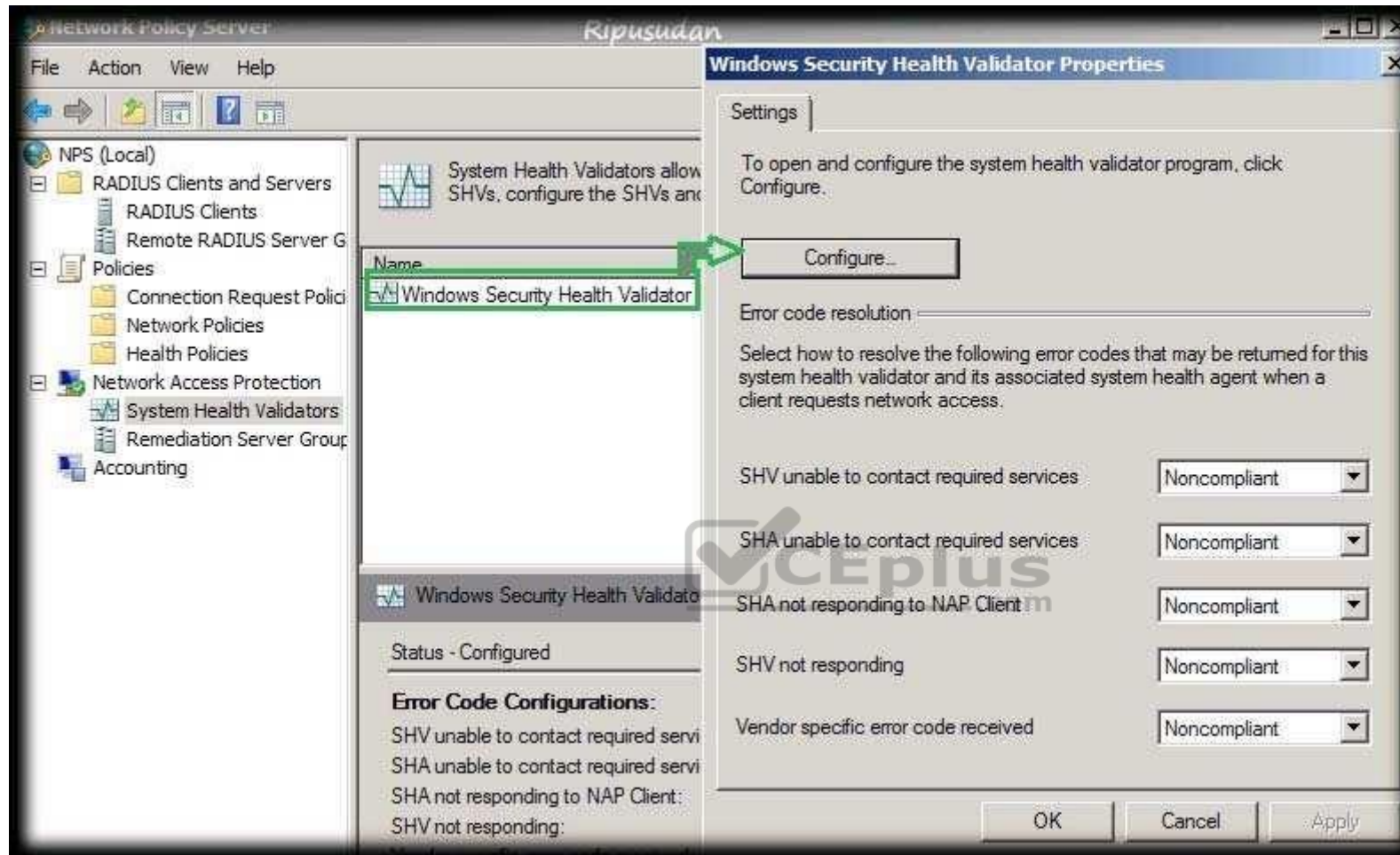
Date: 6/ 1/2007   Time: 12:00:00 PM

( ) 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

* 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.

References:
http://technet.microsoft.com/es-es/library/dd314198(v=ws.10).aspx http://technet.microsoft.com/es-es/magazine/2009.05.goat.aspx http://technet.microsoft.com/es-es/library/dd314173(v=ws.10).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(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/cc772356(v=ws.10).aspx

QUESTION 52
Your network contains two servers named Server1 and Server2 that run windows Server 2012 R2. Server1 and 5erver2 have the Windows Server Update Services server role installed.

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

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

What should you do?

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

Correct Answer: A
Section: Volume A

Explanation
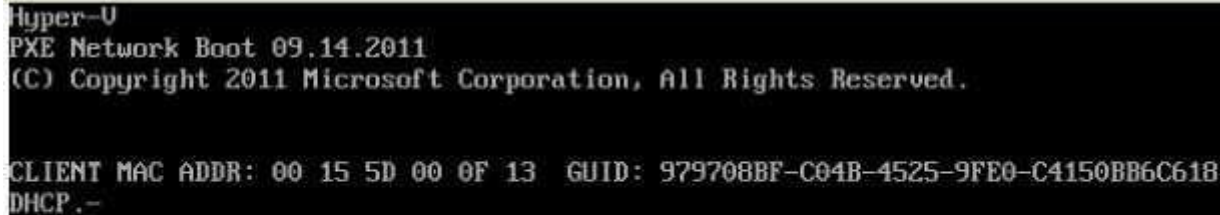
Explanation/Reference:
Explanation:
WSUS Reporting Rollup Sample Tool
This tool uses the WSUS application programming interface (API) to demonstrate centralized monitoring and reporting for WSUS. It creates a single report of update and computer status from the WSUS servers into your WSUS environment. 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

QUESTION 53
You manage a server that runs Windows Server 2012 R2. The server has the Windows Deployment Services server role installed.
You start a virtual machine named VM1 as shown in the exhibit. (Click the Exhibit button.)


```
Hyper-V
PXE Network Boot 09.14.2011
(C) Copyright 2011 Microsoft Corporation, All Rights Reserved.


CLIENT MAC ADDR: 00 15 5D 00 0F 13   GUID: 979708BF-C04B-4525-9FE0-C4150BB6C618
DHCP.-
```

You need to configure a pre-staged device for VM1 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. 979708BFC04B45259FE0C4150BB6C618
B. 979708BF-C04B-4525-9FE0-C4150BB6C618
C. 00155D000F130000000000000000000000
D. 00000000000000000000000155D000F13
E. 00000000-0000-0000-0000-C4150BB6C618

Correct Answer: BD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Use client computer's media access control (MAC) address preceded with twenty zeros or the globally unique identifier (GUID) in the format: {XXXXXXXX-XXXXXXXX-XXX- XXXXXXXXXXXX}.

QUESTION 54
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
To configure data management for a Data Collector Set
▪ In Windows Performance Monitor, expand Data Collector Sets and click User Defined.
▪ In the console pane, right-click the name of the Data Collector Set that you want to configure and click Data Manager.
▪ On1 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. ▪ Click the Actions tab. You can accept the default values or make changes. See the table below for details on each option. ▪ When you have finished making your changes, click OK.

QUESTION 55
You have Windows Server 2012 R2 installation media that contains a file named Install.wim.

You need to identify which images are present in Install.wim.

What should you do?

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

Correct Answer: C
Section: Volume A

Explanation

Explanation:
Option: /Get-
ImageInfo

Arguments:
/ImageFile: <path_to_image.wim>
[{/Index: <Image_index> | /Name: <Image_name>}]

Displays information about the images that are contained in the .wim, vhd or .vhdx file. When used with the Index or /Name argument, information about the specified image is displayed, which includes if an image is a WIMBoot image, if the image is Windows 8.1 Update, see Take Inventory of an Image or Component Using DISM. The /Name argument does not apply to VHD files. You must specify /Index: 1 for VHD files.

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

QUESTION 56
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.

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 57

Your network contains a Hyper-V host named Server1 that hosts 20 virtual machines.

You need to view the amount of memory resources and processor resources each virtual machine uses currently.

Which tool should you use on Server1?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 58
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.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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/cc708480%28v=ws.10%29.aspx http://technet.microsoft.com/en-us/library/cc720466(v=ws.10).aspx

QUESTION 59
Your company has a main office and two branch offices. The main office is located in Seattle. The two branch offices are located in Montreal and Miami. Each office is configured as an Active Directory site.

The network contains an Active Directory domain named contoso.com. Network traffic is not routed between the Montreal office and the Miami office.

You implement a Distributed File System (DFS) namespace named \\contoso.com\public. The namespace contains a folder named Folder1. Folder1 has a folder target in each office.

You need to configure DFS to ensure that users in the branch offices only receive referrals to the target in their respective office or to the target in the main office.

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

A. Set the Ordering method of \\contoso.com\public to Random order.
B. Set the Advanced properties of the folder target in the Seattle office to Last among all targets.
C. Set the Advanced properties of the folder target in the Seattle office to First among targets of equal cost.

D. Set the Ordering method of \\contoso.com\public to Exclude targets outside of the client's site.
E. Set the Advanced properties of the folder target in the Seattle office to Last among targets of equal cost.
F. Set the Ordering method of \\contoso.com\public to Lowest cost.

Correct Answer: CD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Exclude targets outside of the client's site
In this method, the referral contains only the targets that are in the same site as the client. These same-site targets are listed in random order. If no same-site targets exist, the client does not receive a referral and cannot access that portion of the namespace.
Note: Targets that have target priority set to "First among all targets" or "Last among all targets" are still listed in the referral, even if the ordering method is set to Exclude targets outside of the client's site.
Note 2: Set the Ordering Method for Targets in Referrals
A referral is an ordered list of targets that a client computer receives from a domain controller or namespace server when the user accesses a namespace root or folder with targets. After the client receives the referral, the client attempts to access the first target in the list. If the target is not available, the client attempts to access the next target.

QUESTION 60
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 61
Your network contains an Active Directory forest named contoso.com.

The domain contains three servers. The servers are configured as shown in the following table.

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

You plan to implement the BitLocker Drive Encryption (BitLocker) Network Unlock feature.

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

Which role should you identify?

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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:

Explanation:

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

References: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-enable-network-unlock

QUESTION 62

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

You create a custom Data Collector Set (DCS) named DCS1.

You need to configure DCS1 to collect the following requirements:
▪ Automatically run a program when the amount of total free disk space on Server1 drops below 10 percent of capacity. ▪ Log the current values of several registry settings.

Which two should you configure in DCS1? (Each correct answer presents part of the solution. Choose two.)

A. a performance counter
B. system configuration information
C. a Performance Counter Alert
D. event trace data

Correct Answer: BC
Section: Volume B
Explanation

Explanation/Reference:

Explanation:
System configuration information allows you to record the state of, and changes to, registry keys.

Total free disk space:

Create new Data Collector Set.

Which performance counters would you like to monitor?

Performance counters:

\LogicalDisk(_Total)\% Free Space

Add...

Remove

Alert when: Limit:

Below   10

Next   Finish   Cancel

Registry settings
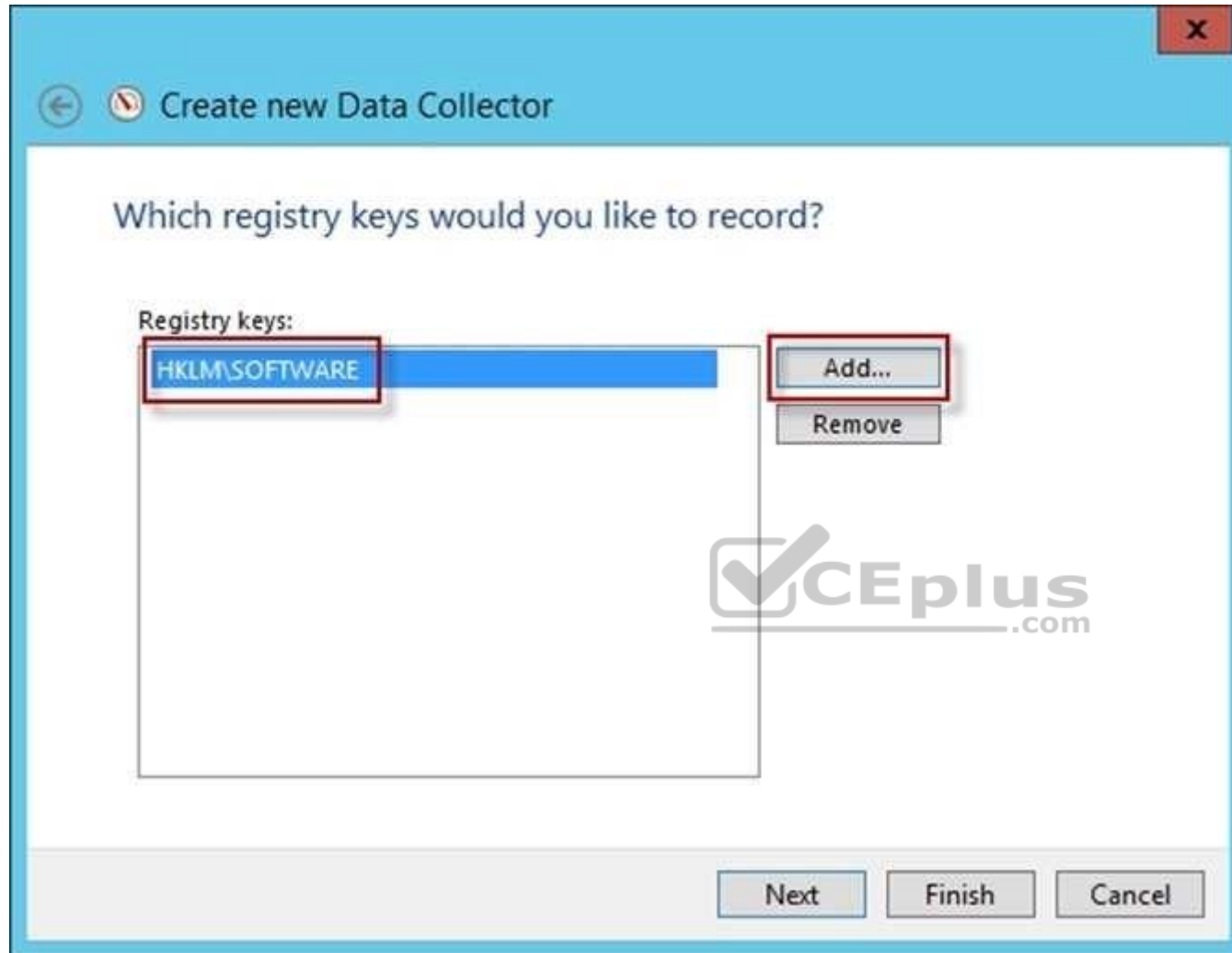
Run a program on alert

DataCollector01 Properties

Alerts | Alert Action | **Alert Task**

Run this task when an alert is triggered:

```
c:\windows\system32\shutdown.exe
```

Task arguments:

```
{usertext}                                              >
```

Task argument user text:

```
-s -f -t 30
```

Example task arguments:

```
-s -f -t 30
```

OK | Cancel | Apply | Help

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

QUESTION 63
Your network contains an Active Directory forest named contoso.com. The functional level of the forest is Windows Server 2008 R2.

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

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

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

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

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

You need to tell User1 what her minimum password length is.

What should you tell User1?

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

Correct Answer: D
Section: Volume B

Explanation

Explanation/Reference:
QUESTION 64
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains 30 user accounts that are used for network administration. The user accounts are members of a domain global group named Group1.

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

Security setting	Requirement
Minimum password length	20
Account is sensitive and cannot be delegated	Disabled
User cannot change password	Disabled
Enforce password history	30

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

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

Hot Area:

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

Correct Answer:

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

Section: Volume B
Explanation

Explanation/Reference:
Note:

* Password Setting Object (PSO) is another name for Fine Grain Password Policies.
* Here you can see all the settings that go into a PSO.

Create Password Settings:

✳ Password Settings

Directly Applies To

Password Settings

Name: ✳ [   ]

Precedence: ✳ [   ]

☑ Enforce minimum password length

    Minimum password length (characters): ✳ [7]

☑ Enforce password history

    Number of passwords remembered: ✳ [24]

☑ Password must meet complexity requirements

☐ Store password using reversible encryption

☑ Protect from accidental deletion

Description:
[   ]

Password age options:

☑ Enforce minimum password age

    User cannot change the password within (days): ✳

☑ Enforce maximum password age

    User must change the password after (days): ✳

☐ Enforce account lockout policy:

    Number of failed logon attempts allowed: ✳

    Reset failed logon attempts count after (mins): ✳

    Account will be locked out

    ◉ For a duration of (mins): ✳

    ○ Until an administrator manually unlocks the accou

Directly Applies To

Name ▲	Mail

ⓐ More Information

OK

QUESTION 65

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

A central store is configured on a domain controller named DC1.

You have a custom administrative template file named App1.admx. App1.admx contains application settings for an application named App1.

You copy App1.admx to the central store. You create a new Group Policy object (GPO) named App1_Settings.

When you edit App1_Settings, you receive the warning message shown in the following exhibit.

Administrative Templates

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

OK
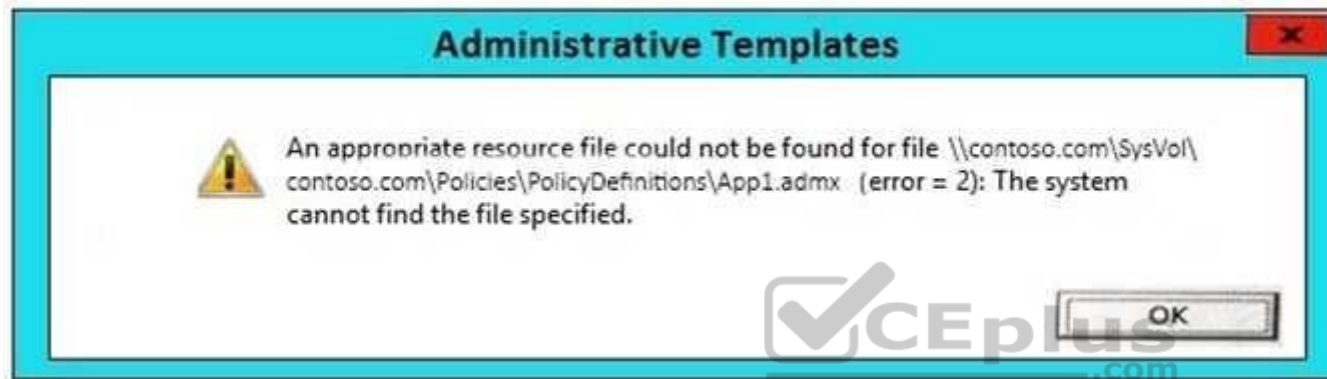
You need to ensure that you can edit the settings for App1 from the App1_Settings GPO.

What should you do?

A. Add an Administrative Template to the App1_Settings GPO.
B. Modify the permissions of the ADMX file.
C. Move the ADMX file to the local Policy definitions folder.
D. Copy an ADML file to the central store.

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/appv-v5/how-to-modify-app-v-50-client-configuration-using-the-admx-template-and-grouppolicy

QUESTION 66

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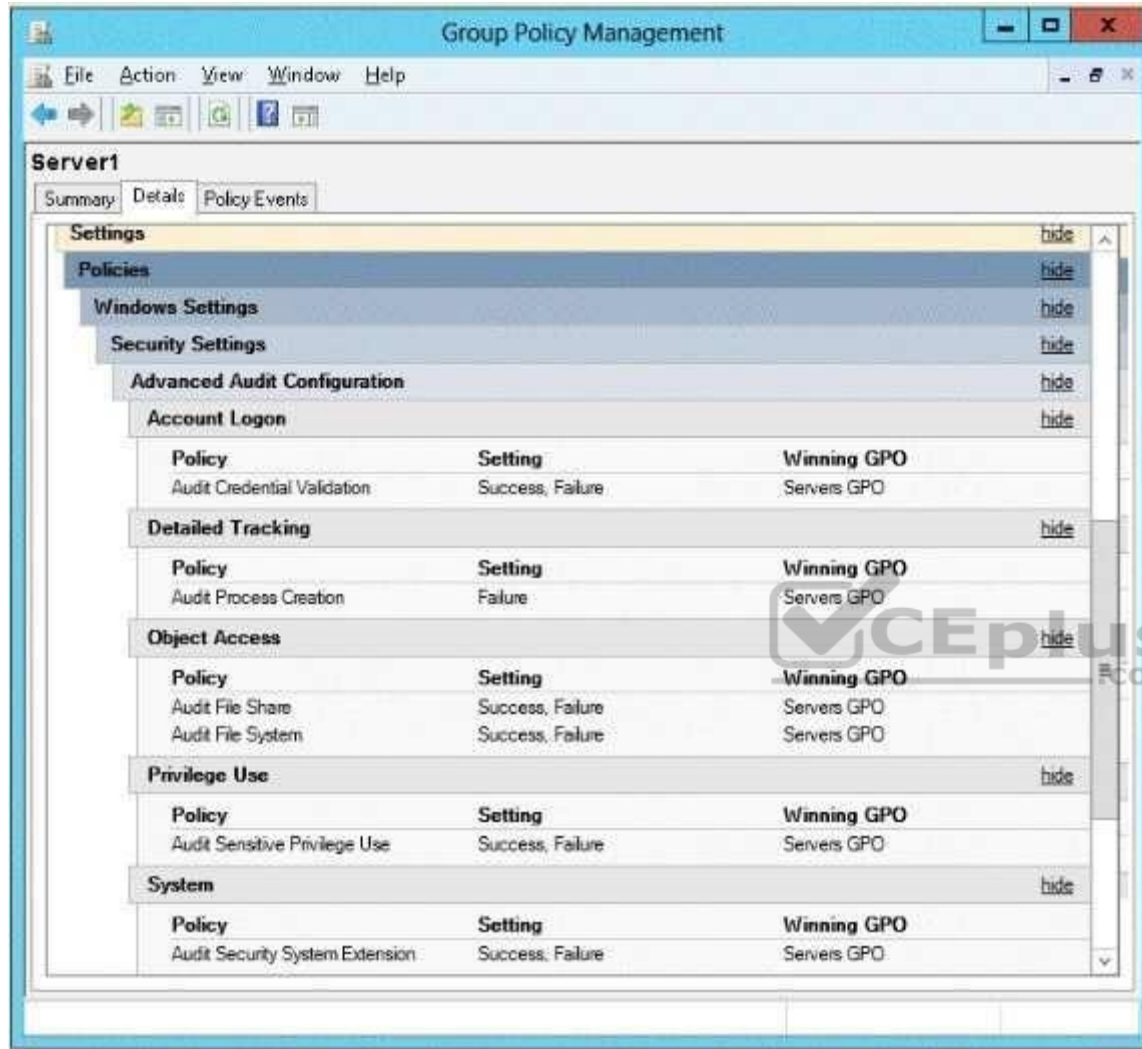
On Server1, you have a folder named C:\Share1 that is shared as Share1. Share1 contains confidential data. A group named Group1 has full control of the content in Share1.

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
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.
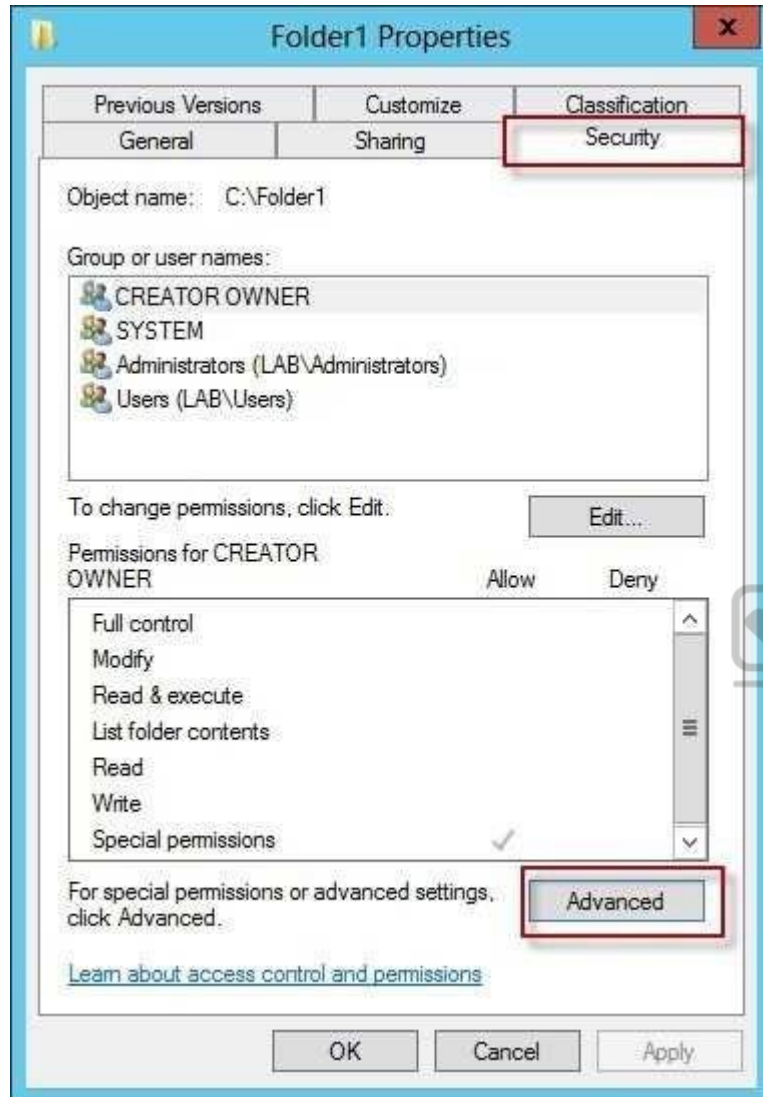
- Click Auditing and Edit.
- Click add, type everyone in the Select User, Computer, or Group.
- Choose Apply onto: This folder, subfolders and files. ▪
Tick on the box "Change permissions"

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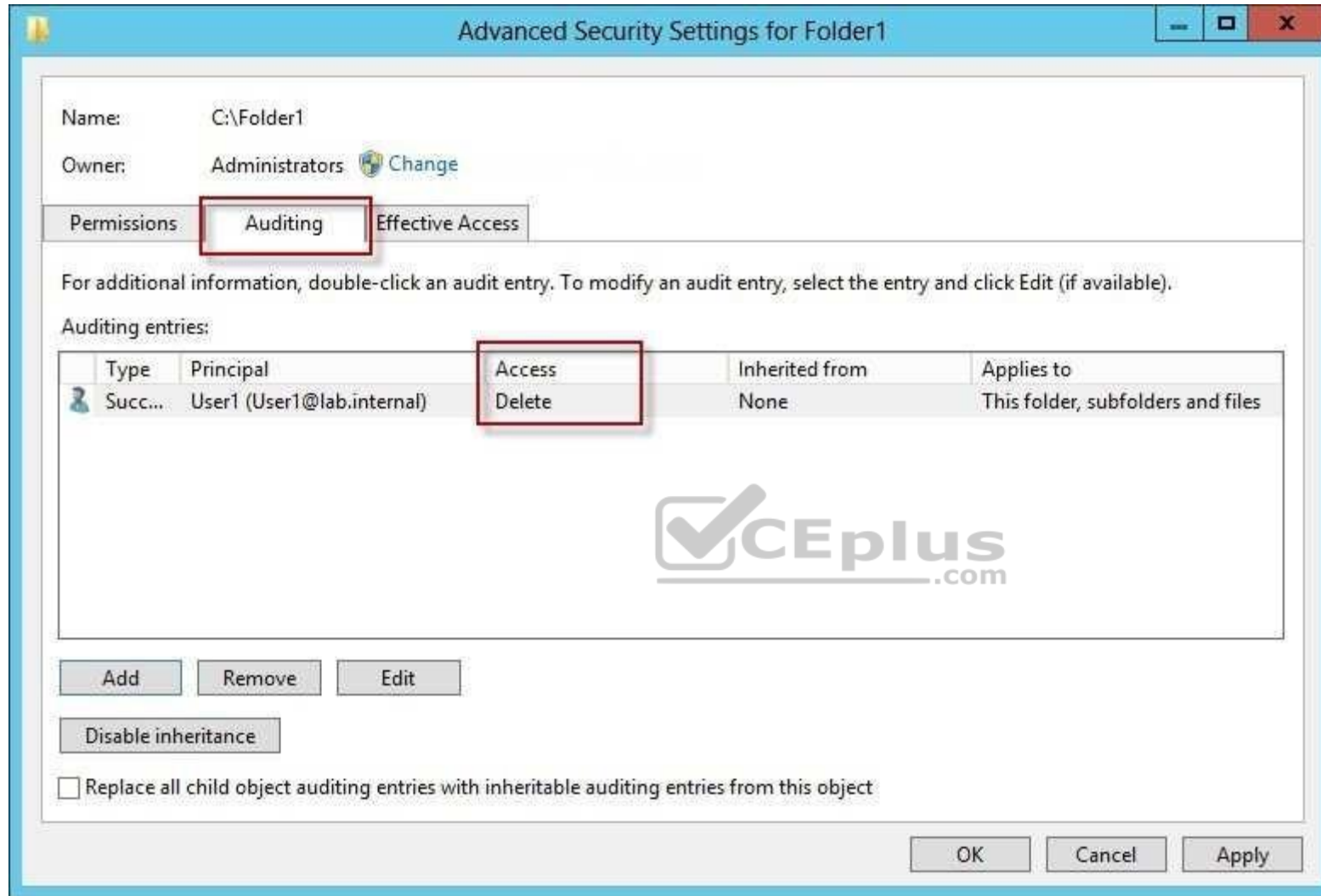
After you enable security auditing on the folders, you should be able to see the folder permission changes in the server's Security event log. Task Category is File System.

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 https://www.itprotoday.com/strategy/auditing-permission-changes-folder

QUESTION 67
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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
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

QUESTION 68
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

The domain contains an Edge Server named Server1. Server1 is configured as a DirectAccess server. Server1 has the following settings:

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

Your company uses split-brain DNS for the contoso.com zone.

You run the Remote Access Setup wizard as shown in the following exhibit. (Click the Exhibit button.)

You need to ensure that client computers on the Internet can establish DirectAccess connections to Server1.

Which additional name suffix entry should you add from the Remote Access Setup wizard?

- A. A Name Suffix value of da1.contoso.com and a blank DNS Server Address value
- B. A Name Suffix value of Server1.contoso.com and a DNS Server Address value of 65.55.37.62
- C. A Name Suffix value of dal.contoso.com and a DNS Server Address value of 65.55.37.62
- D. A Name Suffix value of Server1.contoso.com and a blank DNS Server Address value

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
Split-brain DNS is the use of the same DNS domain for both Internet and intranet resources. For example, the Contoso Corporation is using split brain DNS; contoso.com is the domain name for intranet resources and Internet resources. Internet users use http: //www.contoso.com to access Contoso's public Web site and Contoso employees on the Contoso intranet use http://www.contoso.com to access Contoso's intranet Web site. A Contoso employee with their laptop that is not a DirectAccess client on the intranet that accesses http://www.contoso.com sees the intranet Contoso Web site.

When they take their laptop to the local coffee shop and access that same URL, they will see the public Contoso Web site.
When a DirectAccess client is on the Internet, the Name Resolution Policy Table (NRPT) sends DNS name queries for intranet resources to intranet DNS servers. A typical NRPT for DirectAccess will have a rule for the namespace of the organization, such as contoso.com for the Contoso Corporation, with the Internet Protocol version 6 (IPv6) addresses of intranet DNS servers. With just this rule in the NRPT, when a user on a DirectAccess client on the Internet attempts to access the uniform resource locator (URL) for their Web site (such as http://www.contoso.com), they will see the intranet version. Because of this rule, they will never see the public version of this URL when they are on the Internet.

For split-brain DNS deployments, you must list the FQDNs that are duplicated on the Internet and intranet and decide which resources the DirectAccess client should reach, the intranet version or the public (Internet) version. For each name that corresponds to a resource for which you want DirectAccess clients to reach the public version, you must add the corresponding FQDN as an exemption rule to the NRPT for your DirectAccess clients. Name suffixes that do not have corresponding DNS servers are treated as exemptions.

References: http://technet.microsoft.com/en-
us/library/ee382323(v=ws.10).aspx

QUESTION 69
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.

Correct Answer: A

Section: Volume B
Explanation

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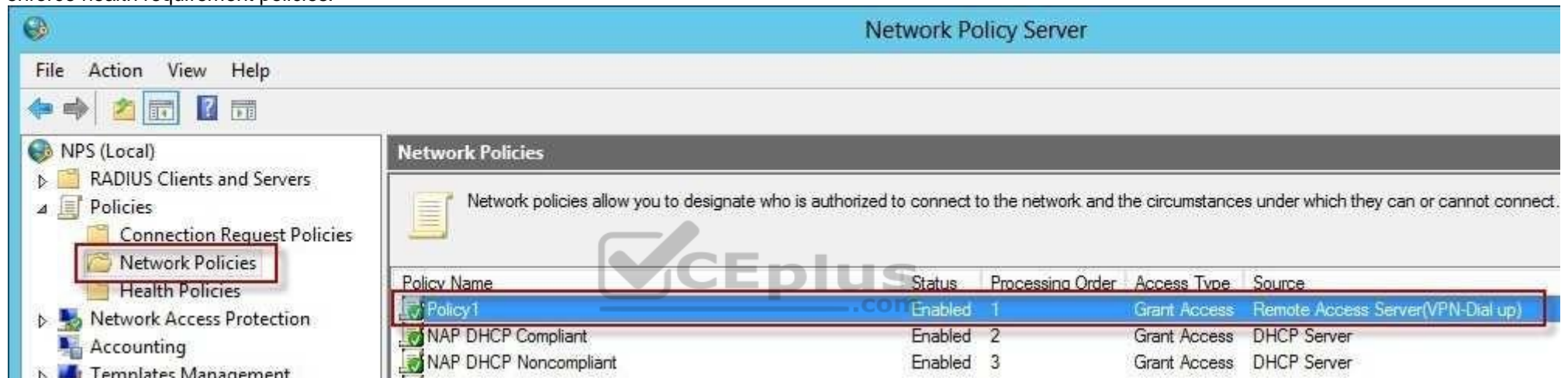
References:
http://technet.microsoft.com/en-us/library/hh831683.aspx http://technet.microsoft.com/en-us/library/cc754107.aspx http://technet.microsoft.com/en-us/windowsserver/dd448603.aspx
http://technet.microsoft.com/en-us/library/dd314165(v=ws.10).aspx http://technet.microsoft.com/en-us/library/dd469733.aspx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

QUESTION 70
Your network contains two servers named Served and Server 2. Both servers run Windows Server 2012 R2 and have the DNS Server server role installed.

On Server1, you create a standard primary zone named contoso.com.

You plan to create a standard primary zone for ad.contoso.com on Server2.

You need to ensure that Server1 forwards all queries for ad.contoso.com to Server2.

What should you do from Server1?

A. Create a trust anchor named Server2.
B. Create a conditional forward that points to Server2.
C. Add Server2 as a name server.
D. Create a zone delegation that points to Server2.

Correct Answer: D
Section: Volume B
Explanation
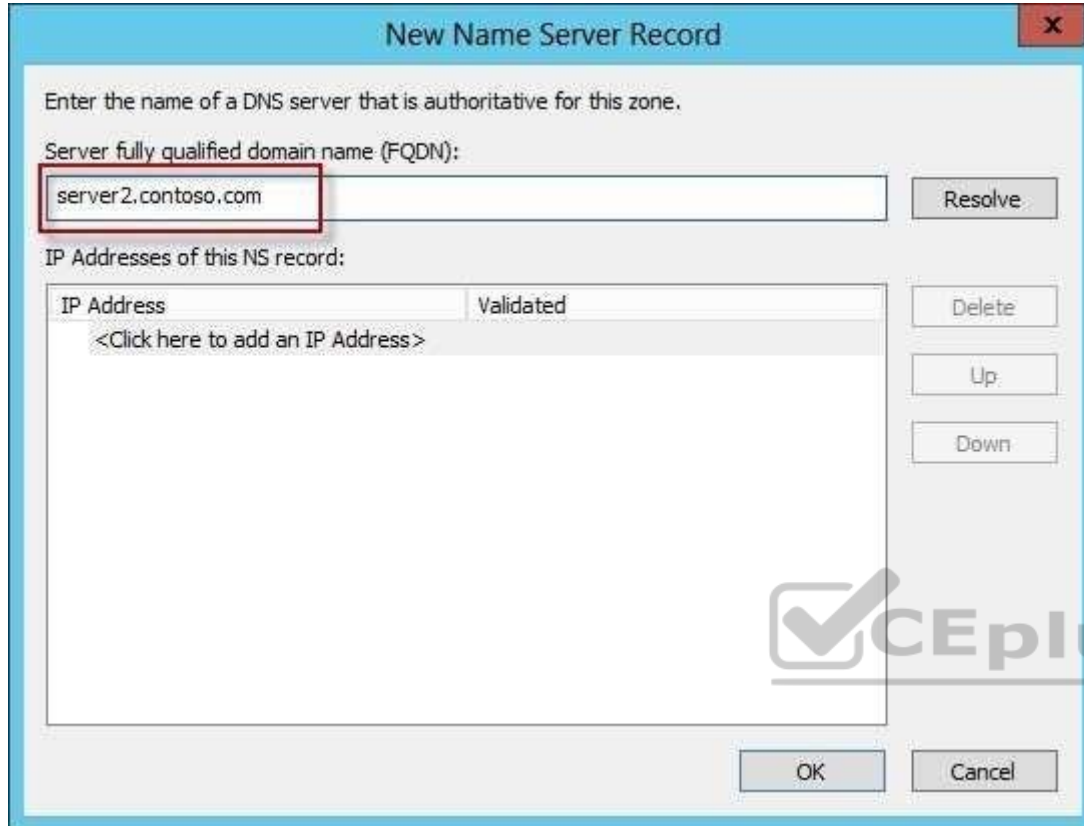
Explanation/Reference:
Explanation:
You can divide your Domain Name System (DNS) namespace into one or more zones. You can delegate management of part of your namespace to another
location or department in your organization by delegating the management of the corresponding zone. For more information, see Understanding Zone Delegation.

New Name Server Record

Enter the name of a DNS server that is authoritative for this zone.

Server fully qualified domain name (FQDN):

`server2.contoso.com`   [Resolve]

IP Addresses of this NS record:

IP Address	Validated
<Click here to add an IP Address>	

[Delete]
[Up]
[Down]

[OK]   [Cancel]
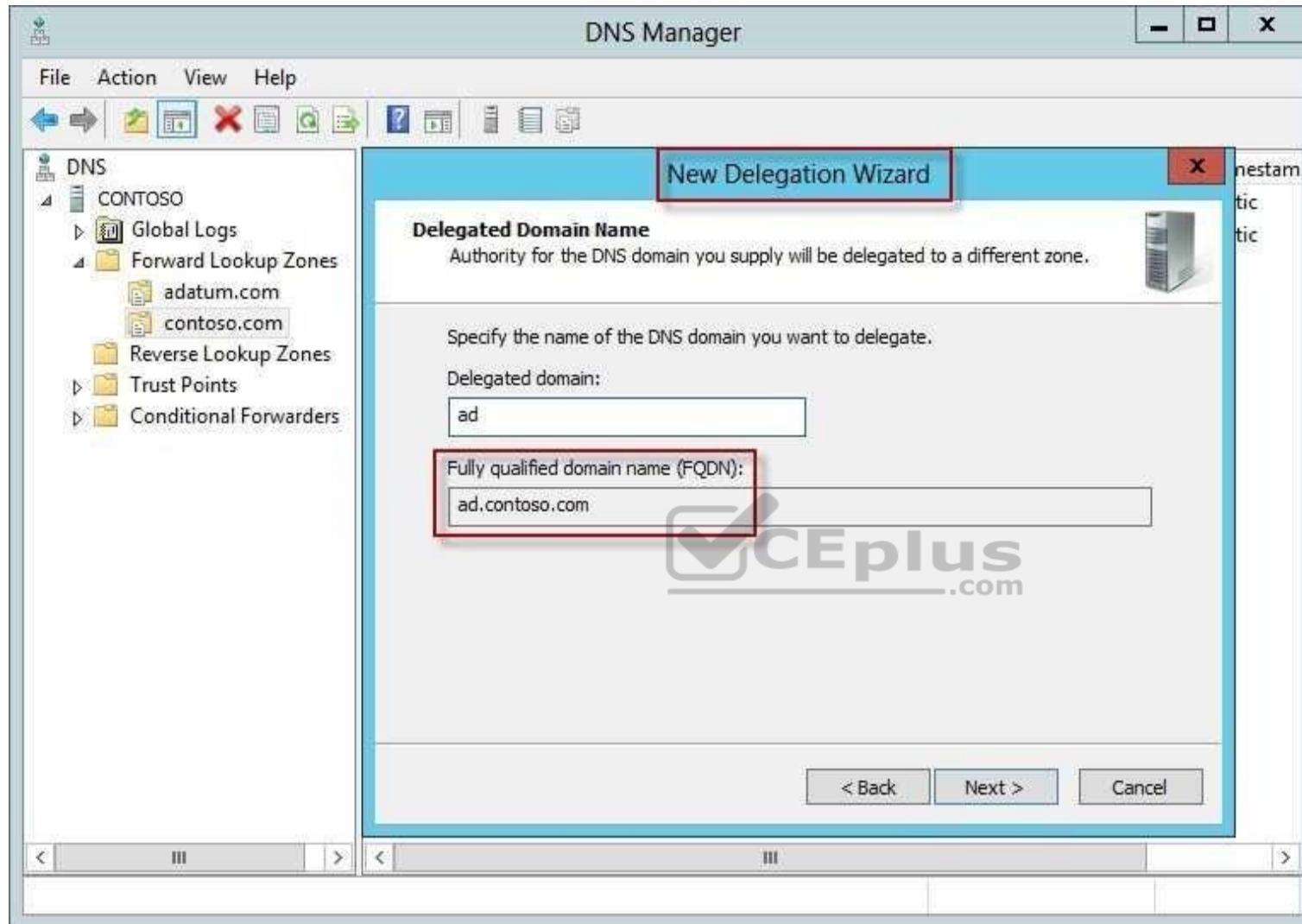
QUESTION 71
Your network contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2 and have the DNS Server server role installed. Server1 hosts a primary zone for contoso.com. Server2 hosts a secondary zone for contoso.com. The zone is not configured to notify secondary servers of changes automatically.

You update several records on Server1.

You need to force the replication of the contoso.com zone records from Server1 to Server2.

What should you do from Server2?

A. Right-click the contoso.com zone and click Reload.
B. Right-click the contoso.com zone and click Transfer from Master.

C. Right-click Server2 and click Update Server Data Files.
D. Right-click Server2 and click Refresh.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
Initiates zone transfer from secondary server
Open DNS; In the console tree, right-click the applicable zone and click Transfer from master.
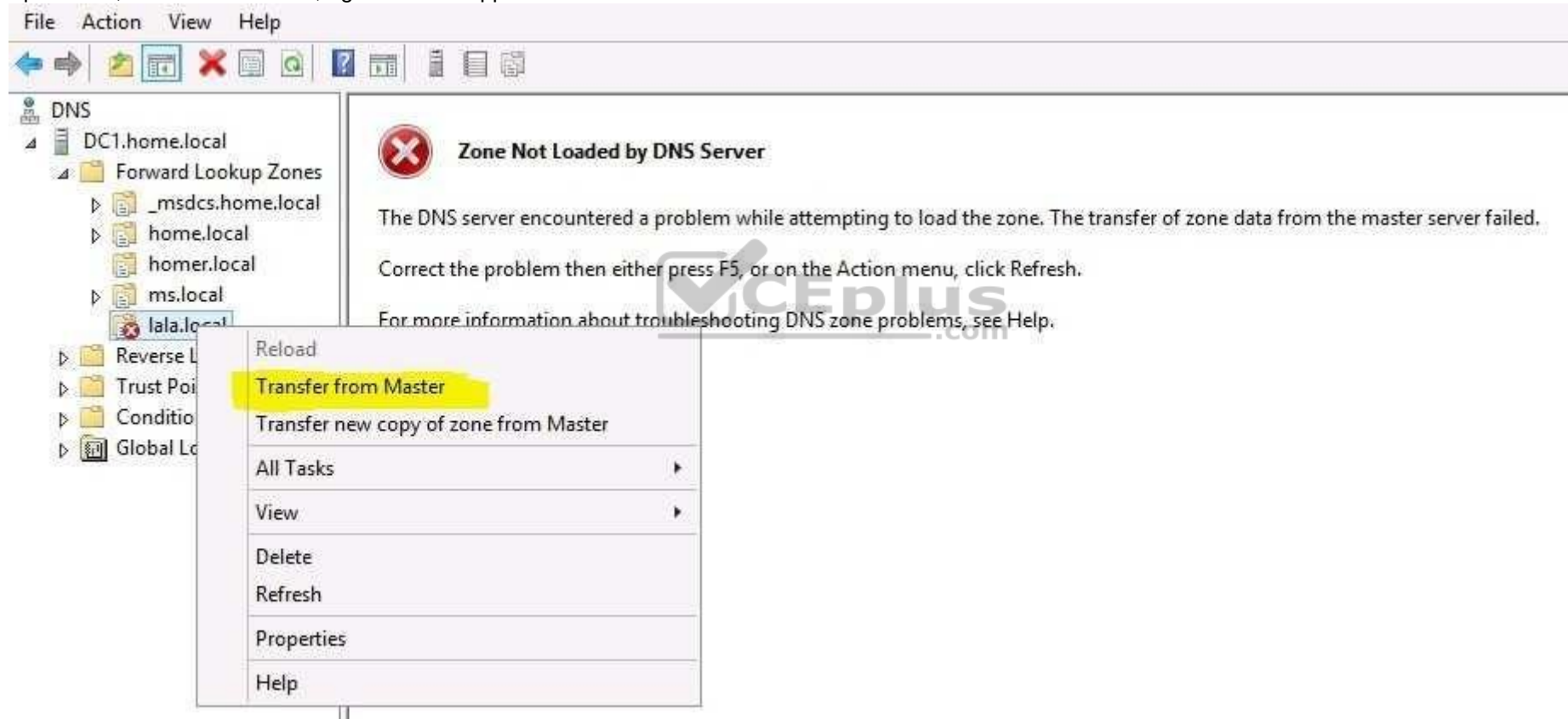
References:
http://technet.microsoft.com/en-us/library/cc786985(v=ws.10).aspx http://technet.microsoft.com/en-us/library/cc779391(v=ws.10).aspx

QUESTION 72
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.

should you use?

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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
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-GPUpdate cmdlet 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.

Domain Cont...

Create a GPO in this domain, and Link it here...

Link an Existing GPO...

Block Inheritance

Gro

Group Policy Update...

Group Policy Modeling Wizard...

WM

New Organizational Unit

Star

View ▶

New Window from Here

tes

roup Polic

Delete

roup Polic

Refresh

Properties

Help

Force Group Policy update

X

You have chosen to force a Group Policy update on all computers within Domain
Controllers and all subcontainers. If you choose 'Yes' below, User and Computer
policy settings will be updated on:

1 Computer

Are you sure you want to update policy for these computers?

| Yes | No | Help |

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

QUESTION 73
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

A domain controller named DO has the ADMX Migrator tool installed. You have a custom Administrative Template file on DC1 named Template1.adm.

You need to add a custom registry entry to Template1.adm by using the ADMX Migrator tool.

Which action should you run first?

A. Load Template

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

Correct Answer: C
Section: Volume B

Explanation

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

References: http://technet.microsoft.com/pt-pt/magazine/2008.02.utilityspotlight%28en-us%29.aspx
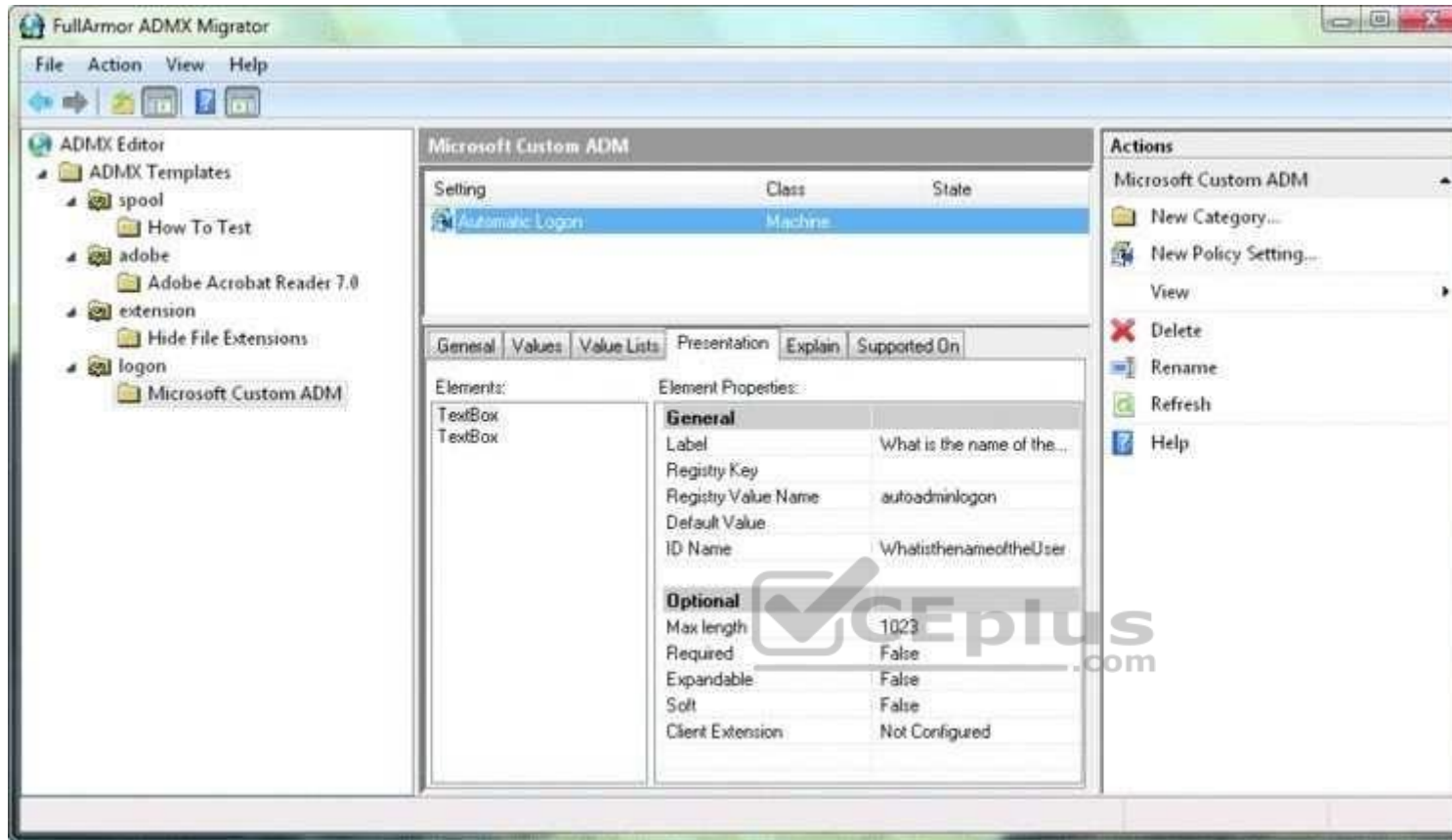
QUESTION 74

Your network contains an Active Directory domain named contoso.com. Network Access Protection (NAP) is deployed to the domain.

You need to create NAP event trace log files on a client computer.

What should you run?

A. logman
B. Register-ObjectEvent

C. tracert
D. Register-EngineEvent

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
You can enable NAP client tracing by using the command line. On computers running Windows Vista®, you can enable tracing by using the NAP Client Configuration console. NAP client tracing files are written in Event Trace Log (ETL) format. These are binary files representing trace data that must be decoded by Microsoft support personnel. Use the o option to specify the directory to which they are written. In the following example, files are written to %systemroot%\tracing \nap. For more information, see Logman (http://go.microsoft.com/fwlink/?LinkId=143549). To create NAP event trace log files on a client computer

- Open a command line as an administrator.
- Type logman start QAgentRt -p {b0278a28-76f1-4e15-b1df-14b209a12613} 0xFFFFFFFF 9 -o %systemroot%\tracing\nap\QAgentRt. etl –ets. Note: To troubleshoot problems with WSHA, use the following GUID: 789e8f15-0cbf-4402-b0ed-0e22f90fdc8d.
- Reproduce the scenario that you are troubleshooting.
- Type logman stop QAgentRt -ets.
- Close the command prompt window.

References: http://technet.microsoft.com/en-us/library/dd348461%28v=ws.10%29.aspx

QUESTION 75
Your network contains three Network Policy Server (NPS) servers named NPS1, NPS2, and NPS3.

NP51 is configured as a RADIUS proxy that forwards connection requests to a remote RADIUS server group named Group1.

You need to ensure that NPS2 receives connection requests. NPS3 must only receive connection requests if NPS2 is unavailable.

How should you configure Group1?

A. Change the Priority of NPS3 to 10.
B. Change the Weight of NPS2 to 10.
C. Change the Weight of NPS3 to 10.
D. Change the Priority of NPS2 to 10.

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:

Explanation:

Priority. Priority specifies the order of importance of the RADIUS server to the NPS proxy server. Priority level must be assigned a value that is an integer, such as 1, 2, or 3. The lower the number, the higher priority the NPS proxy gives to the RADIUS server. For example, if the RADIUS server is assigned the highest priority of 1, the NPS proxy sends connection requests to the RADIUS server first; if servers with priority 1 are not available, NPS then sends connection requests to RADIUS servers with priority 2, and so on. You can assign the same priority to multiple RADIUS servers, and then use the Weight setting to load balance between them.

QUESTION 76

Your network contains two Active Directory forests named adatum.com and contoso.com. The network contains three servers. The servers are configured as shown in the following table.

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

You need to ensure that connection requests from adatum.com users are forwarded to Server2 and connection requests from contoso.com users are forwarded to Server3.

Which two should you configure in the connection request policies on Server1? (Each correct answer presents part of the solution. Choose two.)

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

Correct Answer: AE
Section: Volume B
Explanation

Explanation/Reference:

Explanation:

The User Name attribute group contains the User Name attribute. By using this attribute, you can designate the user name, or a portion of the user name, that must match the user name supplied by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name. You can use pattern matching syntax to specify user names.
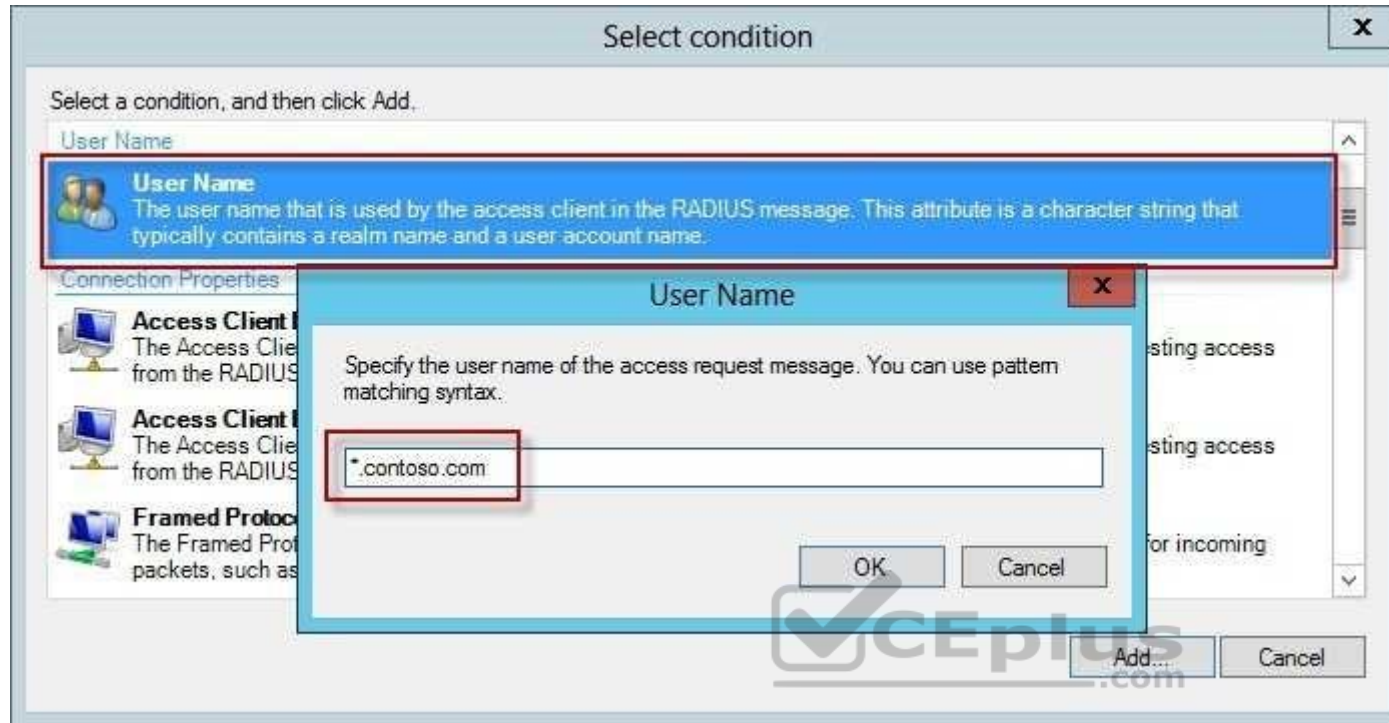
By using this setting, you can override the authentication settings that are configured in all network policies and you can designate the authentication methods and types that are required to connect to your network.

Forward requests to the following remote RADIUS server group . By using this setting, NPS forwards connection requests to the remote RADIUS server group that you specify. If the NPS server receives a valid Access-Accept message that corresponds to the Access- Request message, the connection attempt is considered authenticated and authorized. In this case, the NPS server acts as a RADIUS proxy
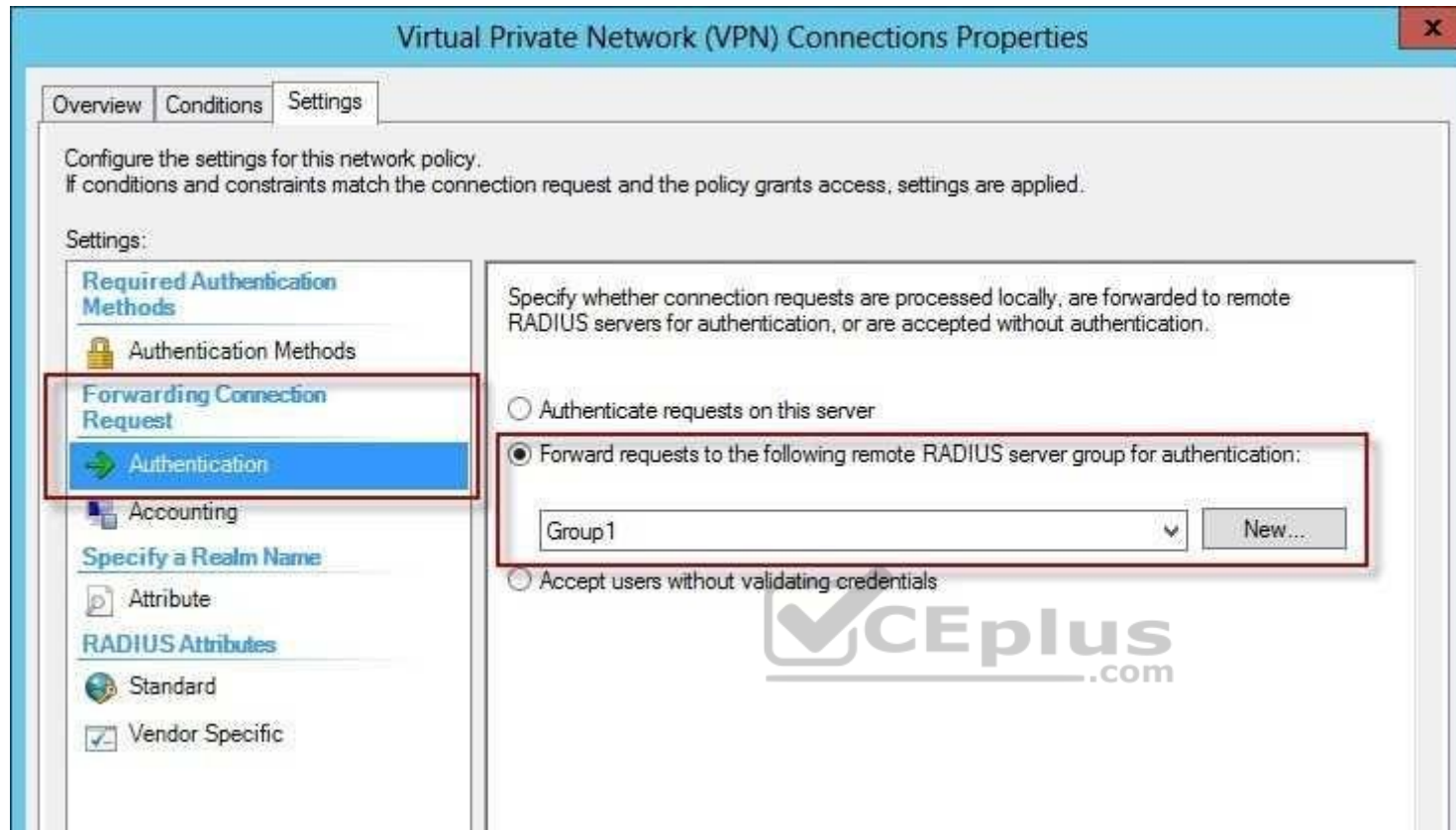
Connection request policies are sets of conditions and profile settings that give network administrators flexibility in configuring how incoming authentication and accounting request messages are handled by the IAS server. With connection request policies, you can create a series of policies so that some RADIUS request messages sent from RADIUS clients are processed locally (IAS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (IAS is being used as a RADIUS proxy). This capability allows IAS to be deployed in many new RADIUS scenarios.

With connection request policies, you can use IAS as a RADIUS server or as a RADIUS proxy, based on the time of day and day of the week, by the realm name in the request, by the type of connection being requested, by the IP address of the RADIUS client, and so on.

References:
http://technet.microsoft.com/en-us/library/cc757328.aspx http://technet.microsoft.com/en-us/library/cc753603.aspx

QUESTION 77
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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
Performance alerts notify you when a specified performance counter exceeds your configured threshold by logging an event to the event log. But rather than notifying you immediately when the counter exceeds the threshold, you can configure a time period over which the counter needs to exceed the threshold, to avoid unnecessary alerts.

Performance Monitoring Details

General | Alert | History & Trending

☑ Enable Event Log Alert with severity | Warning ▾

Alert if value is | more than ▾

15000 ⬍ for 10 ⬍ minute(s) ▾

☑ Notify at most once every | 1 ⬍ hour(s) ▾

☑ Embed chart with email alerts

☐ Enable Trend Detection   Detect Leaks:

mild (few false positives) ▾

Min: 0 , Max: 0 , Last: 0

OK | Cancel | Help
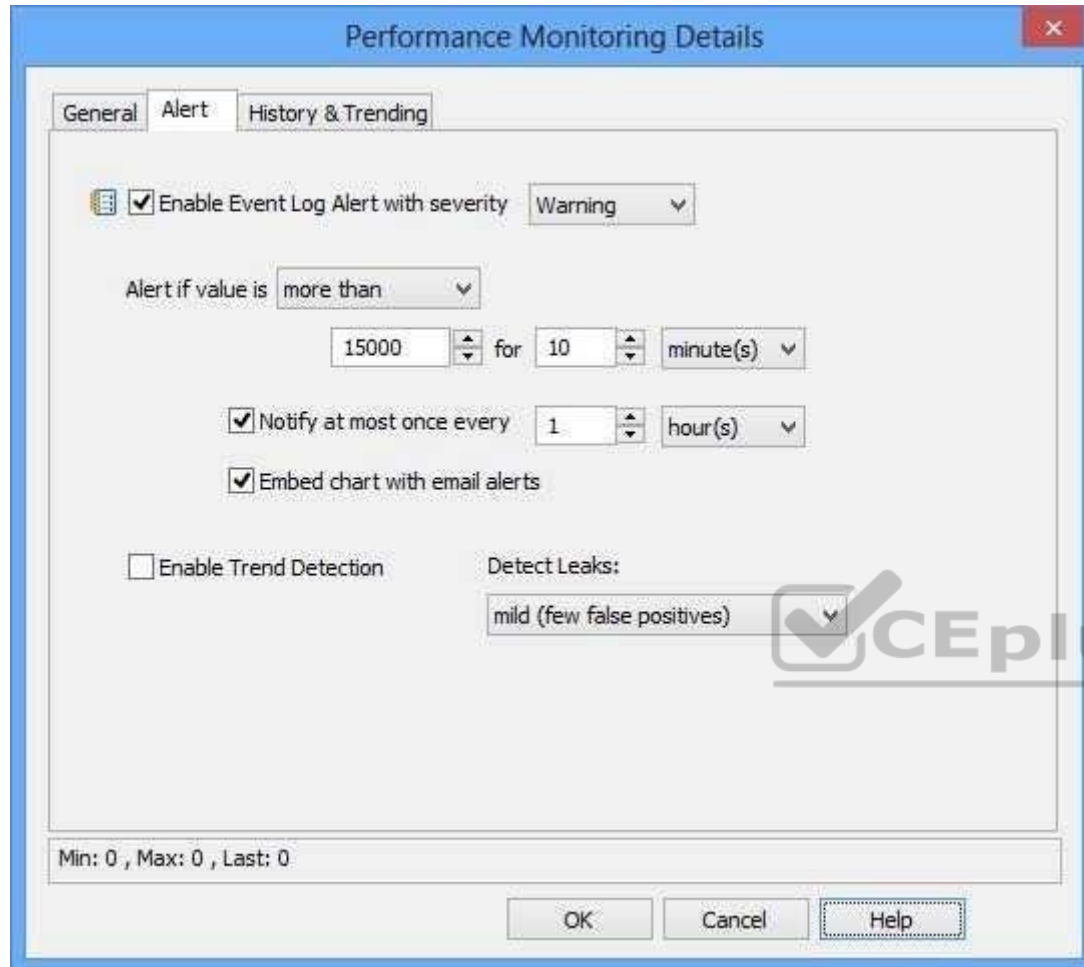
QUESTION 78
You have a server that runs Windows Server 2012 R2.

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 Windows2012.vhd to D:\Mount.

Which tool should you use?

A. Server Manager

B. Device Manager

C. Mountvol

D. Dism

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
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.

QUESTION 79
Your network contains a domain controller named DC1 that runs Windows Server 2012 R2.

You create a custom Data Collector Set (DCS) named DCS1.

You need to configure DCS1 to collect the following information:
▪ The amount of Active Directory data replicated between DC1 and the other domain controllers ▪
The current values of several registry settings

Which two should you configure in DCS1? (Each correct answer presents part of the solution. Choose two.)

A. Event trace data

B. A Performance Counter Alert

C. System configuration information

D. A performance counter

Correct Answer: BD
Section: Volume B
Explanation
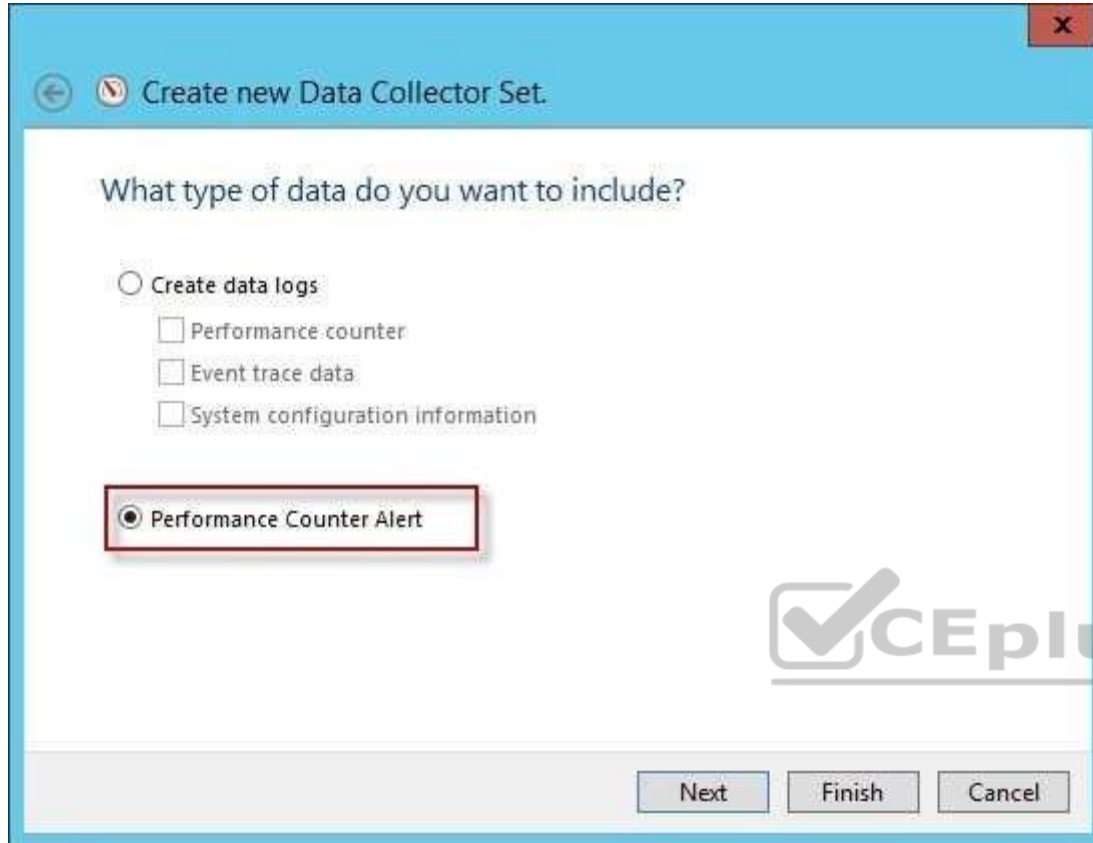
Explanation/Reference:
Explanation:
Automatically run a program when the amount of total free disk space on Server1 drops below 10 percent of capacity. You can also configure alerts to start applications and performance logs Log the current values of several registry settings.

System configuration information allows you to record the state of, and changes to, registry keys.
Total free disk space
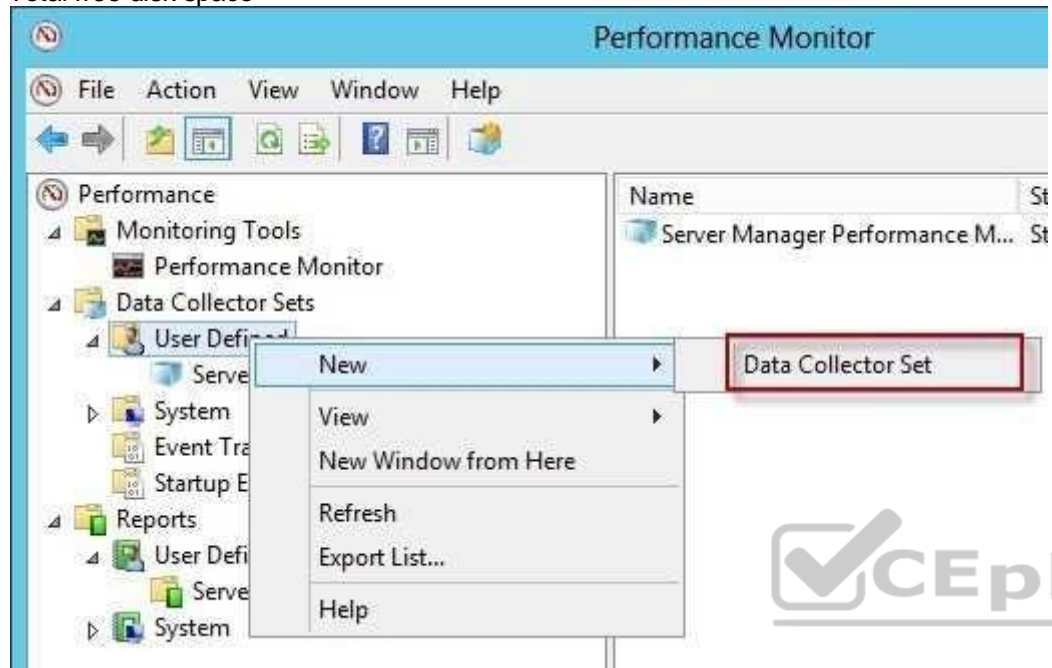
Create new Data Collector Set.

What type of data do you want to include?

○ Create data logs
  ☐ Performance counter
  ☐ Event trace data
  ☐ System configuration information

● Performance Counter Alert

Next   Finish   Cancel

Available counters

Select counters from computer:

<Local computer>   ▾   Browse...

KPSSVC	▾
LogicalDisk	^
% Disk Read Time	
% Disk Time	
% Disk Write Time	
% Free Space	
% Idle Time	
Avg. Disk Bytes/Read	
Avg. Disk Bytes/Transfer	˅

Instances of selected object:

_Total
<All Instances>
C:

▾   Search

Add >>

Added counters

Counter	Parent	Inst...	Computer
LogicalDisk			^
% Free Space	---	_Total	

Remove <<

☑ Show description

Help   OK   Cancel

Description:

% Free Space is the percentage of total usable space on the selected logical disk drive that was free.
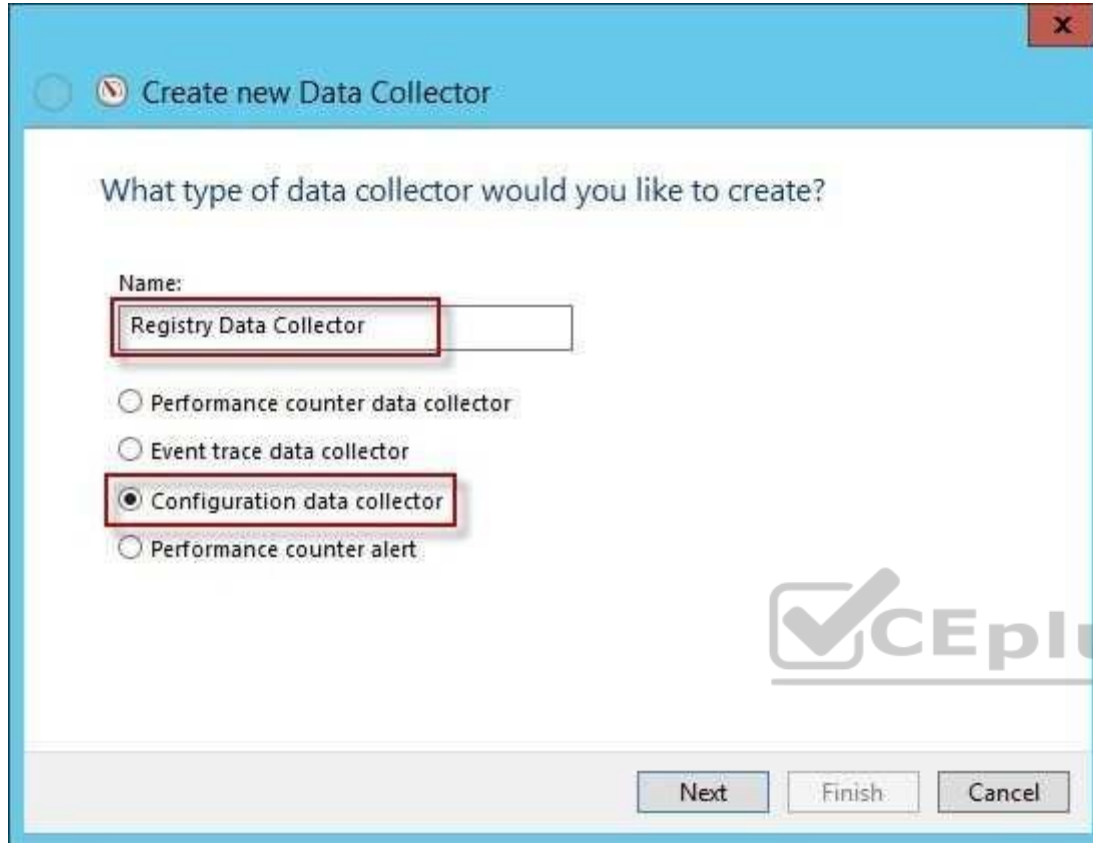
Registry settings

Create new Data Collector
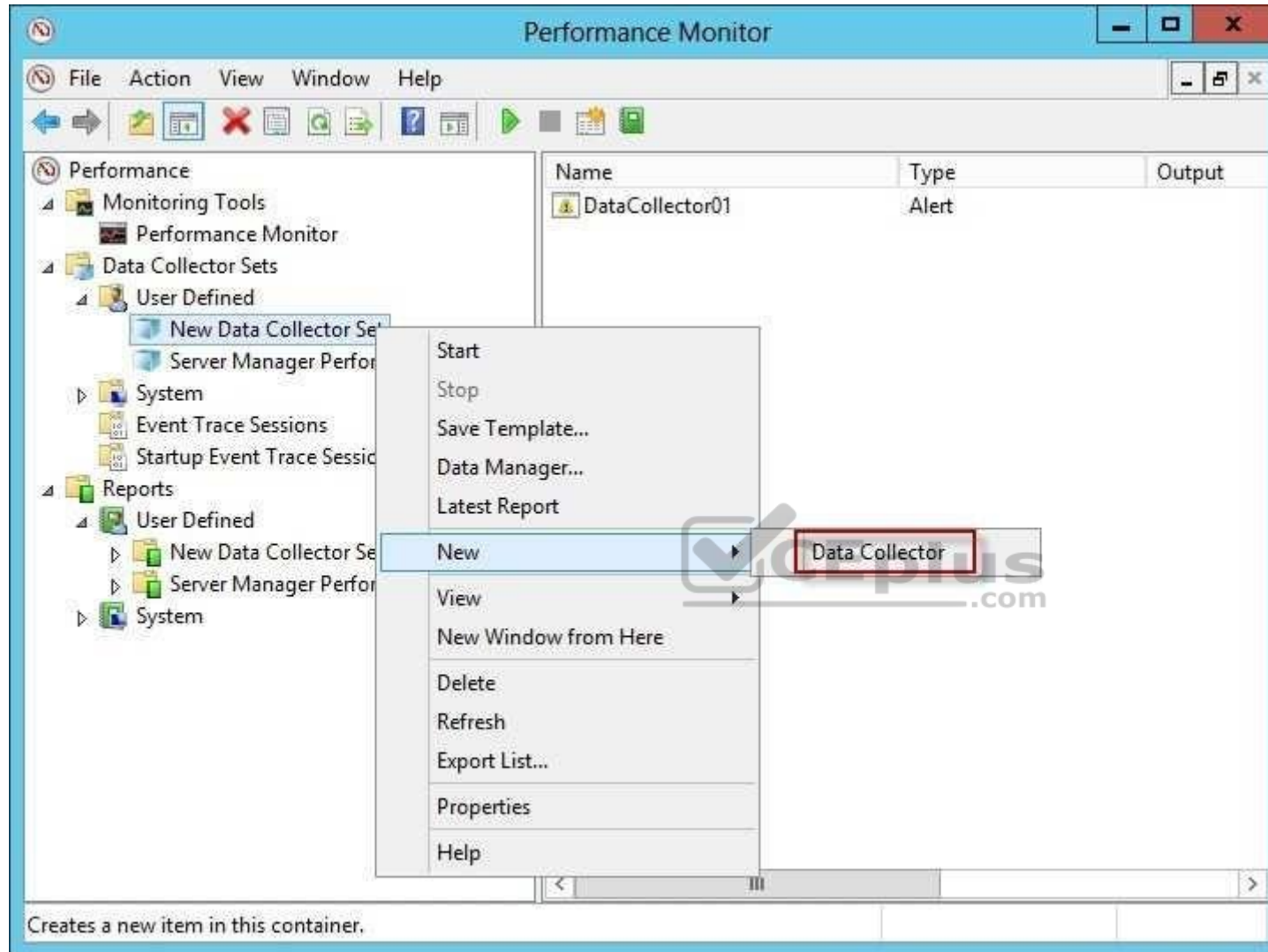
What type of data collector would you like to create?

Name:

Registry Data Collector

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

[Next]   [Finish]   [Cancel]

Run a program on alert

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

QUESTION 80
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Deployment Services server role installed.

Server1 contains two boot images and four install images.

You need to ensure that when a computer starts from PXE, the available operating system images appear in a specific order.

What should you do?

A. Modify the properties of the boot images.
B. Create a new image group.

C. Modify the properties of the install images.
D. Modify the PXE Response Policy.

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:

QUESTION 81
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.

An organizational unit (OU) named ResearchServers contains the computer accounts of all research servers.

All domain users are configured to have a minimum password length of eight characters.

You need to ensure that the minimum password length of the local user accounts on the research servers in the ResearchServers OU is 10 characters.

What should you do?

A. Configure a local Group Policy object (GPO) on each research server.
B. Create and link a Group Policy object (GPO) to the ResearchServers OU.
C. Create a universal group that contains the research servers. Create a Password Settings object (PSO) and assign the PSO to the group.
D. Create a global group that contains the research servers. Create a Password Settings object (PSO) and assign the PSO to the group.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
For a domain, and you are on a member server or a workstation that is joined to the domain
1. Open Microsoft Management Console (MMC).
2. On the File menu, click Add/Remove Snap-in, and then click Add.
3. Click Group Policy Object Editor, and then click Add.
4. In Select Group Policy Object, click Browse.

5. In Browse for a Group Policy Object, select a Group Policy object (GPO) in the appropriate domain, site, or organizational unit--or create a new one, click OK, and then click Finish.
6. Click Close, and then click OK.

7. In the console tree, click Password Policy.
Where?
Group Policy Object [computer name] Policy/Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy
8. In the details pane, right-click the policy setting that you want, and then click Properties.
9.   If you are defining this policy setting for the first time, select the Define this policy setting check box.
10. Select the options that you want, and then click OK.

QUESTION 82
Your network contains an Active Directory domain named contoso.com. The domain contains six domain controllers. The domain controllers are configured as shown in the following table.

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

The network contains a server named Server1 that has the Hyper-V server role installed. DC6 is a virtual machine that is hosted on Server1.

You need to ensure that you can clone DC6.

What should you do?

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

Correct Answer: D
Section: Volume B
Explanation

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

References: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/virtualized-domain-controller-deployment-andconfiguration#BKMK_VDCCloning

QUESTION 83
Your company deploys a new Active Directory forest named contoso.com. The first domain controller in the forest runs Windows Server 2012 R2. The forest contains a domain controller named DC10.

On DC10, the disk that contains the SYSVOL folder fails.

You replace the failed disk. You stop the Distributed File System (DFS) Replication service. You restore the SYSVOL folder.

You need to perform a non-authoritative synchronization of SYSVOL on DC10.

Which tool should you use before you start the DFS Replication service on DC10?

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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
How to perform a non-authoritative synchronization of DFSR-replicated SYSVOL (like "D2" for FRS)

▪ In the ADSIEDIT. MSC tool modify the following distinguished name (DN) value and attribute on each of the domain controllers that you want to make nonauthoritative:

  CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain> msDFSR-Enabled=FALSE
▪ Force Active Directory replication throughout the domain.
▪ Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:
  DFSRDIAG POLLAD

- You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated.
- On the same DN from Step 1, set: msDFSR-Enabled=TRUE
- Force Active Directory replication throughout the domain.
- Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:
  DFSRDIAG POLLAD
- You will see Event ID 4614 and 4604 in the DFSR event log indicating SYSVOL has been initialized. That domain controller has now done a "D2" of SYSVOL.

Note: Active Directory Service Interfaces Editor (ADSI Edit) is a Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory. ADSI Edit (adsiedit. msc) provides a view of every object and attribute in an Active Directory forest. You can use ADSI Edit to query, view, and edit attributes that are not exposed through other Active Directory Microsoft Management Console (MMC) snap- ins: Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and Active Directory Schema.

QUESTION 84
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

On all of the domain controllers, Windows is installed in C:\Windows and the Active Directory database is located in D:\Windows\NTDS\.

All of the domain controllers have a third-party application installed.

The operating system fails to recognize that the application is compatible with domain controller cloning.

You verify with the application vendor that the application supports domain controller cloning.

You need to prepare a domain controller for cloning.

What should you do?

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

Correct Answer: C
Section: Volume B
Explanation
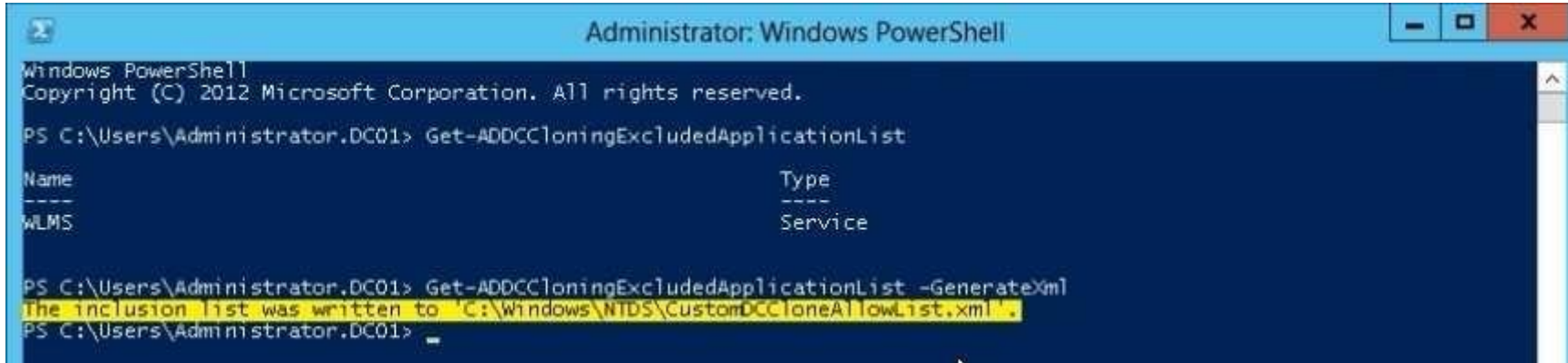
Explanation/Reference:
Explanation:
Place the CustomDCCloneAllowList.xml file in the same folder as the Active Directory database (ntds. dit) on the source Domain Controller.

References:
http://blogs.dirteam.com/blogs/sanderberkouwer/archive/2012/09/10/new-features-in-active-directory-domain-services-in-windows-server-2012-part-13-domaincontroller-cloning.aspx http://www.thomasmaurer.ch/2012/08/windows-server-2012-hyper-v-how-to-clone-a-virtual-domain-controller
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/virtualized-domain-controller-deployment-andconfiguration#BKMK_VDCCloning

QUESTION 85
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.

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
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.

User1 Properties

Organization	Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	**Delegation**

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

- ⦿ Do not trust this user for delegation
- ○ Trust this user for delegation to any service (Kerberos only)
- ○ Trust this user for delegation to specified services only
  - ⦿ Use Kerberos only
  - ○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N:

☐ Expanded   Add...   Remove

OK   Cancel   Apply   Help

QUESTION 86
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012 R2. The forest contains a single domain.

You create a Password Settings object (PSO) named PSO1.

You need to delegate the rights to apply PSO1 to the Active Directory objects in an organizational unit named OU1.

What should you do?

A. From Active Directory Users and Computers, run the Delegation of Control Wizard.
B. From Active Directory Administrative Center, modify the security settings of PSO1.
C. From Group Policy Management, create a Group Policy object (GPO) and link the GPO to OU1.
D. From Active Directory Administrative Center, modify the security settings of OU1.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
PSOs cannot be applied to organizational units (OUs) directly. If your users are organized into OUs, consider creating global security groups that contain the users from these OUs and then applying the newly defined finegrained password and account lockout policies to them. If you move a user from one OU to another, you must update user memberships in the corresponding global security groups.
Go ahead and hit "OK" and then close out of all open windows. Now that you have created a password policy, we need to apply it to a user/group. In order to do so, you must have "write" permissions on the PSO object. We're doing this in a lab, so I'm Domain Admin. Write permissions are not a problem ▪ Open Active Directory Users and Computers (Start, point to Administrative Tools, and then click Active Directory Users and Computers). ▪ On the View menu, ensure that Advanced Features is checked.
▪ In the console tree, expand Active Directory Users and Computers\yourdomain\System\Password Settings Container ▪
In the details pane, right-click the PSO, and then click Properties.
▪ Click the Attribute Editor tab.
▪ Select the msDS-PsoAppliesTo attribute, and then click Edit.

QUESTION 87
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The domain contains two servers. The servers are configured as shown in the following table.

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

All client computers run Windows 8.1 Enterprise.

You plan to deploy Network Access Protection (NAP) by using IPSec enforcement.

A Group Policy object (GPO) named GPO1 is configured to deploy a trusted server group to all of the client computers.

You need to ensure that the client computers can discover HRA servers automatically.

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

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

Correct Answer: ABE
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Requirements for HRA automatic discovery

The following requirements must be met in order to configure trusted server groups on NAP client computers using HRA automatic discovery:

▪ Client computers must be running Windows Vista® with Service Pack 1 (SP1) or Windows XP with Service Pack 3 (SP3). ▪
The HRA server must be configured with a Secure Sockets Layer (SSL) certificate.
▪ The EnableDiscovery registry key must be configured on NAP client computers.

- DNS SRV records must be configured.
- The trusted server group configuration in either local policy or Group Policy must be cleared.

http://technet.microsoft.com/en-us/library/dd296901.aspx

QUESTION 88
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has the Network Policy Server server role installed. The domain contains a server named Server2 that is configured for RADIUS accounting.

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

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

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

Hot Area:

Network Policy Server

File   Action   View   Help

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

Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request

Standard Configuration

Select a configuration scenario from the list and then click

Network Access Protection (NAP)

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, y the configuration of NAP-capable client computers before t compliant with health policy can be placed on a restricted r into compliance.

Configure NAP

Correct Answer:

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 89
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed.

Your company's security policy requires that certificate-based authentication must be used by some network services.

You need to identify which Network Policy Server (NPS) authentication methods comply with the security policy.

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

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

Correct Answer: BD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses serverside public key certificates to authenticate the server.
When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other.

QUESTION 90
Your network contains an Active Directory domain named adatum.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2.

All client computers run Windows 7.

You need to ensure that user settings are saved to \\Server1\Users\.

What should you do?

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

Correct Answer: C
Section: Volume B

Explanation

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

QUESTION 91
A technician installs a new server that runs Windows Server 2012 R2.

During the installation of Windows Server Update Services (WSUS) on the new server, the technician reports that on the Choose Languages page of the Windows Server Update Services Configuration Wizard, the only available language is English.

The technician needs to download updates in French and English.

What should you tell the network technician to do to ensure that the required updates are available?

A. Download WSUS 3.0 in French from the Microsoft Download Center.
B. From the Windows Server Update Services Configuration Wizard, configure the server to use the Microsoft Update servers.
C. Change the System Local of the server to French.
D. Install Microsoft SQL Server 2014, and then configure the default collation to include the accent-sensitive option.
E. Add the French language pack to the server.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
If the server is configured to use an upstream server that does not have the required languages available, then the languages won't be available for you to select. If you configure the server to use the Microsoft Update servers, all language options will be available.

Configure upstream servers to synchronize updates in all languages that are required by downstream replica servers. You will not be notified of needed updates in the unsynchronized languages.

The Choose Languages page of the WSUS Configuration Wizard allows you to get updates from all languages or from a subset of languages. Selecting a subset of languages saves disk space, but it is important to choose all the languages that are needed by all the downstream servers and client computers of a WSUS server. Downstream servers and client computers will not receive all the updates they need if you have not selected all the necessary languages for the upstream server. Make sure you select all the languages that will be needed by all the client computers of all the downstream servers. You should generally download updates in all languages on the root WSUS server that synchronizes to Microsoft Update. This selection guarantees that all downstream servers and client computers will receive updates in the languages that they require.

To choose update languages for a downstream server: If the upstream server has been configured to download update files in a subset of languages: In the WSUS Configuration Wizard, click Download updates only in these languages (only languages marked with an asterisk are supported by the upstream server), and then select the languages for which you want updates.

References: https://technet.microsoft.com/en-us/library/cc708431(v=ws.10).aspx

QUESTION 92
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2.

All client computers run Windows 8 Enterprise.

DC1 contains a Group Policy object (GPO) named GPO1.

You need to update the PATH variable on all of the client computers.

Which Group Policy preference should you configure?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
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.

QUESTION 93
Your company has a main office and a branch office.

The main office contains a server that hosts a Distributed File System (DFS) replicated folder.
You plan to implement a new DFS server in the branch office.

You need to recommend a solution that minimizes the amount of network bandwidth used to perform the initial synchronization of the folder to the branch office.

You recommend using the Export-DfsrClone and Import-DfsrClonecmdlets.

Which additional command or cmdlet should you include in the recommendation?

A. Robocopy.exe
B. Synchost.exe
C. Export-BcCachePackage
D. Sync-DfsReplicationGroup

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
By preseeding files before you set up DFS Replication, add a new replication partner, or replace a server, you can speed up initial synchronization and enable cloning of the DFS Replication database in Windows Server 2012 R2. The Robocopy method is one of several preceding methods

QUESTION 94
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2. Both servers have the File and Storage Services server role, the DFS Namespaces role service, and the DFS Replication role service installed.

Server1 and Server2 are part of a Distributed File System (DFS) Replication group named Group1. Server1 and Server2 are separated by a low-speed WAN connection.

You need to limit the amount of bandwidth that DFS can use to replicate between Server1 and Server2.

What should you modify?

A. The referral ordering of the namespace
B. The staging quota of the replicated folder
C. The cache duration of the namespace
D. The schedule of the replication group

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Scheduling allows less bandwidth the by limiting the time interval of the replication
Does DFS Replication throttle bandwidth per schedule, per server, or per connection?
If you configure bandwidth throttling when specifying the schedule, all connections for that replication group will use that setting for bandwidth throttling. Bandwidth throttling can be also set as a connection-level setting using DFS Management.

To edit the schedule and bandwidth for a specific connection, use the following steps:

- In the console tree under the Replication node, select the appropriate replication group.
- Click the Connections tab, right-click the connection that you want to edit, and then click Properties.
- Click the Schedule tab, select Custom connection schedule and then click Edit Schedule.
- Use the Edit Schedule dialog box to control when replication occurs, as well as the maximum amount of bandwidth replication can consume.
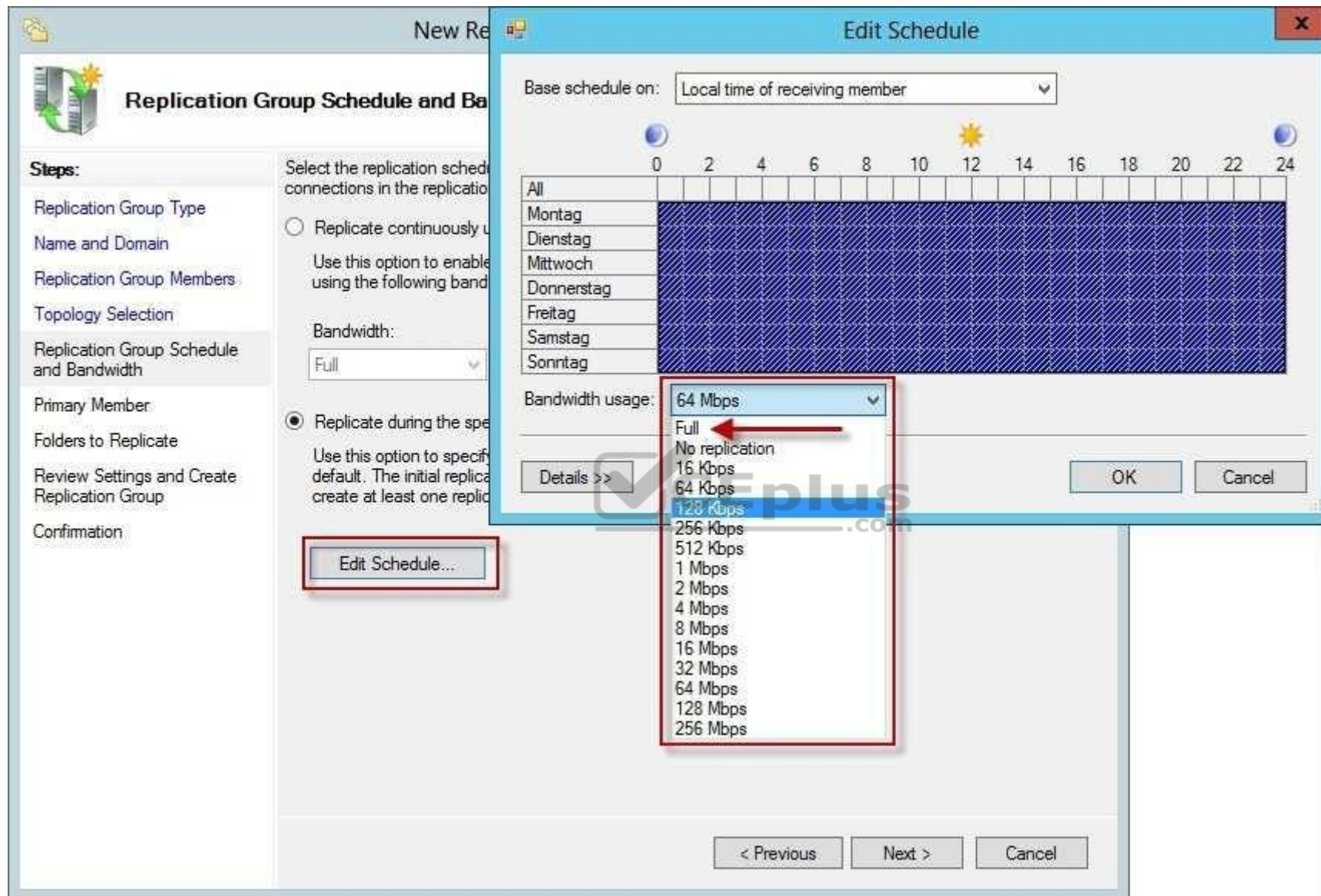
QUESTION 95
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. You plan to use fine-grained password policies to customize the password policy settings of contoso.com.

You need to identify to which Active Directory object types you can directly apply the fine-grained password policies.

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

A. Users
B. Global groups
C. computers
D. Universal groups
E. Domain local groups

Correct Answer: AB
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
First off, your domain functional level must be at Windows Server 2008. Second, Fine-grained password policies ONLY apply to user objects, and global security groups. Linking them to universal or domain local groups is ineffective. I know what you're thinking, what about OU's? Nope, Fine-grained password policy cannot be applied to an organizational unit (OU) directly. The third thing to keep in mind is, by default only members of the Domain Admins group can set fine- grained password policies. However, you can delegate this ability to other users if needed.

Fine-grained password policies apply only to user objects (or inetOrgPerson objects if they are used instead of user objects) and global security groups.

You can apply Password Settings objects (PSOs) to users or global security groups:

References:
http://technet.microsoft.com/en-us/library/cc731589%28v=ws.10%29.aspx http://technet.microsoft.com/en-us/library/cc770848%28v=ws.10%29.aspx http://www.brandonlawson.com/active-directory/creating-fine-grained-password-policies/

QUESTION 96
You have a cluster named Cluster1 that contains two nodes. Both nodes run Windows Server 2012 R2. Cluster1 hosts a virtual machine named VM1 that runs Windows Server 2012 R2.

You configure a custom service on VM1 named Service1.

You need to ensure that VM1 will be moved to a different node if Service1 fails.

Which cmdlet should you run on Cluster1?

A. Add-ClusterVmMonitoredItem
B. Add-ClusterGenericServiceRole
C. Set-ClusterResourceDependency
D. Enable VmResourceMetering

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
The Add-ClusterVMMonitoredItem cmdlet configures monitoring for a service or an Event Tracing for Windows (ETW) event so that it is monitored on a virtual machine. If the service fails or the event occurs, then the system responds by taking an action based on the failover configuration for the virtual machine resource. For example, the configuration might specify that the virtual machine be restarted.

QUESTION 97
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Server Update Services server role installed.

You need to configure Windows Server Update Services (WSUS) to support Secure Sockets Layer (SSL).

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

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

Correct Answer: BCE
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Certificate needs to be installed to IIS, Bindings modifies and wsusutil run.
  ▪ First we need to request a certificate for the WSUSweb site, so open IIS, click the server name, then open Server Certificates.On the Actions pane click Create
                                                                                            Domain Certificate.
  ▪ To add the signing certificate to the WSUS Web site in IIS 7.0On the WSUS server, open Internet Information Services(IIS) Manager. Expand Sites, right-click the WSUS Web site, and then click Edit Bindings. In the Site Binding dialog box, select the https binding, and click Edit to open the Edit Site Binding dialog box.Select the appropriate Web server certificate in the SSL certificate box, and then click OK. Click Close to exit the Site Bindings dialog box, and then click OK to close Internet Information Services (IIS) Manager.
  ▪ WSUSUtil.exe configure ssl<FQDN of the software update point site system> (the name in your certificate)WSUSUtil.exe configure ssl<Intranet FQDN of the software update point site system>.
  ▪ The next step is to point your clients to the correct url, by modifying the existing GPO or creating a new one. Open the policy Specify intranet Microsoft update service location and type the new url in the form https://YourWSUSserver.

The gpupdate /force command will just download all the GPO's and re-apply them to the client, it won't force the client to check for updates. For that you need to use wuauclt /resetautorization /detectnow followed by wuauclt /reportnow

References:
http://technet.microsoft.com/en-us/library/bb680861.aspx http://technet.microsoft.com/en-us/library/bb633246.aspx http://www.vkernel.ro/blog/configure-wsus-to-use-ssl

QUESTION 98
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

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
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

QUESTION 99
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.

How should you configure Service1 from the Services console on the virtual machine?

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

D. From the General settings, modify the Startup type.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Configure the virtual machine to take no action through Hyper-V if the physical computer shuts down by modifying the Automatic Stop Action setting to None.
Virtual machine state must be managed through the Failover Clustering feature.

Virtual machine application monitoring and management
In clusters running Windows Server 2012, administrators can monitor services on clustered virtual machines that are also running Windows Server 2012. This functionality extends the high-level monitoring of virtual machines that is implemented in Windows Server 2008 R2 failover clusters. If a monitored service in a virtual machine fails, the service can be restarted, or the clustered virtual machine can be restarted or moved to another node (depending on service restart settings and cluster failover settings).
This feature increases the uptime of high availability services that are running on virtual machines within a failover cluster.
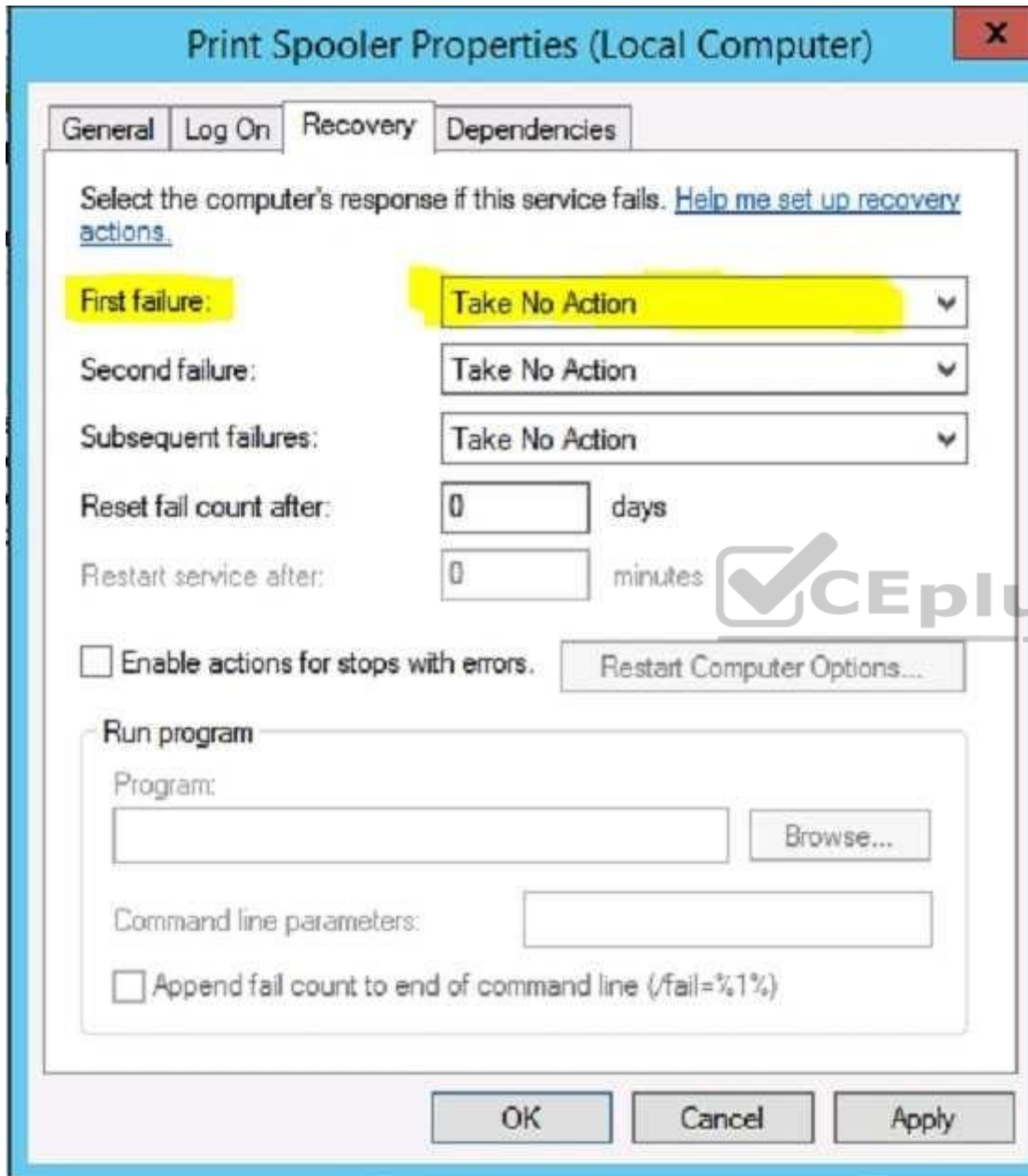
Windows Server 2012 Failover Cluster introduces a new capability for Hyper-V virtual machines (VMs), which is a basic monitoring of a service within the VM which causes the VM to be rebooted should the monitored service fail three times. For this feature to work the following must be configured:
▪ Both the Hyper-V servers must be Windows Server 2012 and the guest OS running in the VM must be Windows Server 2012.
▪ The host and guest OSs are in the same or at least trusting domains.
▪ The Failover Cluster administrator must be a member of the local administrator's group inside the VM.

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

Print Spooler Properties (Local Computer)

General | Log On | Recovery | Dependencies

Select the computer's response if this service fails. Help me set up recovery actions.

First failure: | Take No Action

Second failure: | Take No Action

Subsequent failures: | Take No Action

Reset fail count after: | 0 | days

Restart service after: | 0 | minutes

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

Run program

Program:

| | Browse... |

Command line parameters:

| |

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

OK | Cancel | Apply

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

After the above is true, enabling the monitoring is a simple process.

- Launch the Failover Cluster Manager tool.
- Navigate to the cluster - Roles.
- Right click on the virtual machine role you wish to enable monitoring for and under More
3. Actions select Configure Monitoring.
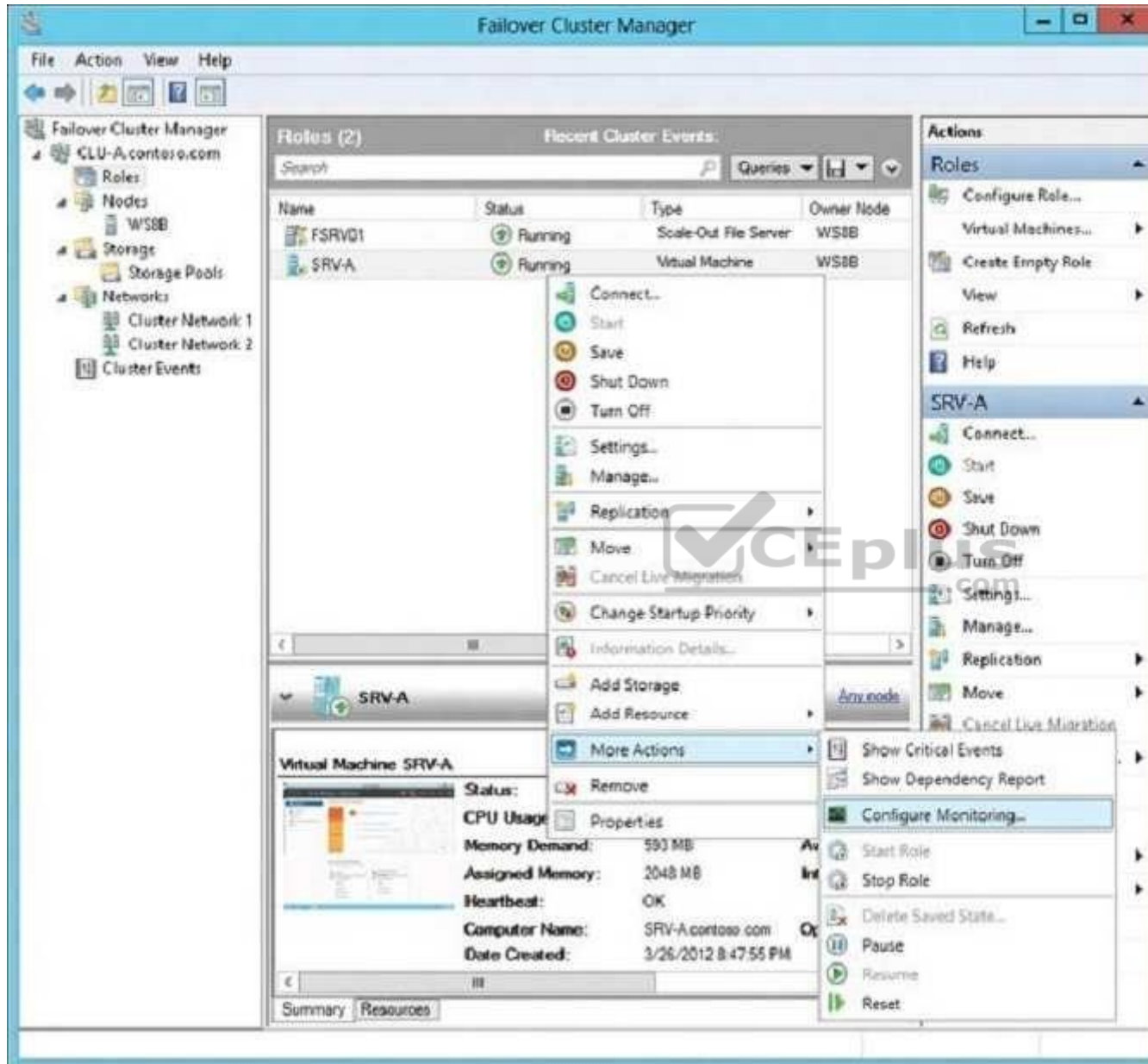
4. The services running inside the VM will be gathered and check the box for the services that 4.
should be monitored and click OK.
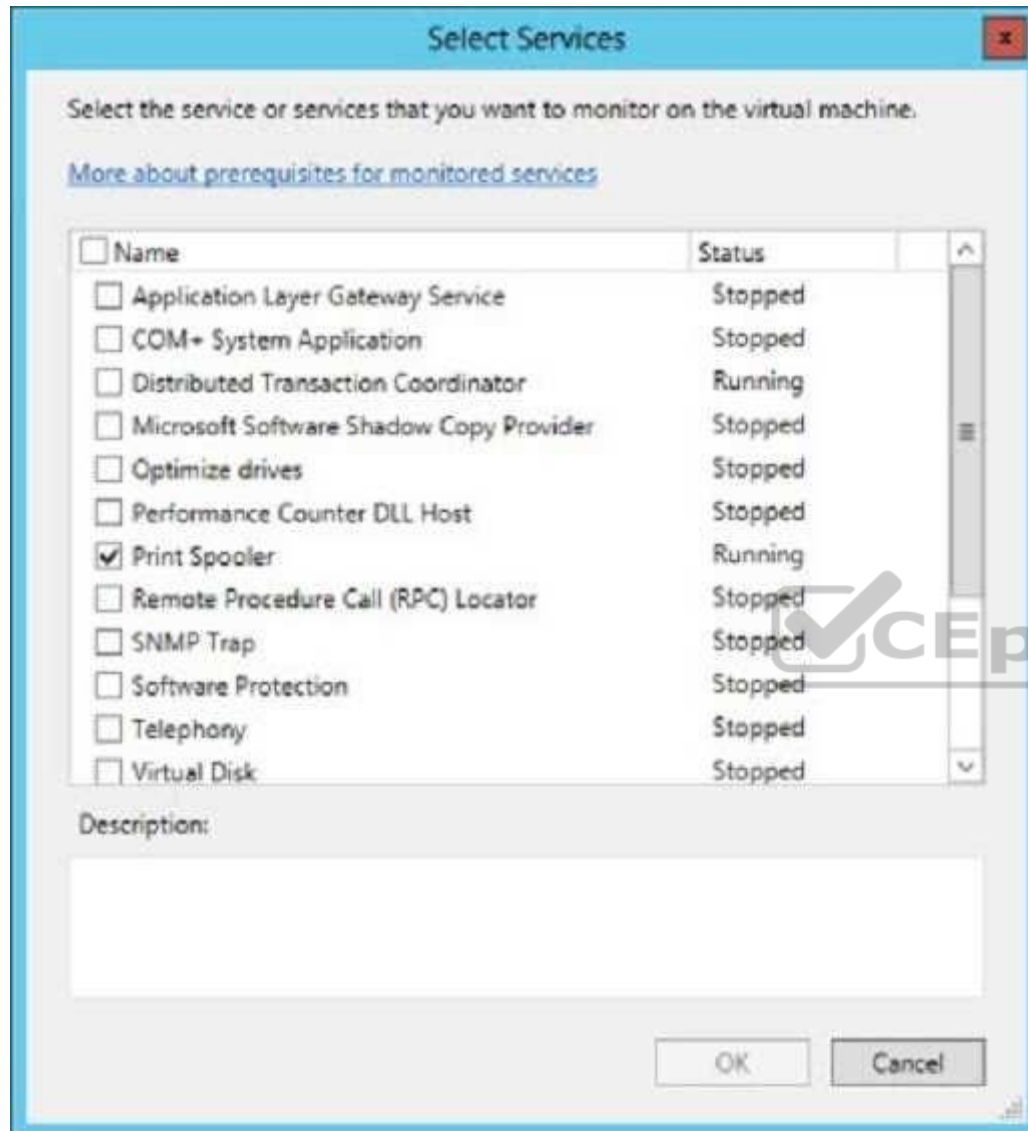
You are done!

Monitoring can also be enabled using the Add-ClusterVMMonitoredItem cmdlet and -VirtualMachine, with the -Service parameters, as the example below shows:
PS C:\Windows\system32> Add-ClusterVMMonitoredItem -VirtualMachine savdaltst01 -Service spooler

References: http://windowsitpro.com/windows-server-2012/enable-windows-server-2012-failover-cluster-hyper-v-vm-monitoring https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc742396(v=ws.11)

QUESTION 100
You have a DNS server named Server1 that runs Windows Server 2012 R2. On Server1, you create a DNS zone named contoso.com.

You need to specify the email address of the person responsible for the zone.

Which type of DNS record should you configure?

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

Correct Answer: A
Section: Volume B

Explanation

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

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

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

home.local
        primary name server = dc1.home.local
        responsible mail addr = hostmaster.home.local
        serial  = 292
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 300 (5 mins)
        default TTL = 1200 (20 mins)
dc1.home.local  internet address = 192.168.1.10
```

QUESTION 101
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. All of the DNS servers in both of the domains run Windows Server 2012 R2.

The network contains two servers named Server1 and Server2. Server1 hosts an Active Directory- integrated zone for contoso.com. Server2 hosts an Active Directory-integrated zone for fabrikam.com. Server1 and Server2 connect to each other by using a WAN link.

Client computers that connect to Server1 for name resolution cannot resolve names in fabrikam.com.

You need to configure Server1 to resolve names in fabrikam.com. The solution must NOT require that changes be made to the fabrikam.com zone on Server2.

What should you create?

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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

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

QUESTION 102
Your network is configured as shown in the exhibit. (Click the Exhibit button.)
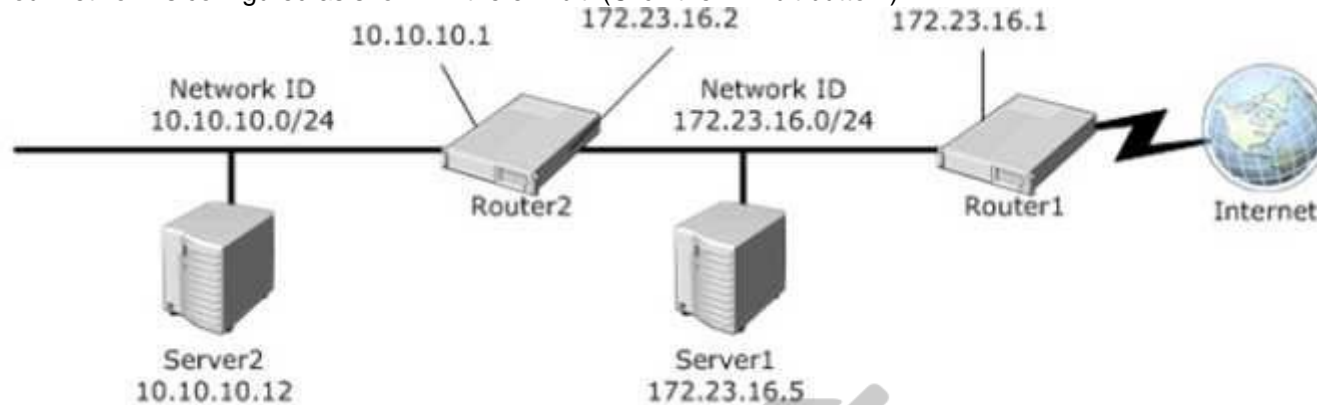
Server1 regularly accesses Server2.

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

You need to optimize the connection path from Server1 to Server2.

Which route command should you run on Server1?

A. Route add -p 10.10.10.0 MASK 255.255.255.0172.23.16.2 METRIC 100
B. Route add -p 10.10.10.0 MASK 255.255.255.0 10.10.10.1 METRIC 50
C. Route add -p 10.10.10.12 MASK 255.255.255.0 10.10.10.1 METRIC 100
D. Route add -p10.10.10.12 MASK 255.255.255.0 10.10.10.0 METRIC 50

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

Destination - specifies either an IP address or host name for the network or host.

subnetmask - specifies a subnet mask to be associated with this route entry. If subnetmask is not specified, 255.255.255.255 is used.

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

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

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

References:
http://support.microsoft.com/kb/299540/en-us http://technet.microsoft.com/en-us/library/cc757323%28v=ws.10%29.aspx

QUESTION 103
Your network contains an Active Directory domain named adatum.com.
You have a standard primary zone named adatum.com.
You need to provide a user named User1 the ability to modify records in the zone. Other users must be prevented from modifying records in the zone.

What should you do first?

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

Correct Answer: C
Section: Volume B
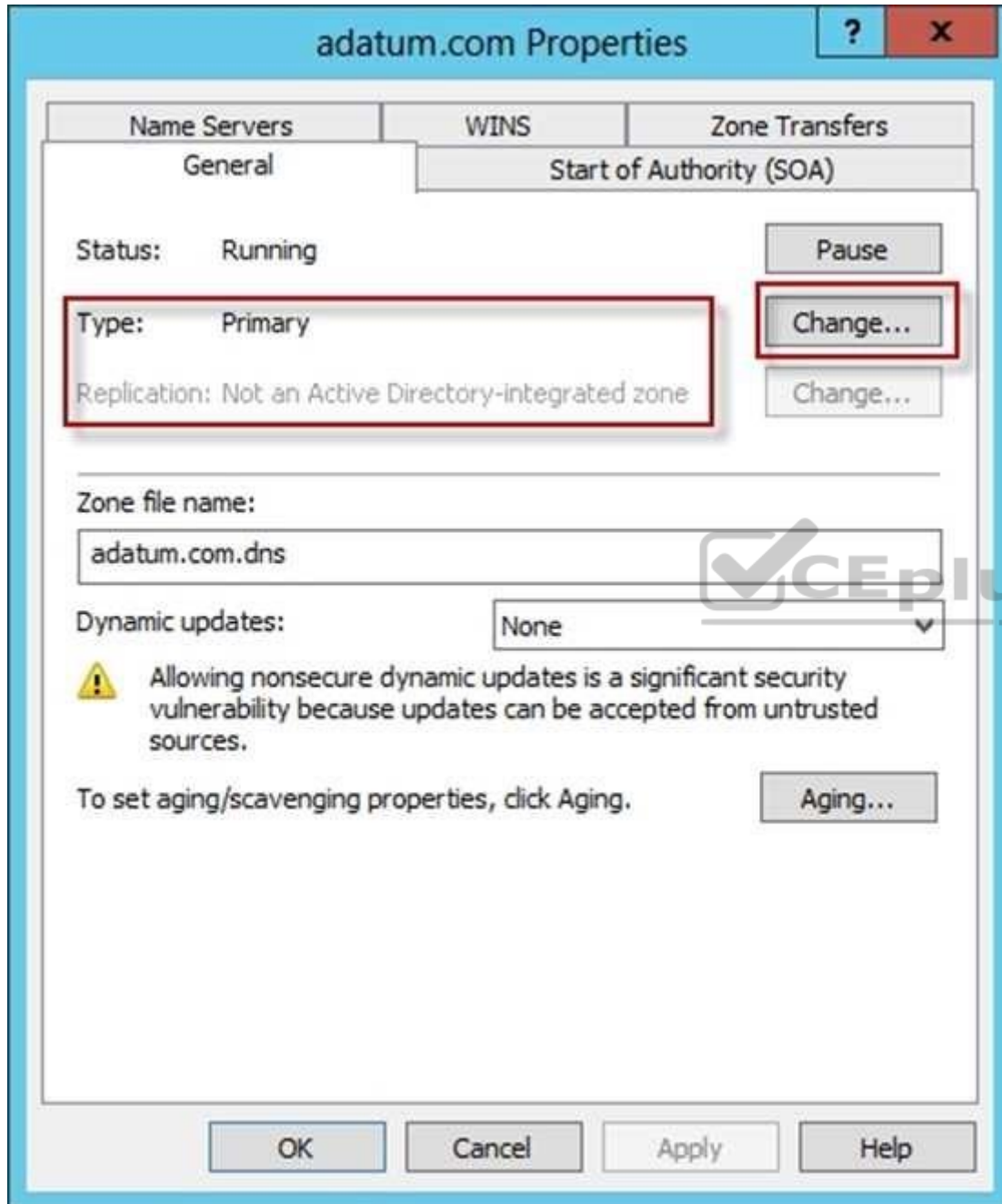
Explanation

Explanation/Reference:
Explanation:
The Zone would need to be changed to a AD integrated zone When you use directory-integrated zones, you can use access control list (ACL) editing to secure a dnsZone object container in the directory tree. This feature provides detailed access to either the zone or a specified resource record in the zone. For example, an ACL for a zone resource record can be restricted so that dynamic updates are allowed only for a specified client computer or a secure group, such as a domain administrators group. This security feature is not available with standard primary zones.

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

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

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

Now there's Security tab:

http://technet.microsoft.com/en-us/library/cc753014.aspx http://technet.microsoft.com/en-us/library/cc726034.aspx

QUESTION 104

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 Management. Link GPO1 to the Domain Controllers organizational unit (OU).
B. In GPO1, configure the Advanced Audit Policy Configuration settings for Audit User Account Management. Move the member servers to a new organizational unit (OU). Link GPO1 to the new OU.
C. In GPO1, configure the Advanced Audit Policy Configuration settings for Audit Sensitive Privilege Use. Link GPO1 to the Domain Controllers organizational unit (OU).
D. In GPO1, configure the Advanced Audit Policy Configuration settings for Audit Sensitive Privilege Use. Move the member servers to a new organizational unit (OU). Link GPO1 to the new OU.

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
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.

QUESTION 105

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

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

85% Threshold Properties

Generate notifications when usage reaches (%):

85

E-mail Message | Event Log | Command | Report

☑ Send e-mail to the following administrators:

[Admin Email]

Format: account@domain. Use semicolons to separate accounts.

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

E-mail message

Type the text to use for the Subject line and message.

To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.

Subject:

[Quota Threshold]% quota threshold exceeded

Message body:

User [Source Io Owner] has exceed the [Quota Threshold]% quota threshold for quota on [Quota Path] on server [Server]. The quota limit is [Quota Limit MB] MB and the current usage is [Quota Used MB] MB ([Quota Used Percent]% of limit).

Select variable to insert:

[Admin Email] ▼   Insert Variable

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

You need to ensure that a user named User1 receives an email notification when the threshold is exceeded.

What should you do?

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

Correct Answer: D
Section: Volume B
Explanation

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

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

To configure e-mail options
In the console tree, right-click File Server Resource Manager, and then click Configure options. The File Server Resource Manager Options dialog box opens.
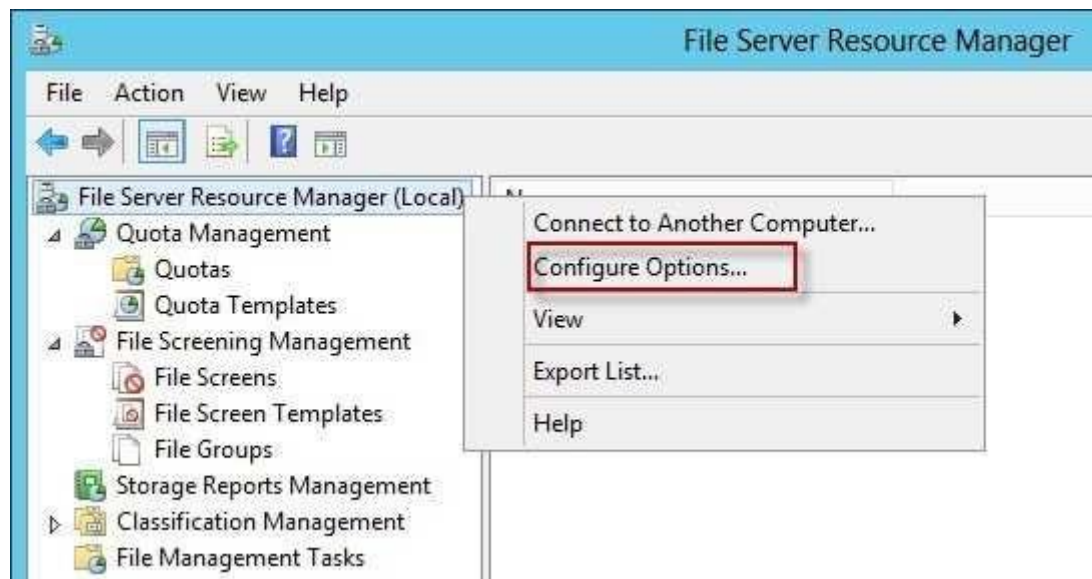
On the E-mail Notifications tab, under SMTP server name or IP address, type the host name or the IP address of the SMTP server that will forward e-mail notifications.

If you want to routinely notify certain administrators of quota or file screening events, under Default administrator recipients, type each e-mail address.

Use the format account@domain. Use semicolons to separate multiple accounts.
To test your settings, click Send Test E-mail.
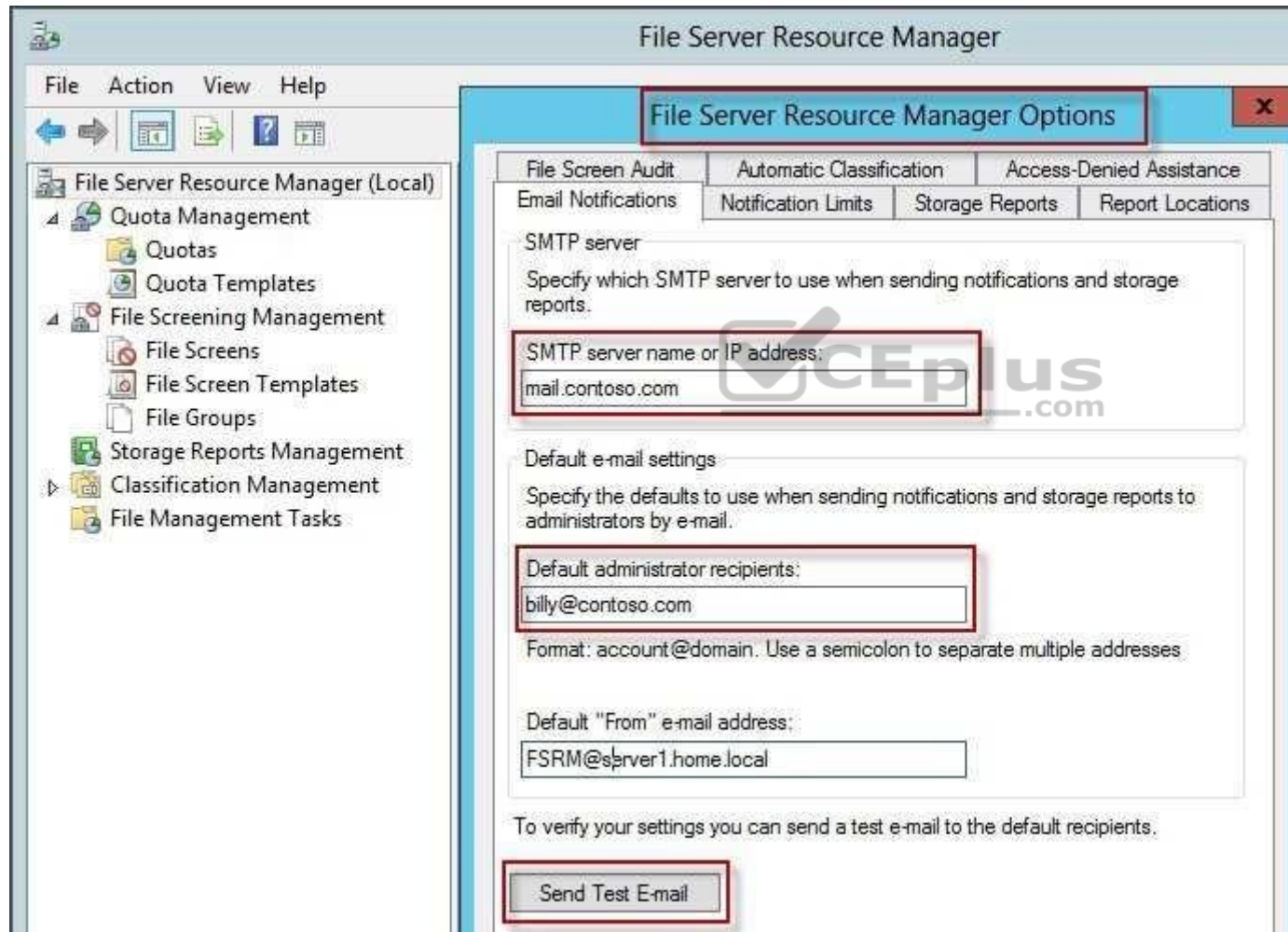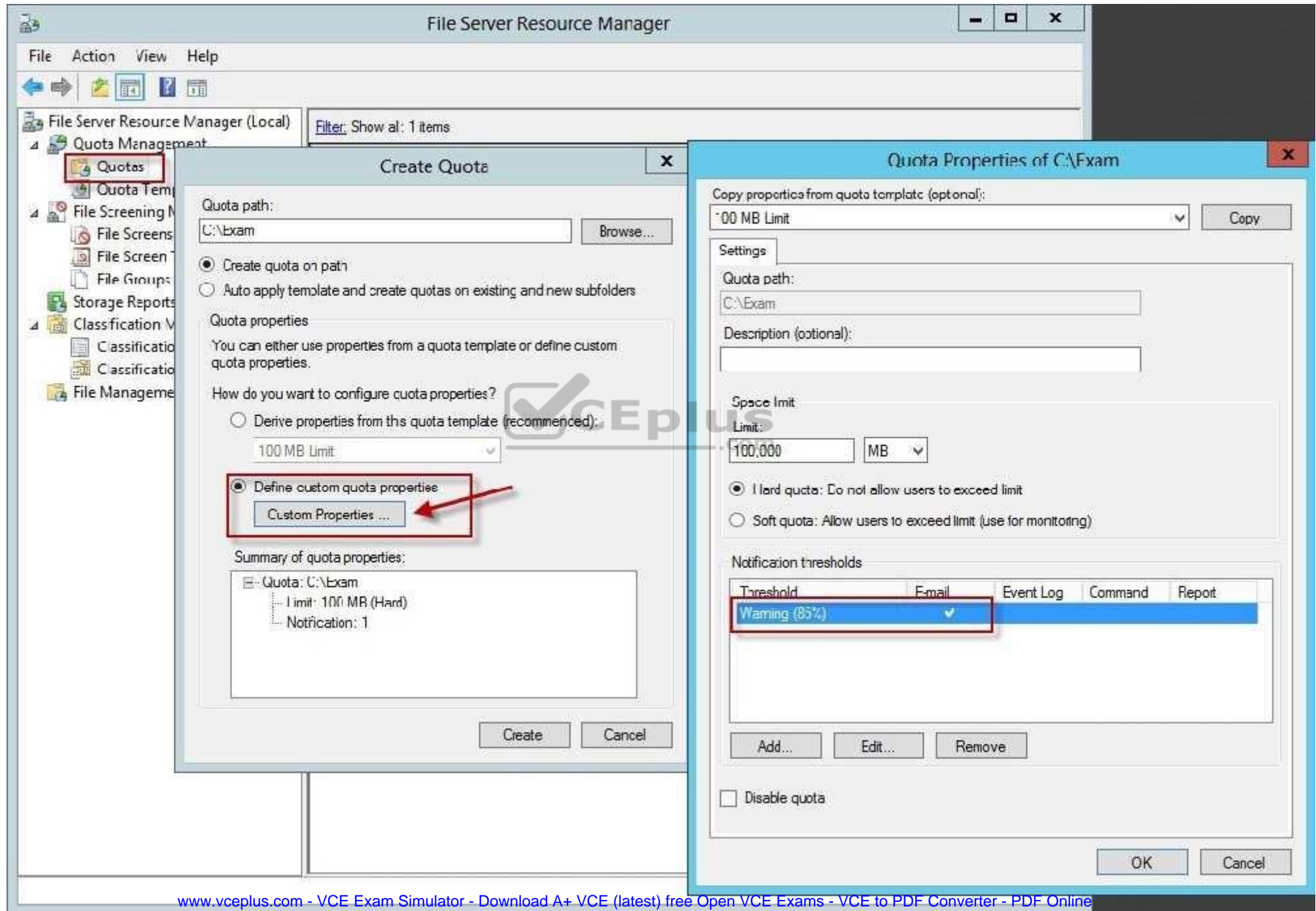
QUESTION 106

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 \\adatum.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.

Correct Answer: BCE
Section: Volume B
Explanation

Explanation/Reference:
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, rightclick 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
▪ 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.

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

Reference:
http://technet.microsoft.com/en-us/library/cc731531.aspx http://technet.microsoft.com/en-us/library/cc772778%28v=ws.10%29.aspx http://technet.microsoft.com/en-us/library/cc732414.aspx
http://technet.microsoft.com/en-us/library/cc772379.aspx http://technet.microsoft.com/en-us/library/cc732863%28v=ws.10%29.aspx http://technet.microsoft.com/en-us/library/cc725830.aspx
http://technet.microsoft.com/en-us/library/cc771978.aspx
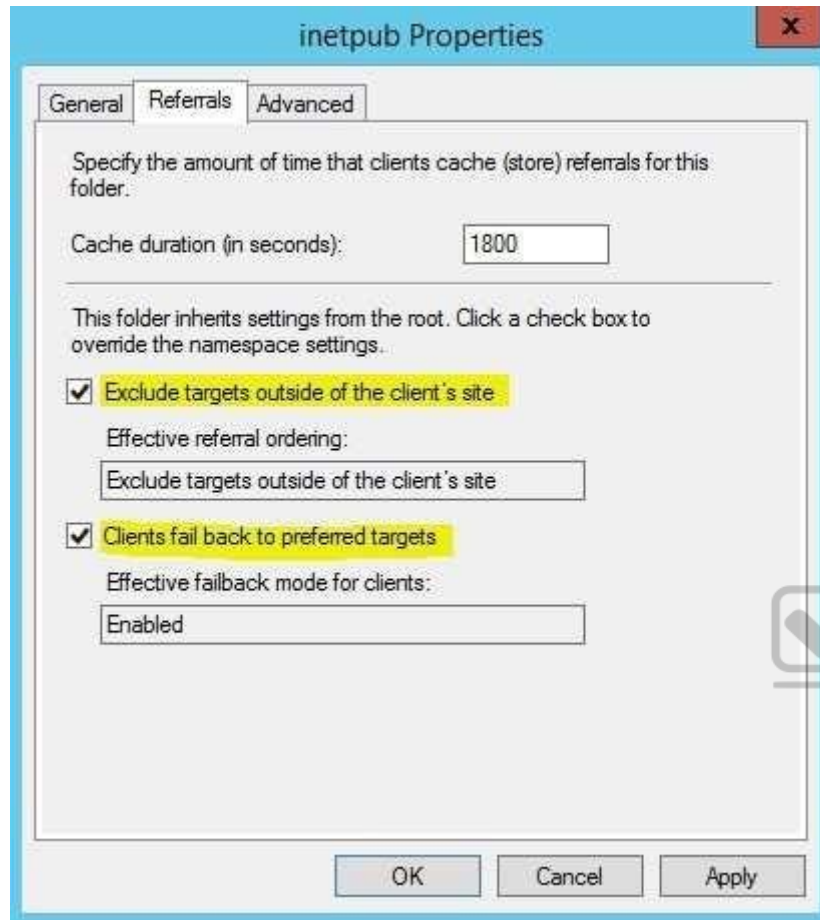
QUESTION 107
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.

Server1 has a folder named Folder1 that is used by the sales department.

You need to ensure that an email notification is sent to the sales manager when a File Screening Audit report is generated.

What should you configure on Server1?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
From the Storage Reports Management node, you can generate reports that will help you understand file use on the storage server. You can use the storage reports to monitor disk usage patterns (by file type or user), identify duplicate files and dormant files, track quota usage, and audit file screening.
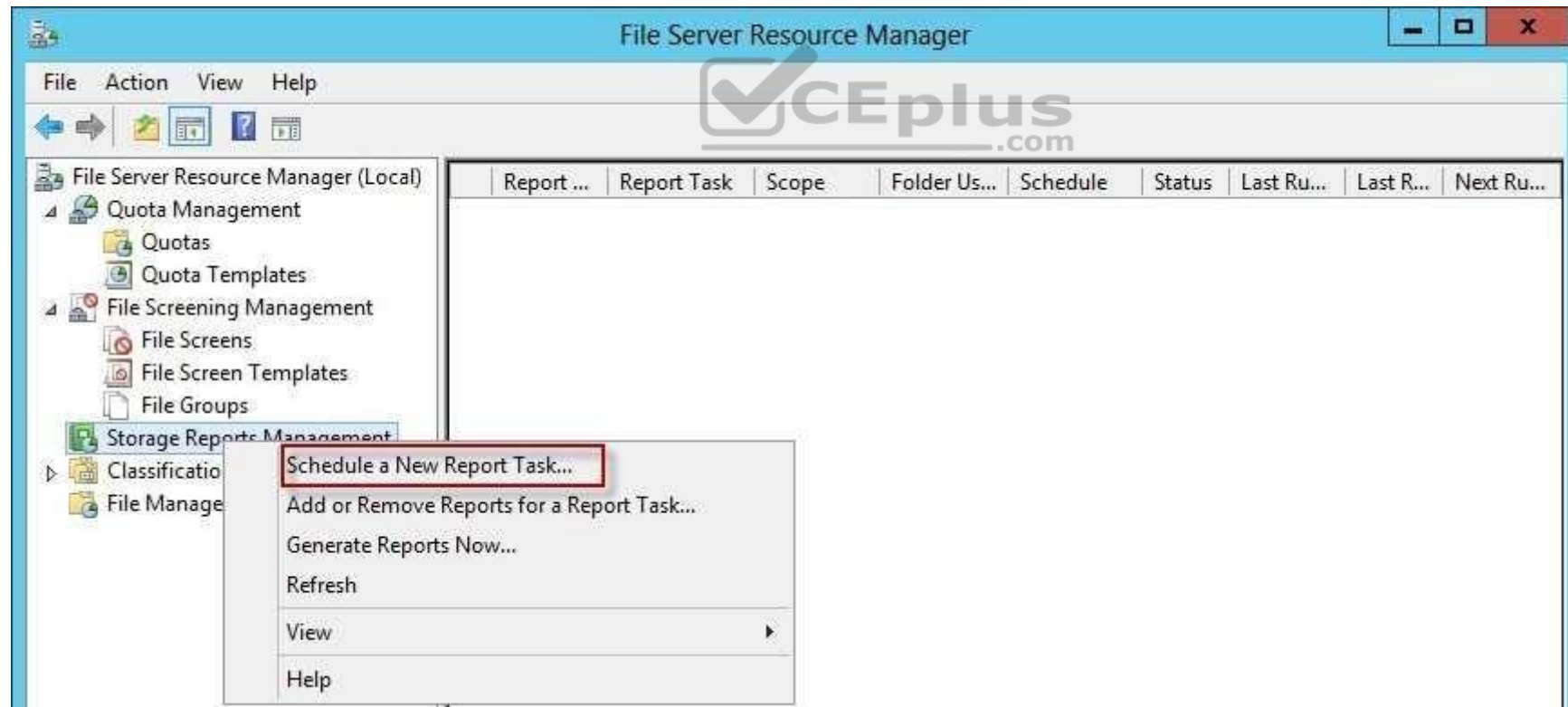
Before you run a File Screen Audit report, in the File Server Resource Manager Options dialog box, on the File Screen Audit tab, verify that the Record file screening activity in the auditing database check box is selected.

Reference:
http://technet.microsoft.com/en-us/library/cc755988.aspx http://technet.microsoft.com/en-us/library/cc730822.aspx http://technet.microsoft.com/en-us/library/cc770594.aspx
http://technet.microsoft.com/en-us/library/cc771212.aspx http://technet.microsoft.com/en-us/library/cc732074.aspx

QUESTION 108
Your network contains an Active Directory domain named adatum.com. The domain contains 10 domain controllers that run Windows Server 2012 R2.

You plan to create a new Active Directory-integrated zone named contoso.com.

You need to ensure that the new zone will be replicated to only four of the domain controllers.

What should you do first?

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

Correct Answer: A
Section: Volume B

Explanation

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

QUESTION 109
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has the Remote Access server role installed.

DirectAccess is implemented on Server1 by using the default configuration.

You discover that DirectAccess clients do not use DirectAccess when accessing websites on the Internet.

You need to ensure that DirectAccess clients access all Internet websites by using their DirectAccess connection.

What should you do?

A. Configure a DNS suffix search list on the DirectAccess clients.
B. Configure DirectAccess to enable force tunneling.
C. Disable the DirectAccess Passive Mode policy setting in the DirectAccess Client Settings Group Policy object (GPO).
D. Enable the Route all traffic through the internal network policy setting in the DirectAccess Server Settings Group Policy object (GPO).

Correct Answer: B
Section: Volume B
Explanation
Explanation/Reference:
Explanation:
With IPv6 and the Name Resolution Policy Table (NRPT), by default, DirectAccess clients separate their intranet and Internet traffic as follows:
▪ DNS name queries for intranet fully qualified domain names (FQDNs) and all intranet traffic is exchanged over the tunnels that are created with the DirectAccess server or directly with intranet servers. Intranet traffic from DirectAccess clients is IPv6 traffic.
▪ DNS name queries for FQDNs that correspond to exemption rules or do not match the intranet namespace, and all traffic to Internet servers, is exchanged over the physical interface that is connected to the Internet. Internet traffic from DirectAccess clients is typically IPv4 traffic.
In contrast, by default, some remote access virtual private network (VPN) implementations, including the VPN client, send all intranet and Internet traffic over the remote access VPN connection. Internet-bound traffic is routed by the VPN server to intranet IPv4 web proxy servers for access to IPv4 Internet resources. It is possible to separate the intranet and Internet traffic for remote access VPN clients by using split tunneling. This involves configuring the Internet Protocol (IP) routing table on VPN clients so that traffic to intranet locations is sent over the VPN connection, and traffic to all other locations is sent by using the physical interface that is connected to the Internet.
You can configure DirectAccess clients to send all of their traffic through the tunnels to the DirectAccess server with force tunneling. When force tunneling is configured, DirectAccess clients detect that they are on the Internet, and they remove their IPv4 default route. With the exception of local subnet traffic, all traffic sent by the DirectAccess client is IPv6 traffic that goes through tunnels to the DirectAccess server.

QUESTION 110
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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
To create DNS Host (A) Records for all internal pool servers
▪ Click Start, click All Programs, click Administrative Tools, and then click DNS.
▪ In DNS Manager, click the DNS Server that manages your records to expand it.
▪ Click Forward Lookup Zones to expand it.
▪ Right-click the DNS domain that you need to add records to, and then click New Host (A or AAAA).
▪ In the Name box, type the name of the host record (the domain name will be automatically appended).
▪ 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.
▪ 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

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

QUESTION 111
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

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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
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).

QUESTION 112
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

Administrators use client computers that run Windows 8.1 to perform all management tasks.
A central store is configured on a domain controller named DC1.

You have a custom administrative template file named App1.admx. App1.admx contains application settings for an application named Appl.

From a client computer named Computer1, you create a new Group Policy object (GPO) named GPO1.

You discover that the application settings for App1 fail to appear in GPO1.

You need to ensure that the App1 settings appear in all of the new GPOs that you create.

What should you do?

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

Correct Answer: B
Section: Volume B
Explanation

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

QUESTION 113
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Server Update Services server role installed.

Server1 stores update files locally in C:\Updates.

You need to change the location in which the update files are stored to D:\Updates.

What should you do?

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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
You might need to change the location where WSUS stores updates locally. This might be required if the disk becomes full and there is no longer any room for new updates. You might also have to do this if the disk where updates are stored fails and the replacement disk uses a new drive letter.
You accomplish this move with the movecontent command of WSUSutil.exe, a command-line tool that is copied to the file system of the WSUS server during WSUS Setup. By default, Setup copies WSUSutil.exe to the following location:
WSUSInstallationDrive:\Program Files\Microsoft Windows Server Update Services\Tools\

QUESTION 114
You have a server named Server1 that runs Windows Server 2012 R2.

You create a custom Data Collector Set (DCS) named DCS1.

You need to configure Server1 to start DCS1 automatically when the network usage exceeds 70 percent.

Which type of data collector should you create?

A. A performance counter alert
B. A configuration data collector

C. A performance counter data collector

D. An event trace data collector

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
Performance alerts notify you when a specified performance counter exceeds your configured threshold by logging an event to the event log. But rather than notifying you immediately when the counter exceeds the threshold, you can configure a time period over which the counter needs to exceed the threshold, to avoid unnecessary alerts.

Performance Monitoring Details

General | Alert | History & Trending

☑ Enable Event Log Alert with severity [Warning ▾]

Alert if value is [more than ▾]

[15000 ▴▾] for [10 ▴▾] [minute(s) ▾]

☑ Notify at most once every [1 ▴▾] [hour(s) ▾]

☑ Embed chart with email alerts

☐ Enable Trend Detection

Detect Leaks:

[mild (few false positives) ▾]

Min: 0 , Max: 0 , Last: 0

[OK] [Cancel] [Help]

QUESTION 115
Your network contains an Active Directory domain named contoso.com. The domain contains a RADIUS server named Server1 that runs Windows Server 2012 R2.

You add a VPN server named Server2 to the network.

On Server1, you create several network policies.

You need to configure Server1 to accept authentication requests from Server2.

Which tool should you use on Server1?

A. Server Manager
B. Add-RemoteAccessRadius
C. New-NpsRadiusClient
D. Connection Manager Administration Kit (CMAK)

Correct Answer: C
Section: Volume B

Explanation

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

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


Name                 : FromServer2
Address              : 10.1.0.0/16
AuthAttributeRequired : False
NapCompatible        : False
SharedSecret         : 123
VendorName           : RADIUS Standard
Enabled              : True
```

New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:

FromServer2

Address (IP or DNS):

10.1.0.0/16   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

Reference: http://technet.microsoft.com/en-us/library/hh918425(v=wps.620).aspx http://technet.microsoft.com/en-us/library/jj872740(v=wps.620).aspx http://technet.microsoft.com/en-us/library/dd469790.aspx

QUESTION 116

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

You need to allow connections that use 802.1x.

What should you create?

A. A network policy that uses Microsoft Protected EAP (PEAP) authentication
B. A network policy that uses EAP-MSCHAP v2 authentication
C. A connection request policy that uses EAP-MSCHAP v2 authentication
D. A connection request policy that uses MS-CHAP v2 authentication

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
802.1X uses EAP, EAP-TLS, EAP-MS-CHAP v2, and PEAP authentication methods:
▪ EAP (Extensible Authentication Protocol) uses an arbitrary authentication method, such as certificates, smart cards, or credentials.
▪ EAP-TLS (EAP-Transport Layer Security) is an EAP type that is used in certificate- based security environments, and it provides the strongest authentication and key determination method.
▪ EAP-MS-CHAP v2 (EAP-Microsoft Challenge Handshake Authentication Protocol version 2) is a mutual authentication method that supports password-based user or computer authentication.
▪ PEAP (Protected EAP) is an authentication method that uses TLS to enhance the security of other EAP authentication protocols.

Connection request policies are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User Service (RADIUS) servers perform the authentication and authorization of connection requests that the server running Network Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS servers are used for RADIUS accounting.
With connection request policies, you can use NPS as a RADIUS server or as a RADIUS proxy, based on factors such as the following: ▪
The time of day and day of the week
▪ The realm name in the connection request
▪ The type of connection being requested
▪ The IP address of the RADIUS client

QUESTION 117
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy Server role service installed.

You plan to configure Server1 as a Network Access Protection (NAP) health policy server for VPN enforcement by using the Configure NAP wizard.

You need to ensure that you can configure the VPN enforcement method on Server1 successfully.

What should you install on Server1 before you run the Configure NAP wizard?

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

Correct Answer: C
Section: Volume B

Explanation

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

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

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

QUESTION 118
DRAG DROP
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed.

All of the VPN servers on your network use Server1 for RADIUS authentication.

You create a security group named Group1.

You need to configure Network Policy and Access Services (NPAS) to meet the following requirements:
▪ Ensure that only the members of Group1 can establish a VPN connection to the VPN servers.
▪ Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later.

Which type of policy should you create for each requirement?
To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Policy Types

| Connection Request Policies |
| Health Policies |
| Network Policies |

Answer Area

Ensure that only the members of Group1 can establish a VPN connection to the VPN servers. | Policy type |

Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later | Policy type |

Select and Place:

Correct Answer:

Policy Types

| Connection Request Policies |

| Health Policies |

| Network Policies |

Answer Area

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

| Network Policies |

Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later

| Network Policies |

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 119
HOTSPOT
Your company has four offices. The offices are located in Montreal, Seattle, Sydney, and New York.

The network contains an Active Directory domain named contoso.com. The domain contains a server named Server2 that runs Windows Server 2012 R2. Server2 has the DHCP Server server role installed.

All client computers obtain their IPv4 and IPv6 addresses from DHCP.

You need to ensure that Network Access Protection (NAP) enforcement for DHCP applies to all of the client computers except for the client computers in the New York office.

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

Hot Area:

DHCP

File   Action   View   Help

DHCP	Contents of DHCP	Status
▲ ▤ server2.contoso.com	▤ server2.contoso.com	
▲ ▤ IPv4		
▷ ▤ Scope [192.168.0.0] Contoso NewYork		
▷ ▤ Scope [192.168.1.0] Contoso Montreal		
▷ ▤ Scope [192.168.2.0] Contoso Seattle		
▷ ▤ Scope [192.168.3.0] Contoso Sydney		
▤ Server Options		
▤ Policies		
▷ ▤ Filters		
▲ ▤ IPv6		
▷ ▤ Scope [fddd:eef8:223b:ea3f::] Contoso New York		
▷ ▤ Scope [fddd:eef8:223b:ea4f::] Contoso Montreal		
▷ ▤ Scope [fddd:eef8:223b:ea5f::] Contoso Seattle		
▷ ▤ Scope [fddd:eef8:223b:ea6f::] Contoso Sydney		
▤ Server Options		

Correct Answer:
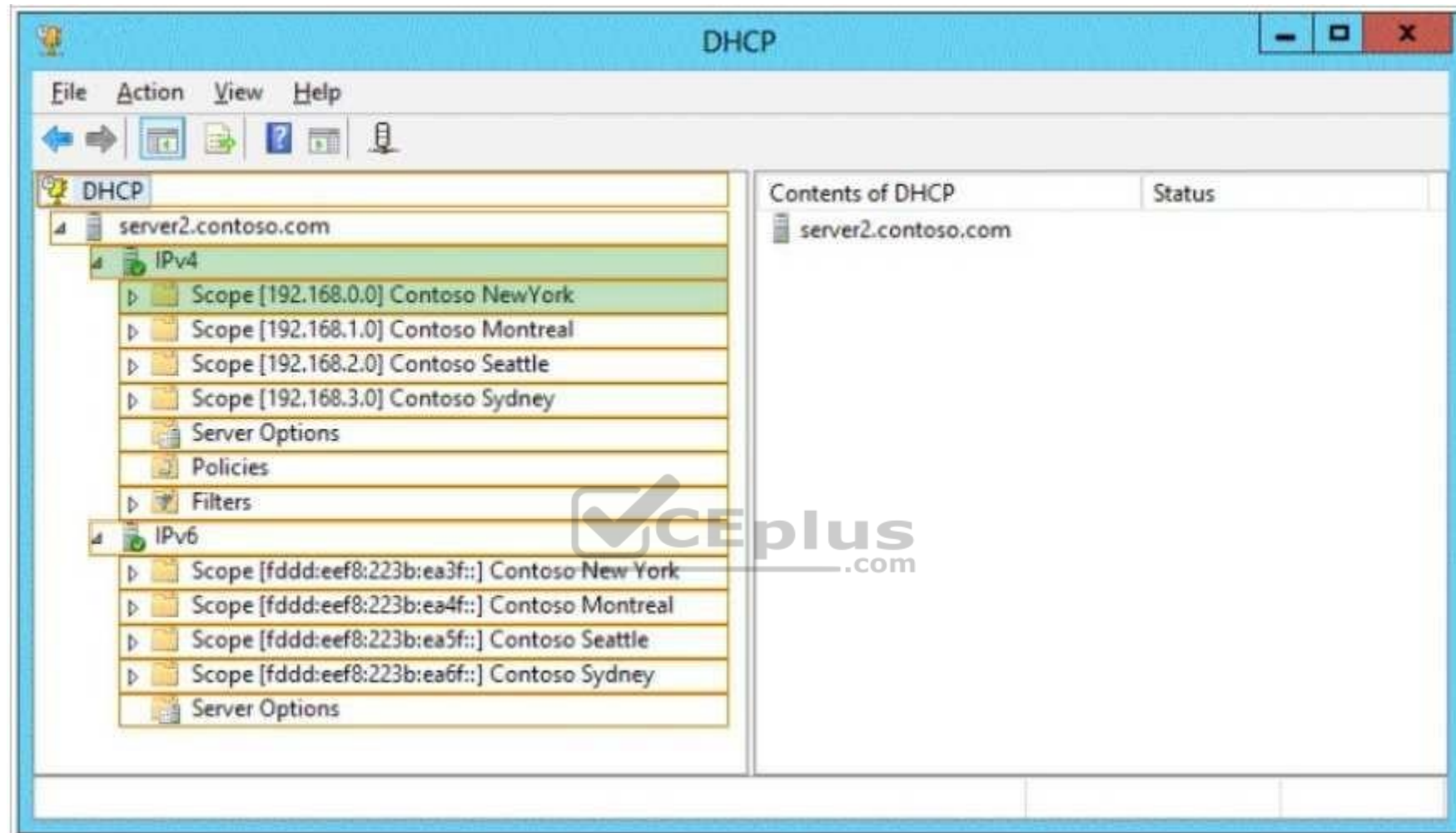
Section: Volume B
Explanation

Explanation/Reference:
QUESTION 120
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.

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
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:
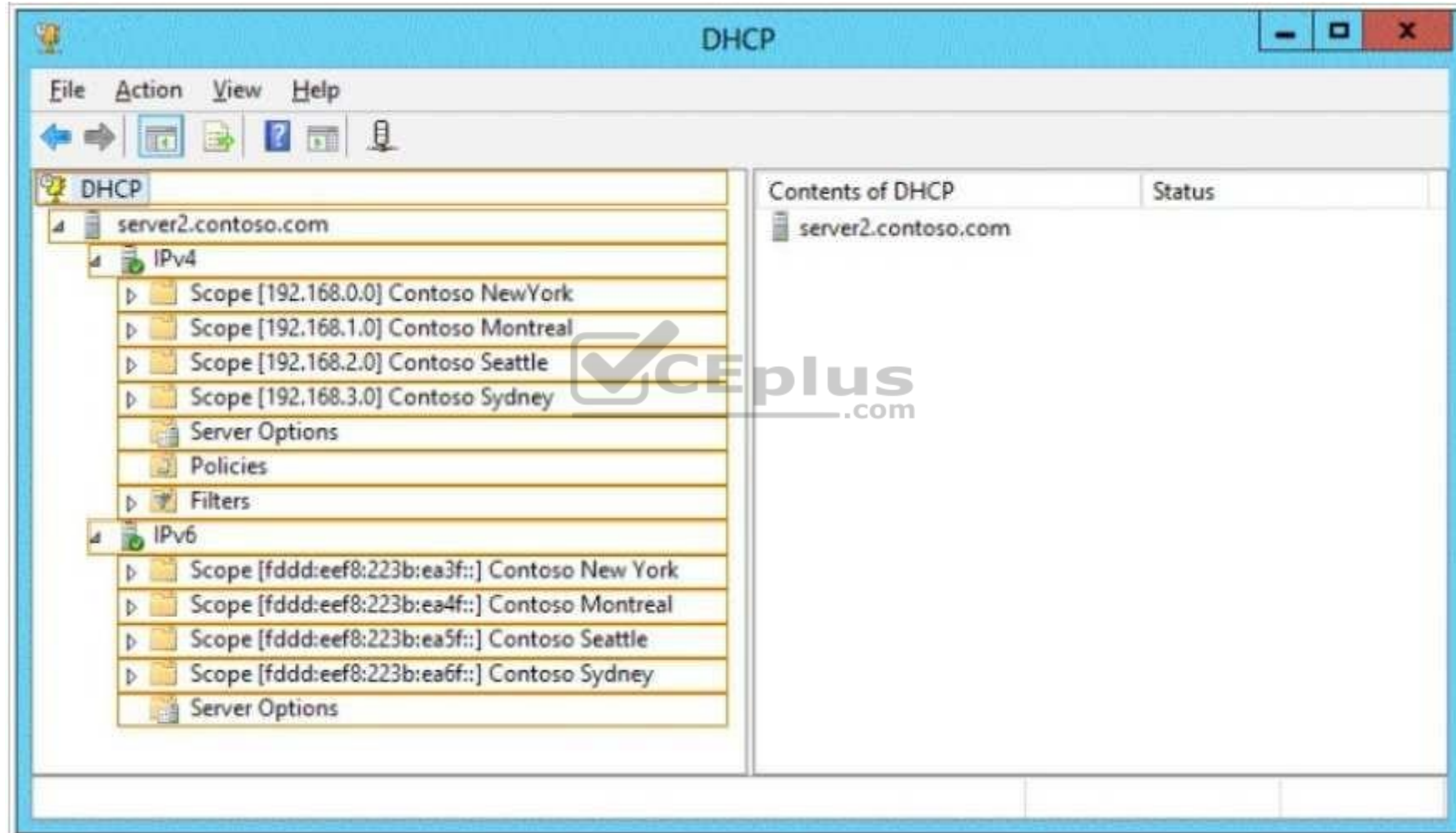http://technet.microsoft.com/en-us/library/cc708431.aspx
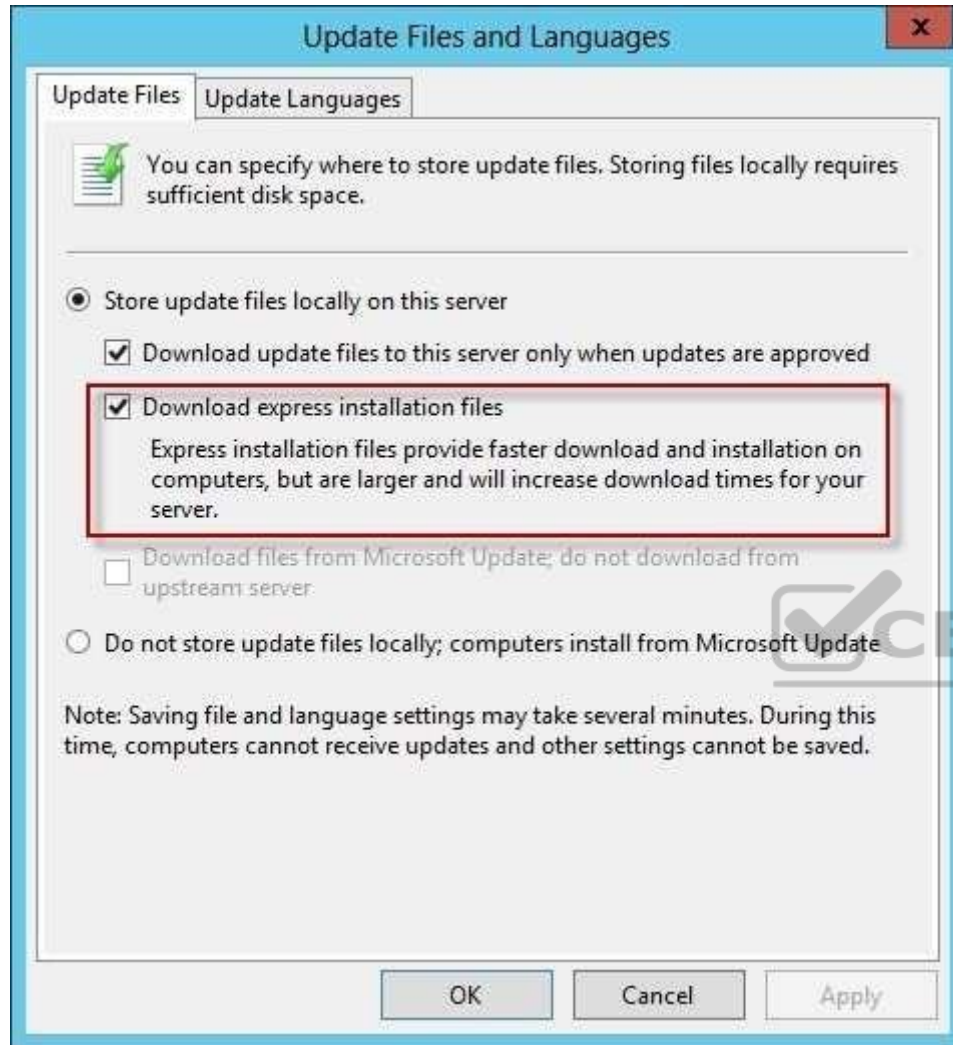
QUESTION 121
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the Network Policy Server role service installed.

You need to enable trace logging for Network Policy Server (NPS) on Server1.
Which tool should you use?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
NPS trace logging files
You can use log files on servers running Network Policy Server (NPS) and NAP client computers to help troubleshoot NAP problems. Log files can provide the detailed information required for troubleshooting complex problems.

You can capture detailed information in log files on servers running NPS by enabling remote access tracing. The Remote Access service does not need to be installed or running to use remote access tracing. When you enable tracing on a server running NPS, several log files are created in %windir %\tracing.

The following log files contain helpful information about NAP:
▪ IASNAP. LOG: Contains detailed information about NAP processes, NPS authentication, and NPS authorization. ▪
IASSAM. LOG: Contains detailed information about user authentication and authorization.

Membership in the local Administrators group, or equivalent, is the minimum required to enable tracing. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups (http://go.microsoft.com/fwlink/?LinkId=83477).

To create tracing log files on a server running NPS

▪ Open a command line as an administrator.
▪ Type netshras set tr * en.
▪ Reproduce the scenario that you are troubleshooting.
▪ Type netshras set tr * dis.
▪ Close the command prompt window.

Reference: http://technet.microsoft.com/en-us/library/dd348461%28v=ws.10%29.aspx

QUESTION 122

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 has the DHCP Server server role and the Network Policy Server role service installed.

Server1 contains three non-overlapping scopes named Scope1, Scope2, and Scope3. Server1 currently provides the same Network Access Protection (NAP) settings to the three scopes.

You modify the settings of Scope1 as shown in the exhibit. (Click the Exhibit button.)
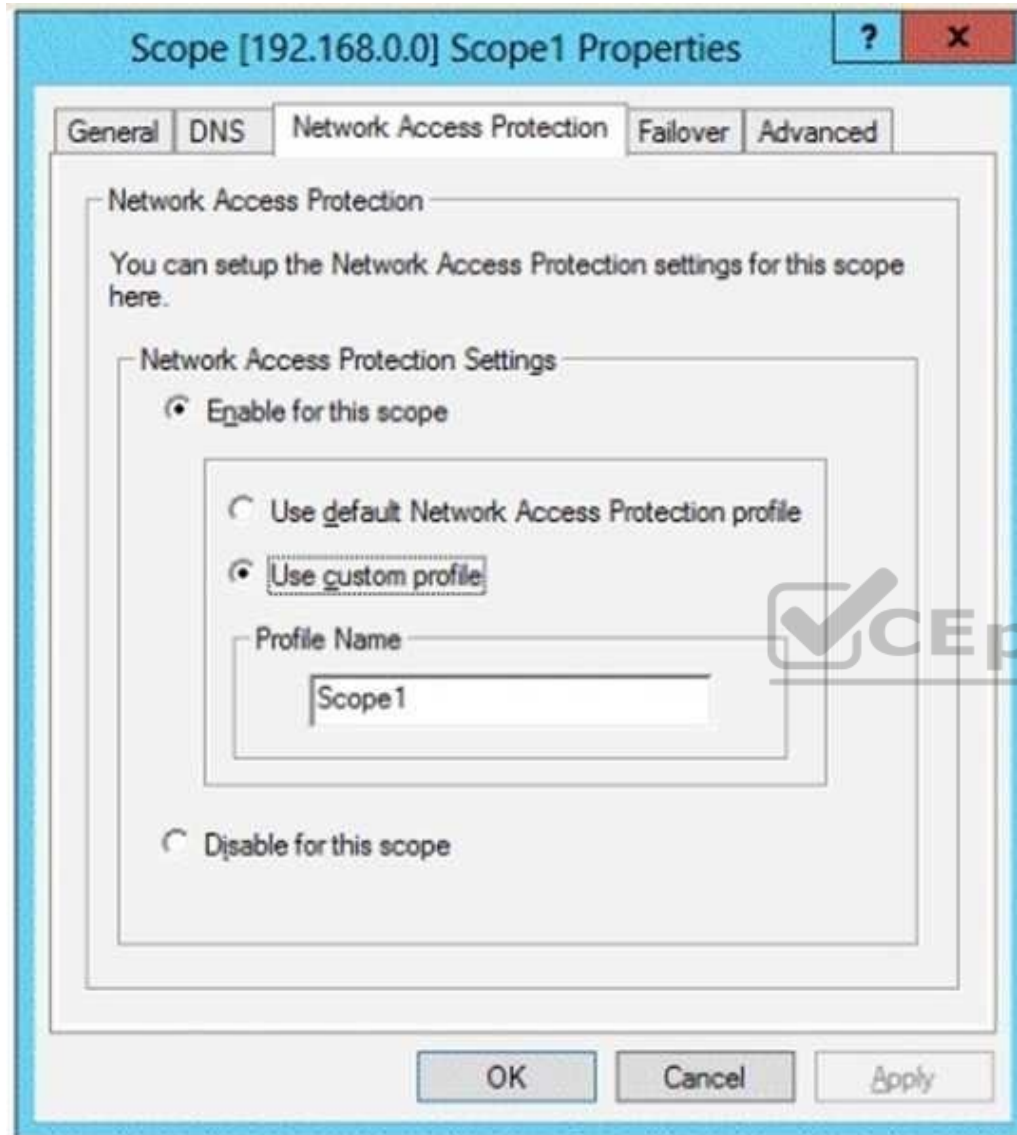
You need to configure Server1 to provide unique NAP enforcement settings to the NAP non- compliant DHCP clients from Scope1.

What should you create?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
MS-Service Class
Restricts the policy to clients that have received an IP address from a DHCP scope that matches the specified DHCP profile name. This condition is used only when you are deploying NAP with the DHCP enforcement method. To use the MS-Service Class attribute, in Specify the profile name that identifies your DHCP scope, type the name of an existing DHCP profile.

Open the NPS console, double-click Policies, click Network Policies, and then double-click the policy you want to configure.
In policy Properties, click the Conditions tab, and then click Add. In Select condition, scroll to the Network Access Protection group of conditions.
If you want to configure the Identity Type condition, click Identity Type, and then click Add. In Specify the method in which clients are identified in this policy, select the items appropriate for your deployment, and then click OK.

The Identity Type condition is used for the DHCP and Internet Protocol security (IPsec) enforcement methods to allow client health checks when NPS does not receive an Access-Request message that contains a value for the User-Name attribute; in this case, client health checks are performed, but authentication and authorization are not performed.

If you want to configure the MS-Service Class condition, click MS-Service Class, and then click Add. In Specify the profile name that identifies your DHCP scope, type the name of an existing DHCP profile, and then click Add.
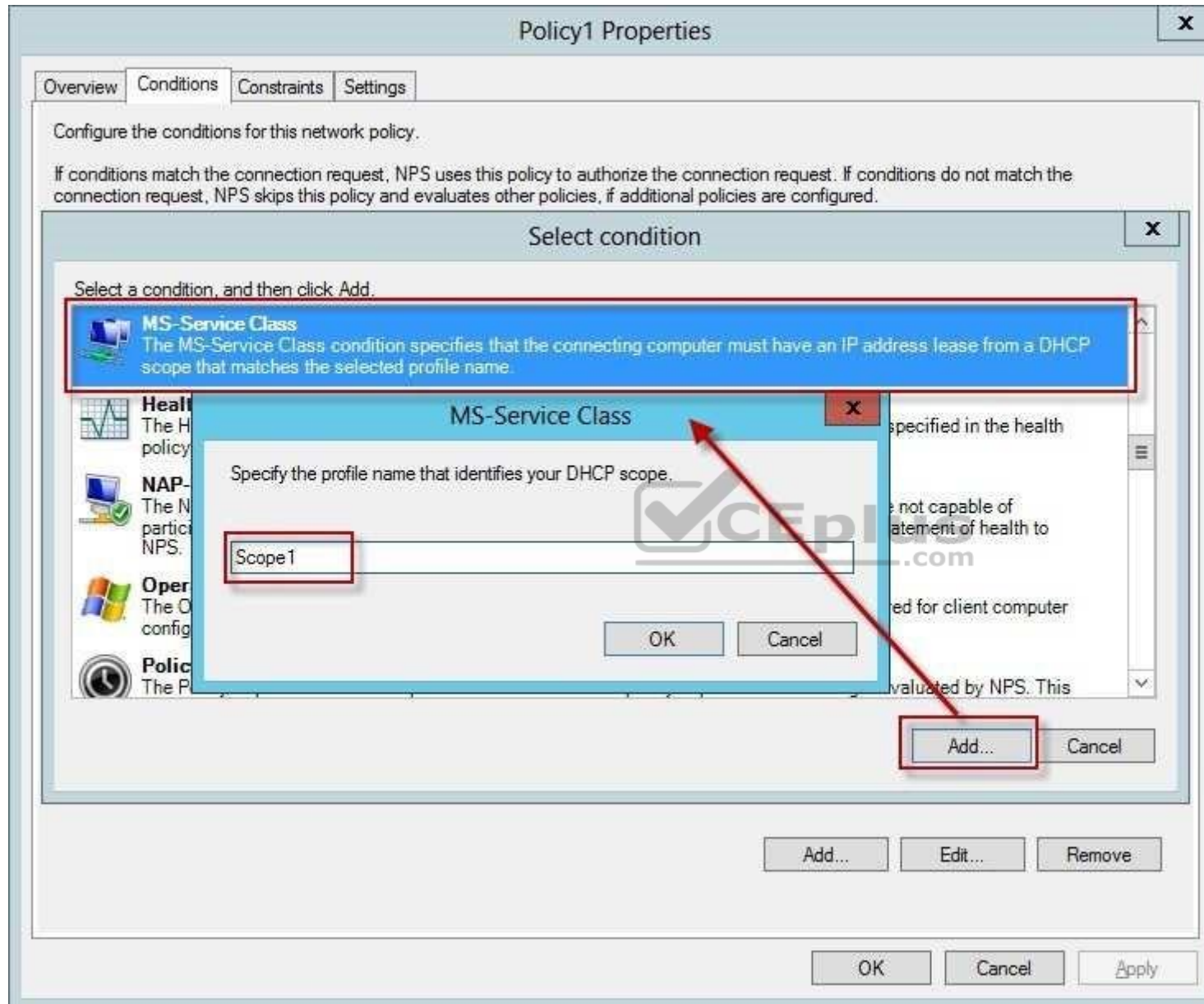
The MS-Service Class condition restricts the policy to clients that have received an IP address from a DHCP scope that matches the specified DHCP profile name.
This condition is used only when you are deploying NAP with the DHCP enforcement method.

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

QUESTION 123
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. One of the domain controllers is named DC1.

The DNS zone for the contoso.com zone is Active Directory-integrated and has the default settings.

A server named Server1 is a DNS server that runs a UNIX-based operating system.

You plan to use Server1 as a secondary DNS server for the contoso.com zone.

You need to ensure that Server1 can host a secondary copy of the contoso.com zone.
What should you do?

A. From DNS Manager, modify the Advanced settings of DC1.
B. From DNS Manager, modify the Zone Transfers settings of the contoso.com zone.
C. From Windows PowerShell, run the Set-DnsServerForwarder cmdlet and specify the contoso.com zone as a target.
D. From DNS Manager, modify the Security settings of DC1.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
There are two ways that a secondary DNS server can be added. In both scenarios you will need to add the new server to the Forwarders list of the primary Domain Controller.
▪ The Set-DnsServerForwarder cmdlet changes forwarder settings on a Domain Name System (DNS) server.
▪ From the primary server, open DNS Manager, right click on the server name and select Properties. Click on the Forwarders tab and click the Edit button in the middle of the dialogue box.

QUESTION 124
Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2008 Service Pack 2 (SP2), Windows Server 2008 R2 Service Pack 1 (SP1), Windows Server 2012, and Windows Server 2012 R2.

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

You need to recover Group1 and identify the names of the users who were members of Group1 prior to its deletion. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do first?

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

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
The Active Directory Recycle Bin does not have the ability to track simple changes to objects. If the object itself is not deleted, no element is moved to the Recycle Bin for possible recovery in the future. In other words, there is no rollback capacity for changes to object properties, or, in other words, to the values of these properties.
There is another approach you should be aware of. Tombstone reanimation (which has nothing to do with zombies) provides the only way to recover deleted objects without taking a DC offline, and it's the only way to recover a deleted object's identity information, such as its objectGUID and objectSid attributes. It neatly solves the problem of recreating a deleted user or group and having to fix up all the old access control list (ACL) references, which contain the objectSid of the deleted object.
Restores domain controllers to a specific point in time, and marks objects in Active Directory as being authoritative with respect to their replication partners.

QUESTION 125
Your network contains an Active Directory domain named adatum.com. All domain controllers run Windows Server 2012 R2. The domain contains a virtual machine named DC2.

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

Name	Type
App1	Service

You need to ensure that you can clone DC2.

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

☐ A. Create an empty file named DCCloneConfig.xml.

☐ B. Add the following information to the DCCloneConfigSchema.xsd file:

```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```

☐ C. Create an empty file named CustomDCCloneAllowList.xml.

☐ D. Create a file named DCCloneConfig.xml that contains the following information:

```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```

☐ E. Create a file named CustomDCCloneAllowList.xml that contains the following information:

```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```

A. Option A
B. Option B
C. Option C
D. Option D

E. Option E

Correct Answer: AE
Section: Volume B
Explanation

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

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

The four primary steps to deploy a cloned virtualized domain controller are as follows:
▪ Grant the source virtualized domain controller the permission to be cloned by adding the source virtualized domain controller to the Cloneable Domain Controllers group.
▪ Run Get-ADDCCloningExcludedApplicationListcmdlet in Windows PowerShell to determine which services and applications on the domain controller are not compatible with the cloning.
▪ Run New-ADDCCloneConfigFile to create the clone configuration file, which is stored in the C:\Windows\NTDS. ▪
In Hyper-V, export and then import the virtual machine of the source domain controller.

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

The clone domain controller will be located in the same site as the source domain controller unless a different site is specified in the DCCloneConfig.xml file.
Note:
▪ The Get-ADDCCloningExcludedApplicationListcmdlet searches the local domain controller for programs and services in the installed programs database, the services control manager that are not specified in the default and user defined inclusion list. The applications in the resulting list can be added to the user defined exclusion list if they are determined to support cloning. lf the applications are not cloneable, they should be removed from the source domain controller before the clone media is created. Any application that appears in cmdlet output and is not included in the user defined inclusion list will force cloning to fail. ▪ The Get- ADDCCloningExcludedApplicationListcmdlet needs to be run before the New- ADDCCloneConfigFilecmdlet is used because if the NewADDCCloneConfigFilecmdlet detects an excluded application, it will not create a DCCloneConfig.xml file.
▪ DCCloneConfig.xml is an XML configuration file that contains all of the settings the cloned DC will take when it boots. This includes network settings, DNS, WINS, AD site name, new DC name and more. This file can be generated in a few different ways.

The New-ADDCCloneConfigcmdlet in PowerShell

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

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

```
                          Administrator: Windows PowerShell                    _  □  x

PS C:\Users\Administrator.DC01> New-ADDCCloneConfigFile -Static -IPv4Address 10.10.10.202 -IPv4DefaultGateway 10.10.10.1
-IPv4SubnetMask 255.255.255.0 -IPv4DNSResolver 10.10.10.73,10.10.10.202 -CloneComputerName DC02 -SiteName Default-First
-Site-Name
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or late
r...
Passed: The domain controller hosting the PDC FSMO role (DC01.accusource.local) was located and running Windows Server 2
012 or later.

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

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

No valid clone configuration files were found at any of the supported locations.

All preliminary validation checks passed.

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

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

DCCloneConfig - Notepad

File Edit Format View Help

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

References: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/virtualized-domain-controller-deployment-andconfiguration#BKMK_VDCCloning http://blogs.dirteam.com/blogs/sanderberkouwer/archive/2012/09/10/new-features-in-active-directory-domain-services-in-windows-server-2012-part-13-domaincontroller-cloning.aspx

QUESTION 126
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2. Both servers have the File and Storage Services server role, the DFS Namespace role service, and the DFS Replication role service installed.

Server1 and Server2 are part of a Distributed File System (DFS) Replication group named Group1. Server1 and Server2 are connected by using a high-speed LAN connection.

You need to minimize the amount of processor resources consumed by DFS Replication.

What should you do?

A. Modify the replication schedule.
B. Modify the staging quota.

C. Disable Remote Differential Compression (RDC).
D. Reduce the bandwidth usage.

Correct Answer: C
Section: Volume B

Explanation

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

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

QUESTION 127
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2.

All sales users have laptop computers that run Windows 8.1. The sales computers are joined to the domain. All user accounts for the sales department are in an organizational unit (OU) named Sales_OU.

A Group Policy object (GPO) named GPO1 is linked to Sales_OU.
You need to configure a dial-up connection for all of the sales users.

What should you configure from User Configuration in GPO1?

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

Correct Answer: B
Section: Volume B
Explanation
Explanation/Reference:
Explanation:

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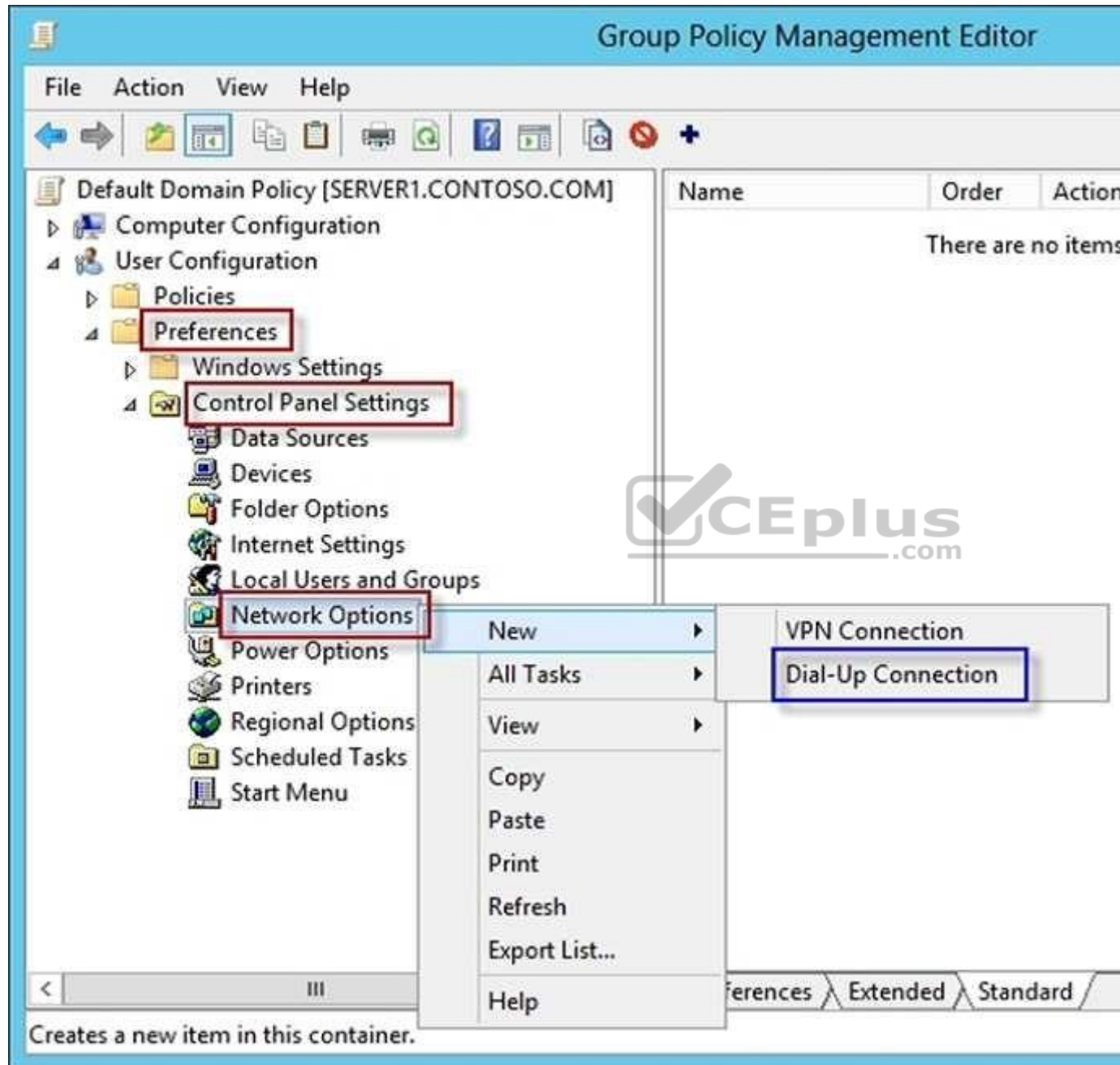
To create a new Dial-Up Connection preference item

Open the Group Policy Management Console. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click Edit.
In the console tree under Computer Configuration or User Configuration, expand the Preferences folder, and then expand the Control Panel Settings folder. Right-click the Network Options node, point to New, and select Dial-Up Connection.

References:
http://technet.microsoft.com/en-us/library/cc772107.aspx http://technet.microsoft.com/en-us/library/cc772449.aspx

QUESTION 128
Your network contains an Active Directory domain named contoso.com.

A user named User1 creates a central store and opens the Group Policy Management Editor as shown in the exhibit. (Click the Exhibit button.)
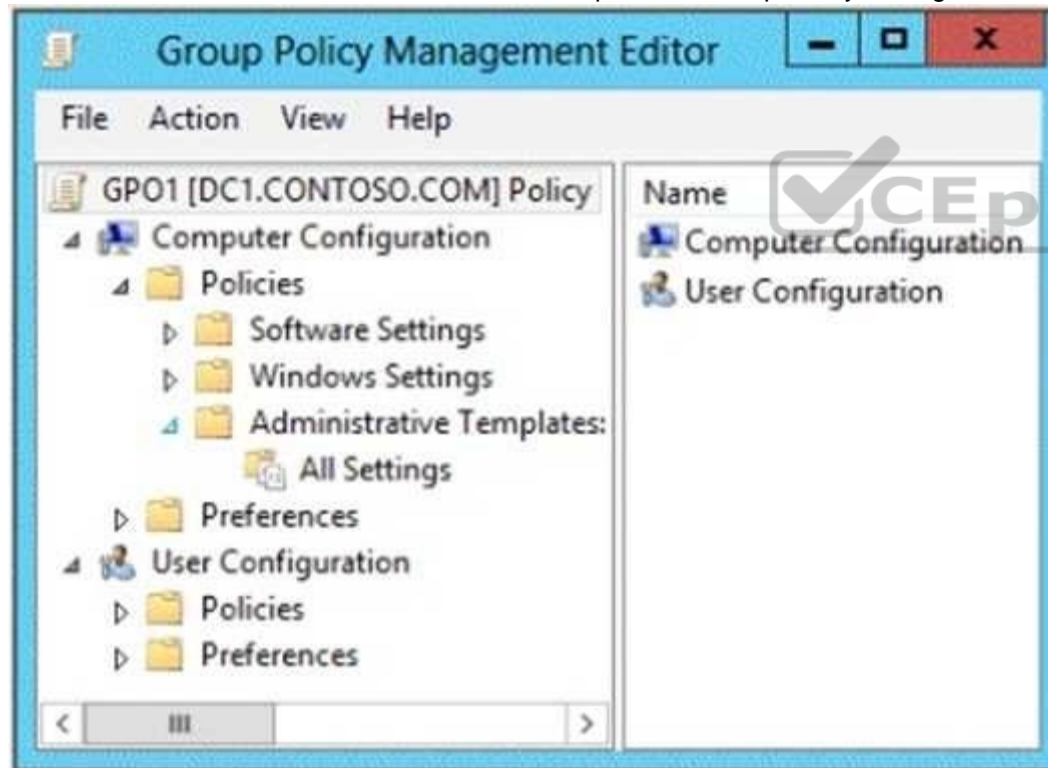
You need to ensure that the default Administrative Templates appear in GPO1.

What should you do?

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

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
In earlier operating systems, all the default Administrative Template files are added to the ADM folder of a Group Policy object (GPO) on a domain controller. The GPOs are stored in the SYSVOL folder. The SYSVOL folder is automatically replicated to other domain controllers in the same domain. A policy file uses approximately 2 megabytes (MB) of hard disk space. Because each domain controller stores a distinct version of a policy, replication traffic is increased.

In Group Policy for Windows Server 2008 and Windows Vista, if you change Administrative template policy settings on local computers, Sysvol will not be automatically updated with the new .admX or .admL files. This change in behavior is implemented to reduce network load and disk storage requirements, and to prevent conflicts between .admX files and.admL files when edits to Administrative template policy settings are made across different locales. To make sure that any local updates are reflected in Sysvol, you must manually copy the updated .admX or .admL files from the PolicyDefinitions file on the local computer to the Sysvol \PolicyDefinitions folder on the appropriate domain controller.

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

To create a Central Store for .admx and .adml files, create a folder that is named PolicyDefinitions in the following location:
\\FQDN\SYSVOL\FQDN\policies

Reference:
http://support.microsoft.com/kb/929841

QUESTION 129
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 the File Server Resource Manager console, create a local classification property.
B. From the File Server Resource Manager console, create a share for Folder1 by selecting the SMB Share – Advanced option.
C. From the File Explorer, modify the Classification tab on Folder1.
D. From File Explorer, modify the Customize tab of Folder1.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
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.

References: https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/jj574182(v=ws.11)#BKMK_12

QUESTION 130
Your company has a main office and a branch office.

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

The main office contains a domain controller named DC1 that runs Windows Server 2012 R2. DC1 is a DNS server and hosts a primary zone for contoso.com. The branch office contains a member server named Server1 that runs Windows Server 2012 R2. Server1 is a DNS server and hosts a secondary zone for contoso.com.

The main office connects to the branch office by using an unreliable WAN link.

You need to ensure that Server1 can resolve names in contoso.com if the WAN link is unavailable for three days.

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

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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
Used by other DNS servers that are configured to load and host the zone to determine when zone data expires if it is not renewed

QUESTION 131
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

DirectAccess is deployed to the network.

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

The remote users report that sometimes their connection is very slow. You need to minimize Group Policy processing across all wireless wide area network (WWAN) connections.

Which Group Policy setting should you configure?

A. Configure Group Policy slow link detection.
B. Configure Direct Access connections as a fast network connection.
C. Configure wireless policy processing.

D. Change Group Policy processing to run asynchronously when a slow network connection is detected.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 132
Your network contains an Active Directory domain named contoso.com.

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

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

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

What should you configure?

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

Correct Answer: D
Section: Volume B
Explanation

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

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

QUESTION 133

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 ensure that only computers that send a statement of health are checked for Network Access Protection (NAP) health requirements.

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

A. The Called Station ID constraints
B. The MS-Service Class conditions
C. The Health Policies conditions
D. The NAS Port Type constraints
E. The NAP-Capable Computers conditions

Correct Answer: CE
Section: Volume B
Explanation

Explanation/Reference:
Reference:
http://technet.microsoft.com/en-us/library/cc753603.aspx http://technet.microsoft.com/en-us/library/cc731220(v=ws.10).aspx http://technet.microsoft.com/en-us/library/cc731560.aspx

QUESTION 134
Your network contains an Active Directory domain named contoso.com. All users have client computers that run Windows 8.1.

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

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

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

What should you configure?

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

Correct Answer: C
Section: Volume B
Explanation
Explanation/Reference:
References: https://technet.microsoft.com/en-us/library/dn789189(v=ws.11).aspx

QUESTION 135
Your network contains a single Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2.

The domain contains 400 desktop computers that run Windows 8 and 10 desktop computers that run Windows XP Service Pack 3 (SP3). All new desktop computers that are added to the domain run Windows 8.

All of the desktop computers are located in an organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1. GPO1 contains startup script settings. You link GPO1 to OU1.

You need to ensure that GPO1 is applied only to computers that run Windows XP SP3.

What should you do?

A. Create and link a WMI filter to GPO1
B. Run the Set-GPInheritance cmdlet and specify the -target parameter.
C. Run the Set-GPLink cmdlet and specify the -target parameter.
D. Modify the Security settings of OU1.

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
WMI Filtering is used to get information of the system and apply the GPO on it with the condition is met.
Security filtering: apply a GPO to a specific group (members of the group)

QUESTION 136
Your network contains an Active Directory domain named contoso.com. The network contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy and Access Services server role installed.

You plan to deploy additional servers that have the Network Policy and Access Services server role installed. You must standardize as many settings on the new servers as possible.

You need to identify which settings can be standardized by using Network Policy Server (NPS) templates.

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

A. IP filters
B. shared secrets
C. health policies
D. network policies
E. connection request policies

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 137
Your network contains an Active Directory domain named contoso.com. The functional level of the forest is Windows Server 2008 R2.

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

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

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

New Namespace Wizard

Namespace Type

Steps:

Namespace Server

Namespace Name and Settings

Namespace Type

Review Settings and Create Namespace

Confirmation

Select the type of namespace to create.

(•) Domain-based namespace

A domain-based namespace is stored on one or more namespace servers and in Active Directory Domain Services. You can increase the availability of a domain-based namespace by using multiple servers. When created in Windows Server 2008 mode, the namespace supports increased scalability and access-based enumeration.

[ ] Enable Windows Server 2008 mode

Preview of domain-based namespace:

`\\contoso.com\Public`

( ) Stand-alone namespace

A stand-alone namespace is stored on a single namespace server. You can increase the availability of a stand-alone namespace by hosting it on a failover cluster.

Preview of stand-alone namespace:

`\\server3\Public`

< Previous   Next >   Cancel

You create two Password Settings objects named PSO1 and PSO2. PSO1 is applied to MarketingUsers. PSO2 is applied to MarketingComputers.

The minimum password length is defined for each policy as shown in the following table.

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

You need to identify the minimum password length required for each marketing user.

What should you identify?

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

Correct Answer: D
Section: Volume B

Explanation

Explanation/Reference:

QUESTION 138
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012.

You have a Group Policy object (GPO) named GPO1 that contains several custom Administrative templates.

You need to filter the GPO to display only settings that will be removed from the registry when the GPO falls out of scope. The solution must only display settings that are either enabled or disabled and that have a comment.

How should you configure the filter?

To answer, select the appropriate options below. Select three.

Filter Options

Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.

Select the type of policy settings to display.

Managed:	Configured:	Commented:
Any ▼	Any ▼	Any ▼

☐ Enable Keyword Filters

☐ Enable Keyword Filters

Filter for word(s): [   ] Any ▼

Within: ☑ Policy Setting Title   ☑ Help Text   ☑ Comment

☐ Enable Requirements Filters

Select the desired platform and application filter(s):

Include settings that match any of the selected platforms. ▼

☐ BITS 1.5
☐ BITS 2.0
☐ BITS 3.5
☐ BITS 4.0
☐ Internet Explorer 10
☐ Internet Explorer 3
☐ Internet Explorer 4
☐ Internet Explorer 5

Select All

Clear All

OK   Cancel

A. Set Managed to: Yes

B. Set Managed to: No C. Set Managed to: Any

D. Set Configured to: Yes E.
Set Configured to: No

F. Set Configured to: Any

G. Set Commented to: YesH. Set Commented to: No

I. Set Commented to: Any

Correct Answer: AFG
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 139
Your network contains an Active Directory domain named adatum.com.

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

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

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

Correct Answer: DF
Section: Volume B
Explanation

Explanation/Reference:
QUESTION 140
Your network contains multiple Active Directory sites.

You have a Distributed File System (DFS) namespace that has a folder target in each site.

You discover that some client computers connect to DFS targets in other sites.

You need to ensure that the client computers only connect to a DFS target in their respective site.

What should you modify?

A. The properties of the Active Directory sites
B. The properties of the Active Directory site links
C. The delegation settings of the namespace
D. The referral settings of the namespace

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Reference: http://www.windowsnetworking.com/articles_tutorials/Configuring-DFS-Namespaces.html

QUESTION 141
Your network contains an Active Directory domain named adatum.com. The domain contains five servers. The servers are configured as shown in the following table.

Server name	Configuration
DC1	Domain controller and DNS server
DC2	Domain controller and DHCP server
Server1	Windows Deployment Services (WDS)
Server2	Certification authority (CA)
Server3	File server

All desktop computers in adatum.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. Server3
B. Server1C. DC2
D. Server2
E. DC1

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
The BitLocker-NetworkUnlock feature must be installed on a Windows Deployment Server (which does not have to be configured--the WDSServer service just needs to be running).

QUESTION 142
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

You pre-create a read-only domain controller (P.QDC) account named RODC1.
You export the settings of RODC1 to a file named Filel.txt.
You need to promote RODC1 by using File1.txt.

Which tool should you use?

A. The Install-WindowsFeature cmdlet
B. The Add-WindowsFeature cmdlet
C. The Dism command
D. The Install-ADDSDomainController cmdlet
E. the Dcpromo command

Correct Answer: E
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 143

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

From the Group Policy Management console, you view the details of a Group Policy object (GPO) named GPO1 as shown in the exhibit. (click the Exhibit button.)
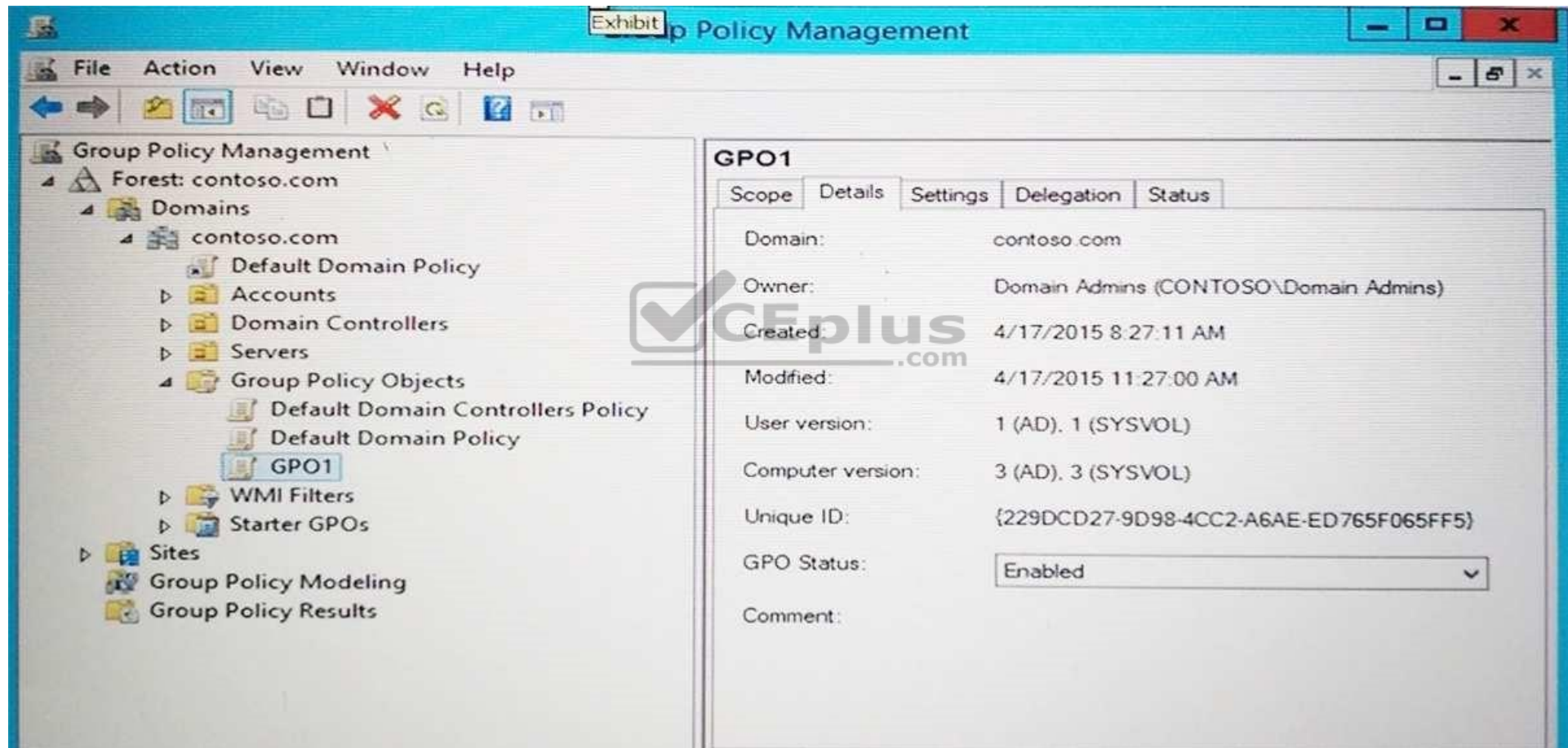
You need to ensure that the comments field of GPO1 contains a detailed description of GPO1.

What should you do?

A. From Active Directory Users and Computers, edit the properties of contoso.com/System/Policies/{229DCD27-9D98-ACC2-A6AE-ED765F065FF5}.
B. OpenGPO1in the Group Policy Management Editor, and then modify the properties of GPO1.
C. From Notepad, edit \\contoso.com\SYSVOL\contoso.com\Policies\{229DCD27-9D98-ACC2-A6AE-ED765F065FF5}\gpt.ini.
D. From Group Policy Management, click View, and then click Customize.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

Adding a comment to a Group Policy object
▪ Open the Group Policy Management Console. Expand the Group Policy Objects node.
▪ Right-click the Group Policy object you want to comment and then click Edit.
▪ In the console tree, right-click the name of the Group Policy object and then click Properties.
▪ Click the Comment tab.
▪ Type your comments in the Comment box. ▪ Click OK

https://technet.microsoft.com/en-

us/library/cc770974.aspx

QUESTION 144
You have a group Managed Service Account named Service01. Three servers named Server01, Server02, and Server03 currently use the Service01 service account.

You plan to decommission Server01.

You need to remove the cached password of the Service01 service account from Server01. The solution must ensure that Server02 and Server 03 continue to use Service01.

Which cmdlet should you run?

A. Set-ADServiceAccount
B. Remove-ADServiceAccount
C. Uninstall-ADServiceAccount
D. Reset-ADServiceAccountPassword

Correct Answer: B

Section: Volume B

Explanation

Explanation/Reference:
Explanation:
The Remove-ADServiceAccount cmdlet removes an Active Directory service account. This cmdlet does not make changes to any computers that use the service account. After this operation, the service account is no longer hosted on the target computer but still exists in the directory.

Incorrect Answers:
C: The Uninstall-ADServiceAccount cmdlet removes an Active Directory service account on the computer on which the cmdlet is run. The specified service account must be installed on the computer.

References: https://docs.microsoft.com/en-us/powershell/module/addsadministration/remove-adserviceaccount?view=win10-ps

QUESTION 145
You have the following Windows PowerShell Output.

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

You need to create a Managed Service Account.

What should you do?

A. Run **New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com –SAMAccountNameservice01**.
B. Run **New-AuthenticationPolicySilo, and then run New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com**.
C. Run **Add-KDSRootKey, and then run New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com**.
D. Run **Set-KDSConfiguration, and then run New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com**.
E. Create a universal group named Service01, and then run **New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com**.

F. Run **New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com –RestrictToOutboundAuthenticationOnly**.

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

From the exhibit we see that the required key does not exist. First we create this key, then we create the managed service account.

The Add-KdsRootKey cmdlet generates a new root key for the Microsoft Group Key Distribution Service (KdsSvc) within Active Directory (AD). The Microsoft Group KdsSvc generates new group keys from the new root key.

The New-ADServiceAccount cmdlet creates a new Active Directory managed service account.

References:
https://docs.microsoft.com/en-us/powershell/module/kds/add-kdsrootkey?view=win10-ps https://docs.microsoft.com/en-us/powershell/module/activedirectory/new-adserviceaccount?view=winserver2012-ps

QUESTION 146
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a HyperV host that runs Windows Server 2012 R2.

You need to identify which domain controller must be online when cloning a domain controller.

Which cmdlet should you use?

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

F. Get-ADAccountAuthorizationGroup
G. Get-ADAuthenticationPolicySilo
H. Get-ADAuthenticationPolicy

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
One requirement for cloning a domain controller is an existing Windows Server 2012 DC that hosts the PDC emulator role. You can run the Get-ADDomain and retrieve which server has the PDC emulator role.

Example: Command Prompt: C:\PS>
Get-ADDomain

Output would include a line such as: PDCEmulator: Fabrikam-DC1.Fabrikam.com

Incorrect Answers:
A: The Get-ADGroupMember cmdlet gets the members of an Active Directory group. Members can be users, groups, and computers.
E: The Get-ADOptionalFeature cmdlet gets an optional feature or performs a search to retrieve multiple optional features from an Active Directory.
F: The Get-ADAuthorizationGroup cmdlet gets the security groups from the specified user, computer or service accounts token.

References:
https://blogs.technet.microsoft.com/canitpro/2013/06/11/step-by-step-domain-controller-cloning/ https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-addomain?view=win10-ps

QUESTION 147
HOTSPOT
Your network contains one Active Directory domain named contoso.com. The domain contains two servers named Server01 and Server02 that run Windows Server 2012 R2.

Server01 is a member of a Distributed File System (DFS) replication group named RG01 that replicates to a folder named RF01.

You plan to replicate RF01 to Server02. RF01 will be pre-staged on Server02.

You need export the DFS files and the DFS database from Server01.

Which tools should you use? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

Export DFS files:

Dfsrmig
Export-BinaryMILog
Export-DFSRClone
Robocopy
Sync-DFSRREplicationGroup

Export DFS database:

Dfsrmig
Export-BinaryMILog
Export-DFSRClone
Robocopy
Sync-DFSRREplicationGroup

Correct Answer:

Answer Area

Export DFS files:

▼
Dfsrmig
Export-BinaryMILog
Export-DFSRClone
Robocopy
Sync-DFSRReplicationGroup

Export DFS database:

▼
Dfsrmig
Export-BinaryMILog
Export-DFSRClone
Robocopy
Sync-DFSRReplicationGroup

Section: Volume B
Explanation

Explanation/Reference:
References: https://technet.microsoft.com/en-us/library/dn495044(v=ws.11).aspx https://technet.microsoft.com/en-us/library/dn482443(v=ws.11).aspx

QUESTION 148
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2008 R2.

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

You have a Windows image file named file1.wim.

You need to add an image of a volume to file1.wim.

What should you do?

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

Correct Answer: D
Section: Volume B
Explanation

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

Incorrect Answers:
A, B: Imagex has been retired and replaced by dism.

References:
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/dism---deployment-image-servicing-and-management-technical-reference-for-windows
https://docs.microsoft.com/en-us/powershell/module/dism/?view=win10-ps

QUESTION 149
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a HyperV host that runs Windows Server 2012 R2.

You need to identify which user accounts were authenticated by RODC1.

Which cmdlet should you use?

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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
The Get-ADDomainControllerPasswordReplicationPolicyUsage cmdlet gets the user or computer accounts that are authenticated by a read-only domain controller (RODC) or that have passwords that are stored on that RODC. The list of accounts that are stored on a RODC is known as the revealed list.
To get accounts that are authenticated by the RODC, use the AuthenticatedAccounts parameter. To get the accounts that have passwords stored on the RODC, use the RevealedAccounts parameter.

References: https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-addomaincontrollerpasswordreplicationpolicyusage?view=win10-ps

QUESTION 150
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a HyperV host that runs Windows Server 2012 R2.

You need to identify whether deleted objects can be recovered from the Active Directory Recycle Bin.

Which cmdlet should you use?

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

Correct Answer: E
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The Get-ADOptionalFeature cmdlet gets an optional feature or performs a search to retrieve multiple optional features from an Active Directory.

Example: Get-ADOptionalFeature 'Recycle Bin Feature' Get
the optional feature with the name 'Recycle Bin Feature'.

References: https://docs.microsoft.com/en-us/powershell/module/addsadministration/get-adoptionalfeature?view=win10-ps

QUESTION 151
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a HyperV host that runs Windows Server 2012 R2.

You need to identify which domain controllers are authorized to be cloned by using virtual domain controller cloning.

Which cmdlet should you use?

A. Get-ADGroupMember
B. Get-ADDomainControllerPasswordReplicationPolicy

C. Get-ADDomainControllerPasswordReplicationPolicyUsage

D. Get-ADDomain

E. Get-ADOptionalFeature

F. Get-ADAccountAuthorizationGroup

G. Get-ADAuthenticationPolicySilo

H. Get-ADAuthenticationPolicy

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
One requirement for cloning a domain controller is an existing Windows Server 2012 DC that hosts the PDC emulator role. You can run the Get-ADDomain and retrieve which server has the PDC emulator role.

Example: CommandPrompt: C:\PS>
Get-ADDomain

Output would include a line such as: PDCEmulator: Fabrikam-DC1.Fabrikam.com

References:
http://blogs.technet.com/b/canitpro/archive/2013/06/12/step-by-step-domain-controller-cloning.aspx https://technet.microsoft.com/en-us/library/ee617224.aspx

QUESTION 152
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a HyperV host that runs Windows Server 2012 R2.

You need to identify which security principals are authorized to have their password cached on RODC1.

Which cmdlet should you use?

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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

The Get-ADDomainControllerPasswordReplicationPolicy gets the users, computers, service accounts and groups that are members of the applied list or denied list for a read-only domain controller's (RODC) password replication policy. To get the members of the applied list, specify the AppliedList parameter. To get the members of the denied list, specify the DeniedList parameter.

Example: Get from an RODC domain controller password replication policy the allowed accounts showing the name and object class of each:

Get-ADDomainControllerPasswordReplicationPolicy -Identity "FABRIKAM-RODC1" -Allowed | ft Name,ObjectClass

QUESTION 153
You have two Windows Server Update Services (WSUS) servers named Server01 and Server02. Server01 synchronizes from Microsoft Update. Server02 synchronizes updates from Server01. Both servers are members of the same Active Directory domain.

You configure Server01 to require SSL for all WSUS metadata by using a certificate issued by an enterprise root certification authority (CA).

You need to ensure that Server02 synchronizes updates from Server01.

What should you do on Server02?

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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
We configure server02 to use server01 as a proxy for the updates through the wsusutil.exe configure sslproxy <ssl_proxy_ip_or_name> <port>

Server01 is the ssl_proxy and the port is 443 (the sll port).

References:
http://blogs.technet.com/b/craigf/archive/2009/05/04/a-work-around-when-using-different-proxies-for-http-and-ssl-in-wsus-3-0-sp1.aspx

QUESTION 154
Your network contains one Active Directory domain named controso.com. The domain contains a file server named Server01 that runs Windows Server 2012 R2. Server01 has an operating system drive and a data drive. Server01 has a Trusted Platform Module (TPM).

You need to enable BitLocker Drive Encryption (BitLocker) for the data drive on Server01.

Which cmdlet should you run first?

A. Unblock-TPM
B. Enable-BitLocker
C. Add-BitLockerKeyProtector
D. Install-WindowsFeature

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:

References:
https://technet.microsoft.com/en-GB/library/jj612864.aspx

QUESTION 155
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1. All servers run Windows Server 2012 R2.

You have two user accounts named User1 and User2. User1 and User2 are members of a group named Group1. User1 has the Department value set to Sales. User2 has the Department value set to Marketing. User1 has the Employee Type value set to Full Time Employee. User2 has the Employee Type value set to Contract Employee.

You create the auditing entry as shown in the exhibit. (Click the Exhibit button.)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the exhibit.

Note: Each correct selection is worth one point.

Hot Area:

Answer Area

To ensure that an audit event is logged when User1 deletes files on Server1, you must ...

▼
modify the Principal setting.
modify the Permissions settings.
modify the Employee Type setting.
modify the condition for the Department va

You must ... to ensure that an audit an event is logged when User2 opens files on Server1.

▼
add a condition
modify the Principal setting
modify the Permissions settings
modify the condition for the Department va

Correct Answer:

Answer Area

To ensure that an audit event is logged when User1 deletes files on Server1, you must ...

▼
modify the Principal setting.
modify the Permissions settings.
modify the Employee Type setting.
modify the condition for the Department va

You must ... to ensure that an audit an event is logged when User2 opens files on Server1.

▼
add a condition
modify the Principal setting
modify the Permissions settings
modify the condition for the Department va

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 156
Your network contains one Active Directory forest named contoso.com.

You create a starter Group Policy Object (GPO) named Starter_GPO1.

From the Delegation tab of Starter_GPO1, you add a group named GPO_Admins and you assign the Edit settings permissions to the group.

You create a new GPO named GPO1 from Starter_GPO1.

You need to identify which action can be performed by the members of the GPO_Admins group.

What should you identify?

A. Modify the Delegation settings of Starter_GPO1.
B. Modify the Group Policy preferences in Starter_GPO1.
C. Link a WMI filter to GPO1.
D. Modify the Administrative Templates in GPO1.

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Because permission rights applied to starter GPO objects are relative to the starter GPO objects only, the GPO_Admins will be able to modify the Delegation settings of Starter_GPO1.

Incorrect Answers:
B: Starter GPOs do not have preferences, only Administrative Template policy settings.
C, D: Permission rights applied to starter GPO objects are relative to the starter GPO objects only; they are not inherited by actual GPOs created from starter GPOs.

References: https://technet.microsoft.com/en-us/library/cc753200.aspx

QUESTION 157
DRAG DROP
Your network contains a production Active Directory forest named contoso.com and a test Active Directory forest named test.contoso.com. There is no network connectivity between contoso.com and test.contoso.com.

The test.contoso.com domain contains a Group Policy object (GPO) named GPO1.

You need to apply the settings in GPO1 to the contoso.com domain.

Which four actions should you perform?

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

Select and Place:

Actions

Run the **Get-GPO** cmdlet.

Run the **Save-NetGPO** cmdlet.

Run the **Import-GPO** cmdlet.

Run the **Restore-GPO** cmdlet.

Run the **Copy-GPO** cmdlet.

Run the **Backup-GPO** cmdlet.

Create a GPO in contoso.com.

Use removable media to transfer the contents of test.contoso.com to contoso.com.

Answer Area

Correct Answer:

Actions

Run the **Get-GPO** cmdlet.

Run the **Save-NetGPO** cmdlet.

Run the **Restore-GPO** cmdlet.

Run the **Copy-GPO** cmdlet.

Answer Area

Run the **Backup-GPO** cmdlet.

Use removable media to transfer the contents of test.contoso.com to contoso.com.

Create a GPO in contoso.com.

Run the **Import-GPO** cmdlet.

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 158
Your network contains one Active Directory domain named contoso.com.

You pilot DirectAccess on the network.

During the pilot deployment, you enable DirectAccess only for a group named Contoso\Test Computers.

Once the pilot is complete, you need to enable DirectAccess for all of the client computers in the domain.

What should you do?

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

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

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

QUESTION 159
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a HyperV host that runs Windows Server 2012 R2.

You need to identify whether the members of the Protected Users group will be prevented from authenticating by using NTLM.
Which cmdlet should you use?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:

References:
https://technet.microsoft.com/en-us/library/dn466518.aspx

QUESTION 160
You have a Windows Server Update Services (WSUS) server named Server1. Server1 synchronizes from Microsoft Update.

You plan to deploy a new WSUS server named Server2. Server2 will synchronize updates from Server1. Server2 will be separated from Server1 by a firewall.

You need to identify which port must be open on the firewall so that Server2 can synchronize the updates.

Which port should you identify?

A. 8530
B. 3389
C. 80
D. 443

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
WSUS upstream and downstream servers will synchronize on the port configured by the WSUS Administrator. By default, these ports are configured as follows:
On WSUS 3.2 and earlier, port 80 for HTTP and 443 for HTTPS On WSUS 6.2 and later (at least Windows Server 2012), port 8530 for HTTP and 8531 for HTTPS
The firewall on the WSUS server must be configured to allow inbound traffic on these ports.

References:
https://technet.microsoft.com/en-GB/library/hh852346.aspx

QUESTION 161
Your network is configured as shown in the exhibit. (Click the Exhibit button.)
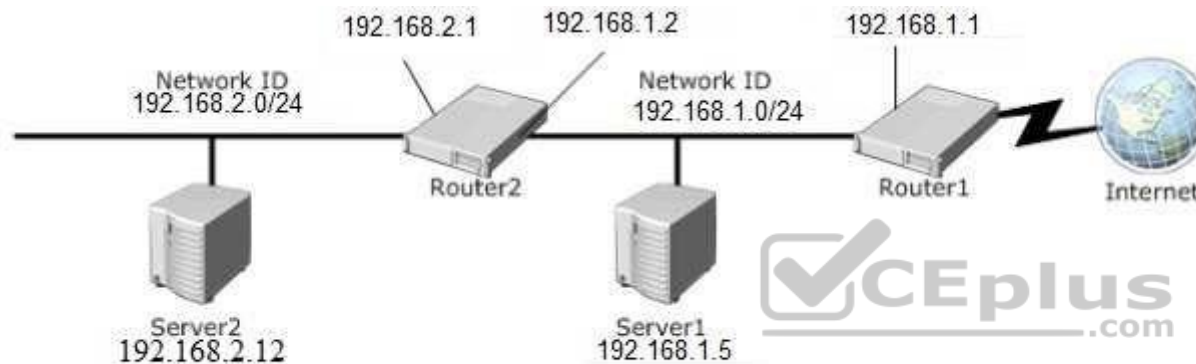
Server1 regularly accesses Server2.

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

You need to optimize the connection path from Server1 to Server2.

Which route command should you run on Server1?

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

Correct Answer: C

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 162
Your network contains an Active Directory forest named contoso.com. The functional level of the forest is Windows Server 2008 R2.

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

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

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

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

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

PSO applied to a user takes priority over PSO applied to computers or groups.

QUESTION 163
Your network contains an Active Directory domain named contoso.com.

You create a new user account named Admin5.

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

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

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

Correct Answer: CD
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 164
Your company is testing DirectAccess on Windows Server 2012 R2.

Users report that when they connect to the corporate network by using DirectAccess, access to Internet websites and Internet hosts is slow. The users report that when they disconnect from DirectAccess, access to the Internet websites and the Internet hosts is much faster.

You need to identify the most likely cause of the performance issue.

What should you identify?

A. DirectAccess uses a self-signed certificate.
B. Force tunneling is enabled.
C. The corporate firewall blocks TCP port 8080.
D. The DNS suffix list is empty.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:

QUESTION 165
You deploy a Windows Server Update Services (WSUS) server named Server01.

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

You need to ensure that the computers are assigned to the correct computer groups automatically when the GPO is deployed.

Which two actions should you perform before you deploy the GPO? Each correct answer presents part of the solution.

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

Correct Answer: BD
Section: Volume B
Explanation

Explanation/Reference:
References: https://technet.microsoft.com/en-
us/library/dd939829(v=ws.10).aspx **QUESTION 166**
Your network contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2.

On Server1, you create a Data Collector Set (DCS) named Data1.

You need to export Data1 to Server2.

What should you do first?

A. Right-click Data1 and click Data Manager… B.
Right-click Data1 and click Export list…
C. Right-click Data1 and click Properties.
D. Right-click Data1 and click Save template…

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

QUESTION 167
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains one Active Directory Domain Services domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a HyperV host that runs Windows Server 2012 R2.

You need to identify which user accounts were authenticated by RODC01.

Which Windows PowerShell cmdlet should you run?

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

F. Get-ADAccountAuthorizationGroup
G. Get-ADAuthenticationPolicySilo
H. Get-ADAuthenticationPolicy

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
https://technet.microsoft.com/en-us/library/ee617194.aspx

QUESTION 168
You have three Windows Server Update Services (WSUS) servers named Server01, Server02, Server03. Server01 synchronizes from Microsoft Update.

You need to ensure that only Server02 and Server03 can synchronize from Server01.

What should you do on Server01?

A. Modify %ProgramFiles%\Update Services\ WebServices\serversyncwebservice\Web.config.
B. From the Update Services console, modify the Automatic Approvals options.
C. Modify %ProgramFiles%\Update Services\ WebServices\serversyncwebservice\SimpleAuth.asmx.
D. From the Update Services console, modify the Update Source and Proxy Server options.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
https://technet.microsoft.com/en-us/library/hh852346(v=ws.11).aspx

QUESTION 169
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. One of the domain controllers is named DC1.

The DNS zone for the contoso.com zone is Active Directory-integrated and has the default settings.

A server named Server1 is a DNS server that runs a UNIX-based operating system.

You plan to use Server1 as a secondary DNS server for the contoso.com zone.

You need to ensure that Server1 can host a secondary copy of the contoso.com zone.

What should you do?

A. From Windows PowerShell, run the Set-DnsServerSetting cmdlet and specify DC1 as a target.
B. From DNS Manager, modify the Security settings of DC1.
C. From DNS Manager, modify the Security settings of the contoso.com zone.
D. From DNS Manager, modify the Zone Transfers settings of the contoso.com zone.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
References: https://technet.microsoft.com/en-us/library/cc771652(v=ws.11).aspx#BKMK_cmd

QUESTION 170
You have two Windows Server Update Services (WSUS) servers named Server01 and Server02. Server01 synchronizes from Microsoft Update. Server02 synchronizes updates from Server01. Both servers are members of the same Active Directory domain.

You configure Server01 to require SSL for all WSUS metadata by using a certificate issued by an enterprise root certification authority (CA).

You need to ensure that Server02 synchronizes updates from Server01.

What should you do on Server02?

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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
References: http://jackstromberg.com/2013/11/enabling-ssl-on-windows-server-update-services-wsus/

QUESTION 171
You have the following Windows PowerShell Output.

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

You need to create a Managed Service Account.

What should you do?

A. Run New-AuthenticationPolicySilo, and then run New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com.
B. Create a universal group named Service01, and then run New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com. C. Run New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com -RestrictToOutboundAuthenticationOnly.
D. Run New-ADServiceAccount –Name "service01" –DNSHostName service01.contoso.com -RestrictToSingleComputer.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
References: https://technet.microsoft.com/en-us/library/hh852236(v=wps.630) https://dirteam.com/sander/2012/09/04/new-features-in-active-directory-domain-services-in-windows-server-2012-part-8-group-msas-gmsas/

QUESTION 172
Your network contains a single Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that hosts the primary DNS zone for contoso.com.

All servers dynamically register their host names.

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

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

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

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

A. 1

B. 3

C. 4

D. 2

Correct Answer: D
Section: Volume B

Explanation

Explanation/Reference:
Explanation:

To create DNS Host (A) Records for all internal pool servers
▪ Click Start, click All Programs, click Administrative Tools, and then click DNS.
▪ In DNS Manager, click the DNS Server that manages your records to expand it. ▪
Click Forward Lookup Zones to expand it.
▪ Right-click the DNS domain that you need to add records to, and then click New Host (A or AAAA).
▪ In the Name box, type the name of the host record (the domain name will be automatically appended).
▪ 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.
▪ 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

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

QUESTION 173
Your network contains one Active Directory domain named contoso.com. The domain contains a server named Server01 that runs Windows Server 2012 R2.
Server01 does not have a Trusted Platform Module (TPM).

You need to ensure that you can enable BitLocker Drive Encryption (BitLocker) on the operating system drive.

Which Group Policy setting should you configure?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
To make use of BitLocker on a drive without TPM, you should run the gpedit.msc command. You must then access the Require additional authentication at startup setting by navigating to Computer Configuration\Administrative Templates\Windows Components\Bit Locker Drive Encryption\Operating System Drives under Local Computer Policy.

References: http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/

QUESTION 174
HOTSPOT

Your network contains an Active Directory named contoso.com.
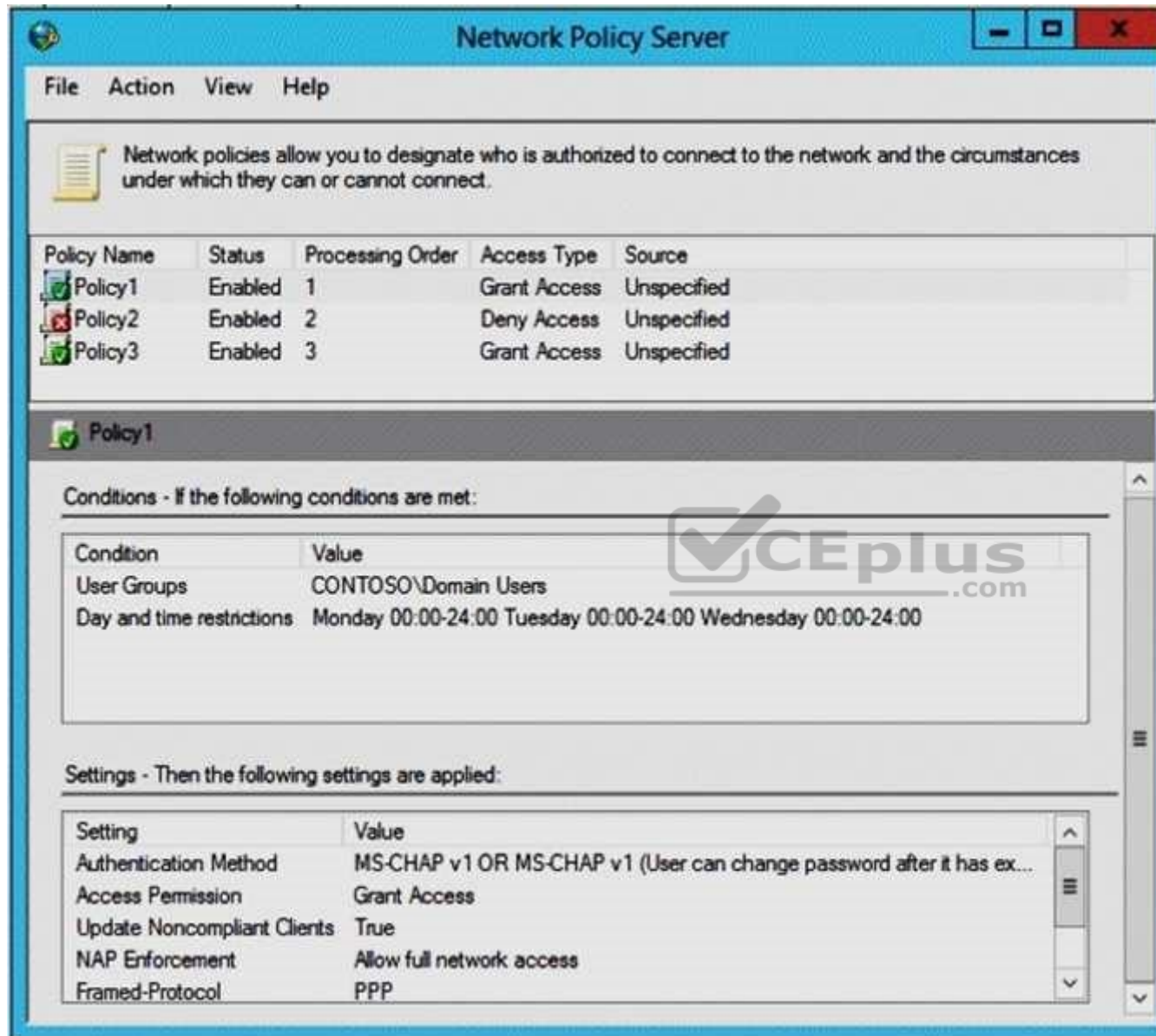
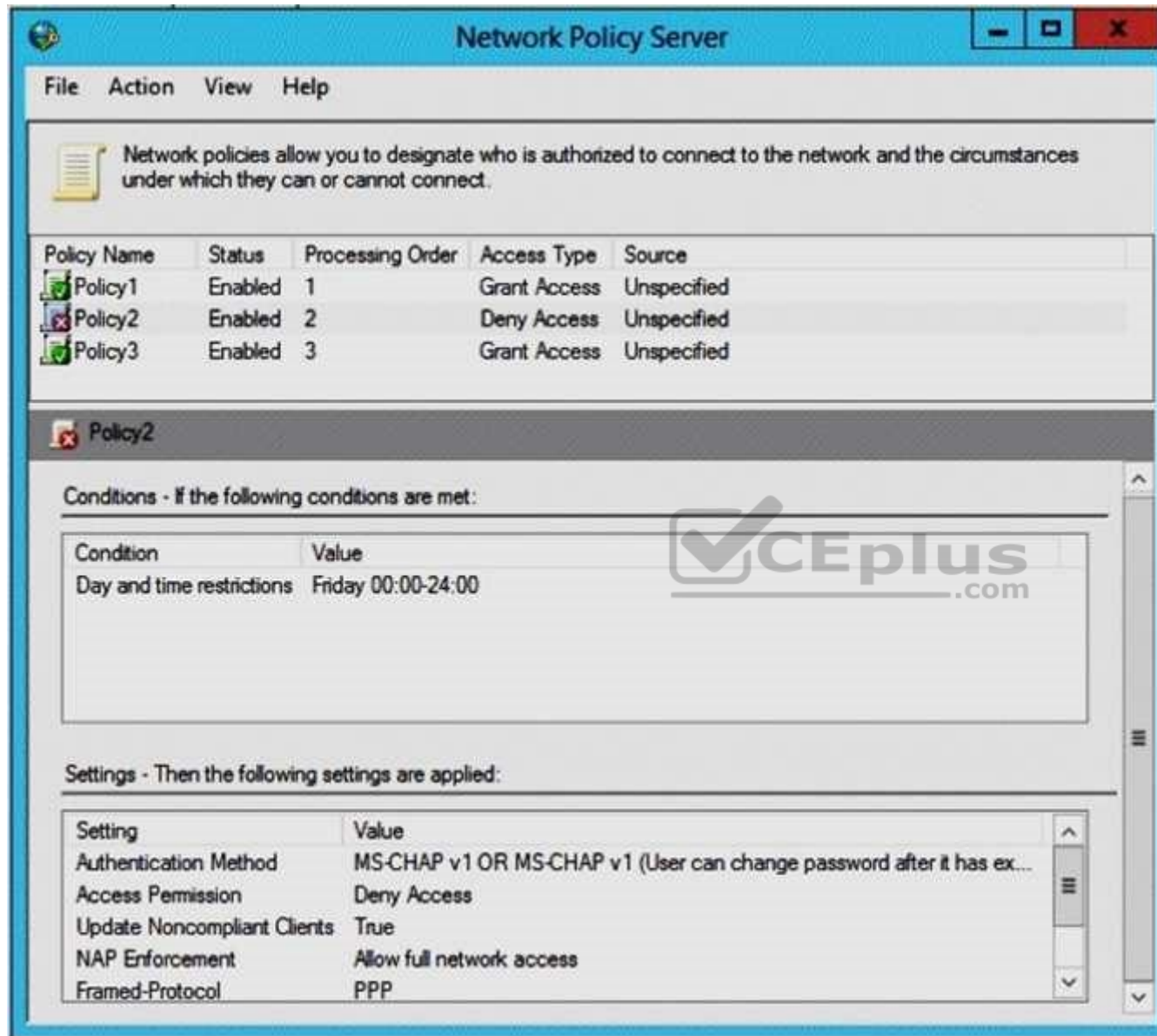You have users named User1 and User2.

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

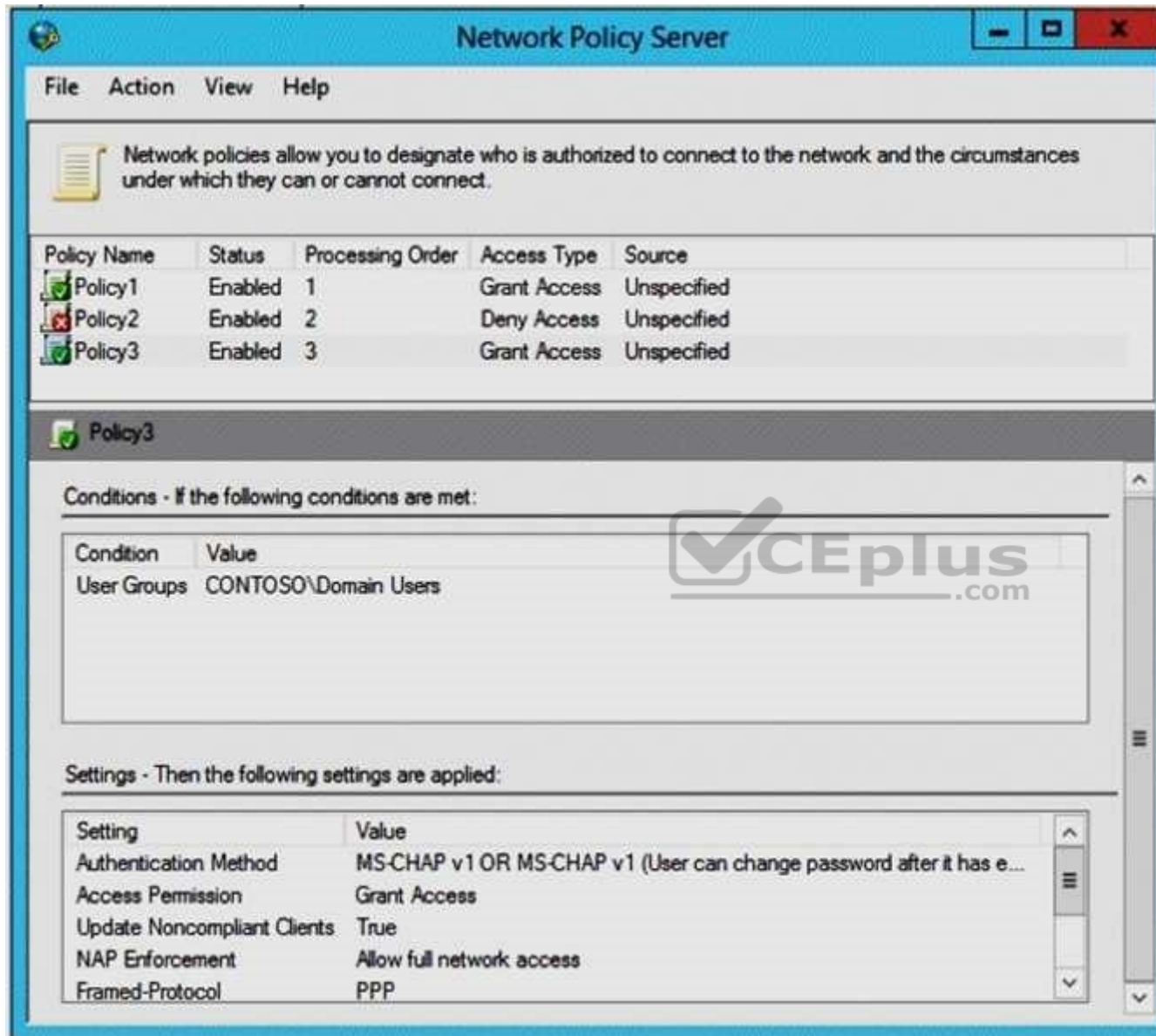A policy named Policy1 is shown in the Policy1 exhibit. (Click the Exhibit button.)

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

Network Policy Server

File   Action   View   Help

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

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

Policy2

Conditions - If the following conditions are met:

Condition	Value
Day and time restrictions	Friday 00:00-24:00

Settings - Then the following settings are applied:

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

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. **NOTE:** Each correct selection is worth one point.

Hot Area:

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

Correct Answer:

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

Section: Volume B
Explanation

Explanation/Reference:

QUESTION 175
You have a Windows Server Updates (WSUS) server named Server01.

You need to prevent the WSUS service on Server01 from being updated automatically.

What should you do from the Update Services console?

A. From the Automatic Approvals options, modify the Advanced settings.
B. From the Products and Classifications options, modify the Products settings.

C. From the Automatic Approvals options, modify the Default Automatic Approval Rule.

D. From the Products and Classifications, modify the Classifications settings.

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
References: https://prajwaldesai.com/configuring-wsus-3-0-sp2-on-windows-
server/

QUESTION 176
Your network contains an Active Directory domain.

A Group Policy object (GRO) named GPO1 is linked to the domain. GPO1 has the settings shown in the following table.

Policy	Policy setting
Enforce password history	5 passwords remembered
Minimum password length	10 characters

You import the backup of a GPO named GPO named GPO2. GPO2 has the settings shown in the following table.

Policy	Policy setting
Minimum password length	5 characters
Store passwords using reversible encryption	Enabled

You import the backup of GPO2 into GPO1.

You need to identify the configurations in GPO1.

What should you identify?

- Minimum password length is set to 5 characters.
- Enforce password history is set to 5 passwords remembered.
- Store passwords using reversible encryption is set to Enabled.

- Minimum password length is set to 10 characters.
- Enforce password history is set to 5 passwords remembered.
- Store passwords using reversible encryption is set to Not Enabled.

- Enforce password history is set to Not Defined.
- Minimum password length is set to 5 characters.
- Store passwords using reversible encryption is set to Enabled.

- Enforce password history is set to Not Defined.
- Minimum password length is set to 10 characters.
- Store passwords using reversible encryption is set to Enabled.

A.

B.

C.

D.

Correct Answer: C

Section: Volume B

Explanation

Explanation/Reference:
References: http://www.dell.com/support/article/za/en/zabsdt1/sln283515/windows-server-how-to-import-a-group-policy-objects-settings-into-another-group-policyobject?lang=en