

Microsoft.70-411.v2015-07-30.by.PT.300q

## VCEplus.com

Number: 70-411  
Passing Score: 700  
Time Limit: 120 min  
File Version: 1.0

**Microsoft Exam 70-411**

**Administering Windows Server 2012 R2**

**300 Questions  
Created 30 July 2015**

### **Exam Topics Covered:**

Deploy, manage, and maintain servers (15-20%).

- Deploy and manage server images
- Implement patch management
- Monitor servers

Configure File and Print Services (15-20%).

- Configure Distributed File System (DFS)
- Configure File Server Resource Manager (FSRM)
- Configure file and disk encryption
- Configure advanced audit policies

Configure network services and access (15-20%).

- Configure DNS zones
- Configure DNS records
- Configure virtual private network (VPN) and routing
- Configure DirectAccess

Configure a Network Policy Server (NPS) infrastructure (10-15%).

- Configure Network Policy Server
- Configure NPS policies
- Configure Network Access Protection (NAP)

Configure and manage Active Directory (15-20%).

- Configure service authentication
- Configure domain controllers
- Maintain Active Directory
- Configure account policies

Configure and manage Group Policy (15-20%).

- Configure Group Policy processing
- Configure Group Policy settings
- Manage Group Policy Objects (GPOs)
- Configure Group Policy Preferences (GPP)

<https://www.microsoft.com/learning/en-us/exam-70-411.aspx>

### **Development Notes:**

Answers to all questions, as written in this study guide, have been researched and verified to be correct through Microsoft TechNet or the Microsoft Developer Network (MSDN). A specific Microsoft URL is provided for each question as an exact reference. Explanations provided reflect condensed reproductions of content from Microsoft.

When possible, the URL provided as a reference will apply specifically to Windows Server 2012 R2. However, not all server roles, features, and services are new, nor have been completely redeveloped. Often, Microsoft has not updated a particular TechNet article because the technology, or the basic concepts of that technology, has not substantially changed. Therefore, occasionally a referenced URL will point to an article which states applicability to Windows Server 2008, or rarely even Windows Server 2003. Regardless, the quoted text will still be directly applicable to the proper answer of the referenced question.

The concept of choosing a “best answer” for questions on Microsoft examinations is based on Microsoft’s determination of a best answer, usually meaning the performance of a defined task with the least amount of administrative actions. In past versions of this collection of practice questions, even if the answer choice had been recorded correctly, the explanation may have been inaccurate. Therefore, sources and opinions other than Microsoft official online publications were not trusted for content to be included here.

This collection of practice questions is developed with the intention to act as a valid and functional study guide, not simply as a question and answer memory tool. Explanations are provided as concisely as possible to target the specific task or topic addressed by the question. However, whenever possible, actual screen shots from Windows Server 2012 R2 and other graphics are provided with the quoted Microsoft text to aid in both conceptual understanding and memory retention.

Practice questions were adapted from multiple practice tests obtained from the following sources:

[www.ActualTests.com](http://www.ActualTests.com)  
[www.BrainDumps.com](http://www.BrainDumps.com)  
[www.CertKiller.com](http://www.CertKiller.com)  
[www.EnsurePass.com](http://www.EnsurePass.com)

[www.ExamCollection.com](http://www.ExamCollection.com)  
[www.ExactQuestions.com](http://www.ExactQuestions.com)  
[www.ExamSoon.com](http://www.ExamSoon.com)  
[www.PassGuide.com](http://www.PassGuide.com)  
[www.PassLeader.com](http://www.PassLeader.com)  
[www.TestKing.com](http://www.TestKing.com)

**Sections**

1. Deploy, manage, and maintain servers
2. Configure File and Print Services
3. Configure network services and access
4. Configure a Network Policy Server (NPS) infrastructure
5. Configure and manage Active Directory
6. Configure and manage Group Policy

## Exam A

### QUESTION 1

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

You need to identify the permissions of the mounted images in Install.wim.

What should you do?

- A. Run dism.exe and specify the /Get-MountedImageInfo 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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

In a previous version of this practice exam, the correct option listed was the parameter /Get-MountedWimInfo. However, that option is no longer an available DISM command-line parameter in Windows Server 2012 R2. Therefore, the answer was updated to provide the /Get-MountedImageInfo parameter option.

The **/Get-MountedImageInfo** parameter option lists the images that are currently mounted and information about the mounted image such as whether the image is valid, **read/write permissions**, mount location, mounted file path, and mounted image index.

<https://technet.microsoft.com/en-us/library/hh825258.aspx>

### QUESTION 2

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:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

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.

<https://technet.microsoft.com/en-us/library/cc749267.aspx>

### **QUESTION 3**

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:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

## Configuring event subscriptions

Event log forwarding enables you to centralize the collection and management of events from multiple computers. Rather than having to examine the event log of each computer by making a remote connection to that computer, event log forwarding enables you to do one of the following:

- Configure a central computer to collect specific events from source computers. Use this option in environments in which you need to consolidate events from only a small number of computers.
- Configure source computers to forward specific events to a collector computer. Use this option when you have a large number of computers from which you want to consolidate events. You configure this method using Group Policy.

Event log forwarding enables you to configure the specific events that are forwarded to the central computer. This enables the computer to forward important events. It isn't necessary to forward all events from the source computer. If you discover something that warrants further investigation from the forwarded traffic, you can log on to the original source computer and view all the events from that computer in a normal manner.

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

- **Configure Forwarder Resource Usage** This policy determines the maximum event forwarding rate in events per second. If this policy is not configured, events will be transmitted as soon as they are recorded.
- **Configure Target Subscription Manager** This policy enables you to set the location of the collector computer.

Both of these policies are located in the "Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding" node. When configuring the subscription, you must also specify the computer groups that hold the computer accounts of the computers that will be forwarding events to the collector. You do this in the Computer Groups dialog box.

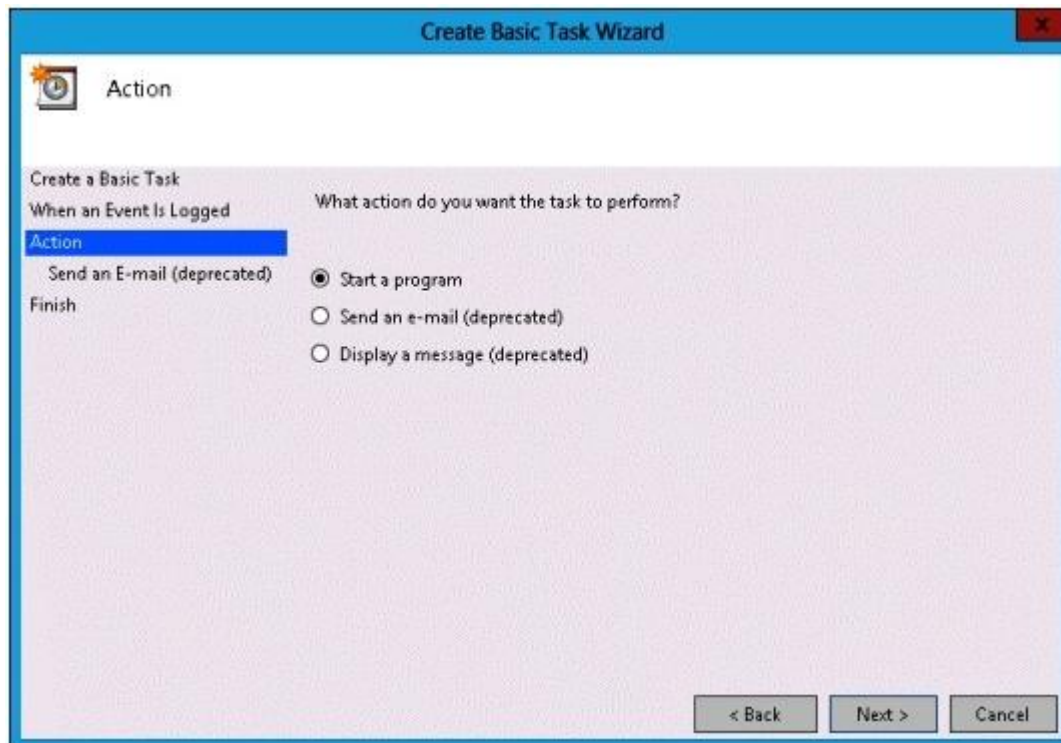
## Attaching event-driven tasks

Event Viewer enables you to attach tasks to specific events. A drawback to the process of creating event-driven tasks is that you need to have an example of the event that triggers the task already present in the event log. Events are triggered based on an event having the same log, source, and event ID.

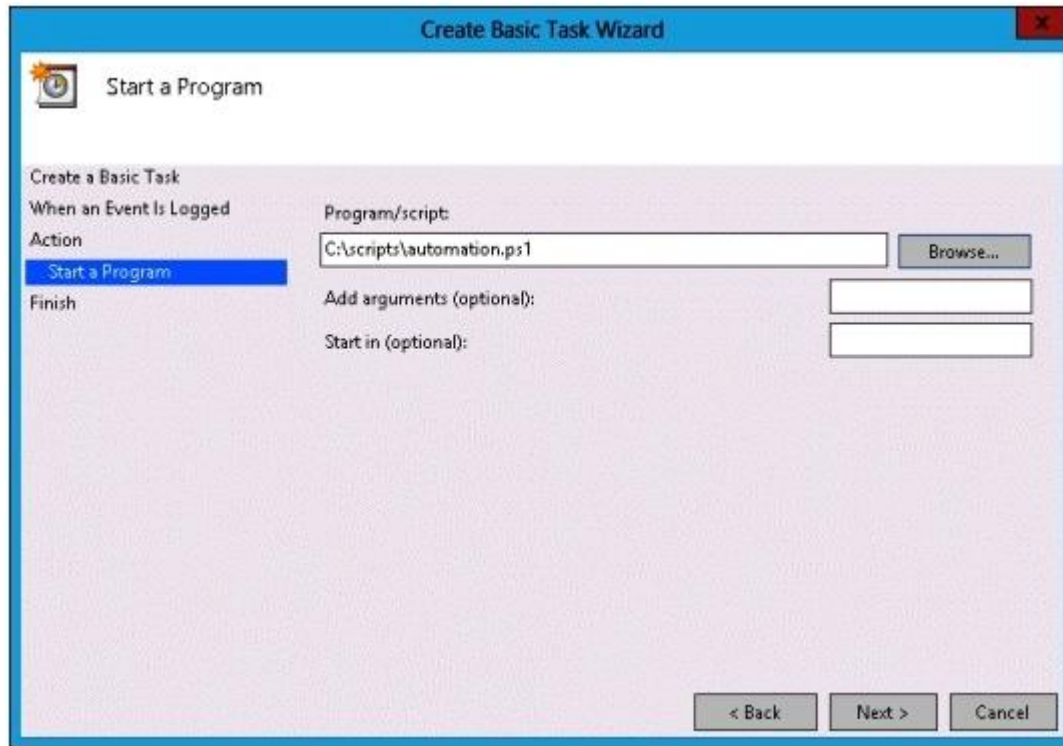
To attach a task to a specific event, perform the following steps:

1. Open Event Viewer. Locate and select the event upon which you want to base the new task.
2. On the Event Viewer Actions pane, click Attach Task To This Event. The Create Basic Task Wizard displays.
3. On the Create A Basic Task page, review the name of the task that you want to create. By default, the task is named after the event. Click Next.
4. On the When An Event is Logged page, review the information about the event. This will list the log from which the event originates, the source of the event, and the event ID. Click Next.

5. On the Action page, shown below, you can choose the task to perform. The Send An E-Mail and Display A Message tasks are deprecated, and you get an error if you try to create a task using these actions. Click Next.



6. On the Start A Program page, shown below, specify the program or script that should be automatically triggered as well as additional arguments.



7. After you complete task creation, you can modify the task to specify the security context under which the task executes. By default, event tasks run only when the user is signed on. You can configure the task to run whether the user is signed on or not.

<https://www.microsoftpressstore.com/articles/article.aspx?p=2217266&seqNum=2>

#### QUESTION 4

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.

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

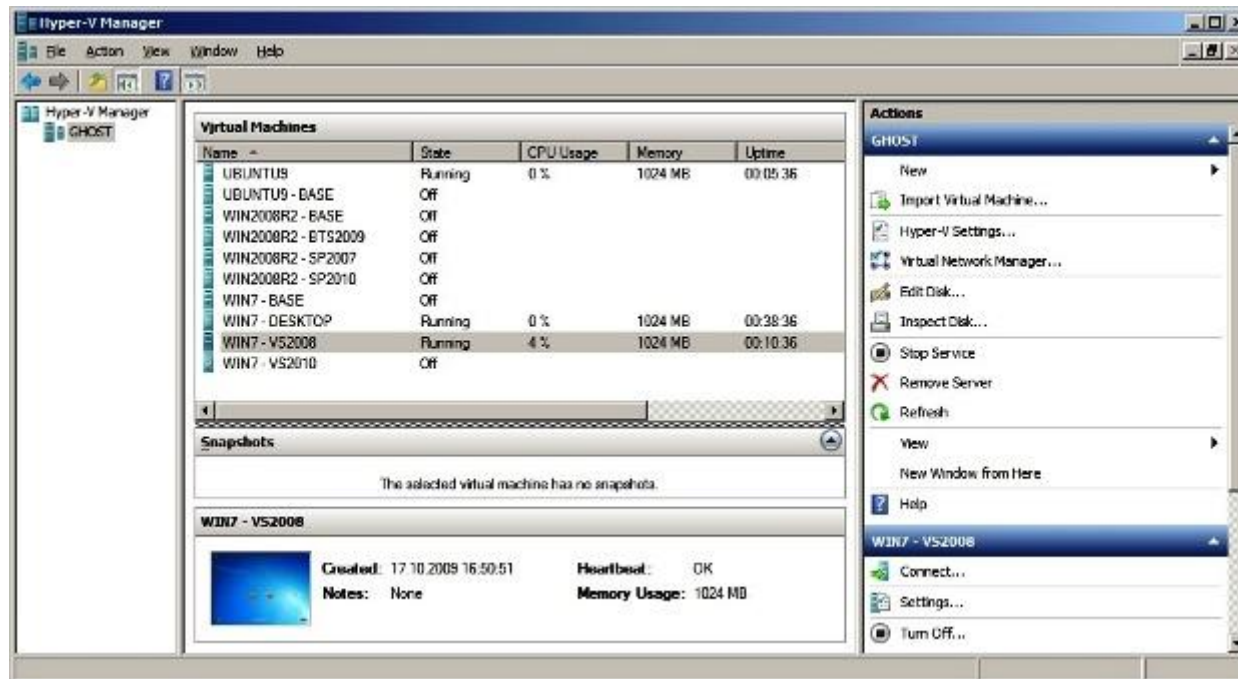
Which tool should you use on Hyperv1?

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

## D. Resource Monitor

**Correct Answer: C****Section: Deploy, manage, and maintain servers****Explanation****Explanation/Reference:**

The **Hyper-V Manager tool** is a Microsoft Management Console (MMC) snap-in that is used to manage the Hyper-V role and virtual machine configurations.



<https://technet.microsoft.com/en-us/library/dn632582.aspx>

**QUESTION 5**

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: B**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

### **Terminology**

**Logical Processor:** A thread of execution on a physical processing unit which can be a core or a thread on a symmetric multi-threaded (SMT) system.

**Virtual Processor:** A virtualized instance of a logical processor exposed to virtual machines.

<http://blogs.technet.com/b/matthts/archive/2012/10/14/windows-server-sockets-logical-processors-symmetric-multi-threading.aspx>

To view CPU usage information for virtual machines running on a server running Hyper-V, use Performance and Reliability Monitor to view the data from Hyper-V performance counters. To open Performance and Reliability Monitor, click **Start**, click **Run**, and then type **perfmon**.

The following performance counters provide information when viewed on the management operating system (the operating system that runs the Hyper-V role):

Hyper-V Hypervisor **Logical Processor** % Guest Run time: Identifies how much of the physical processor is being used to run the virtual machines. This counter does not identify the individual virtual machines or the amount consumed by each virtual machine.

Hyper-V Hypervisor **Virtual Processor** % Guest Run time: Identifies how much of the virtual processor is being consumed by a virtual machine.

**Note:** There is no direct mapping of virtual processor consumption to logical processor consumption because the virtual processors can be scheduled on any of the logical processors.

<https://technet.microsoft.com/en-us/library/cc742454.aspx>

**QUESTION 6**

Your network contains two servers named Server1 and Server2 that run windows Server 2012 R2. Server1 and Server2 have the Windows Server Update Services server role installed. Server1 synchronizes from Microsoft Update. Server2 is a Windows Server Update Services (WSUS) replica of Server1.

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

What should you do?

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

**Correct Answer: A**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

**To create a replica group for centralized management of multiple WSUS servers**

1. Install WSUS on a computer at a site where it can be managed by an administrator.
2. Install WSUS on a computer at a remote site, in the same way as in Step 1. When you have launched the Configuration Wizard, go to the **Choose Upstream Server** page, select the **Synchronize from another Windows Server Update Services server** check box, and then enter the name of the WSUS server from step 1.
3. If you are planning to use SSL for this connection, select the **Use SSL when synchronizing update information** check box.
4. Select the **This is a replica of the upstream server** check box.

5. Repeat steps 2, 3, and 4 as necessary to add additional WSUS servers to the replica group.

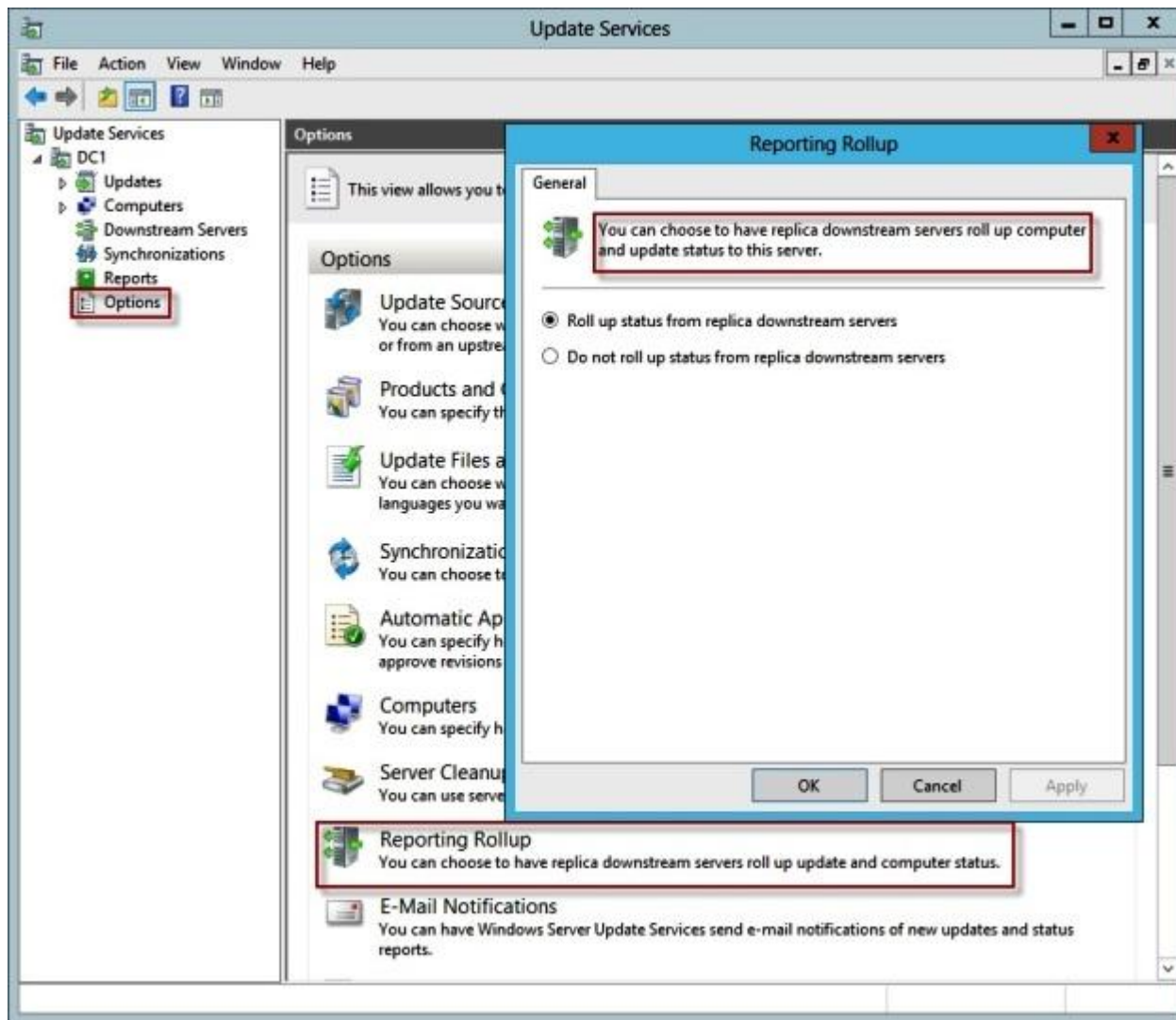
### Enable reporting rollup from replica servers

You can roll up computer and update status from replica servers to their upstream server.

#### To enable reporting rollup from replica servers

1. In the WSUS administration console on the upstream server, click **Options**, and then **Reporting Rollup**.
2. Select the **Roll up status from replica downstream servers** check box, and then click **OK**.





[https://technet.microsoft.com/en-us/library/cc708506\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc708506(v=ws.10).aspx)

#### QUESTION 7

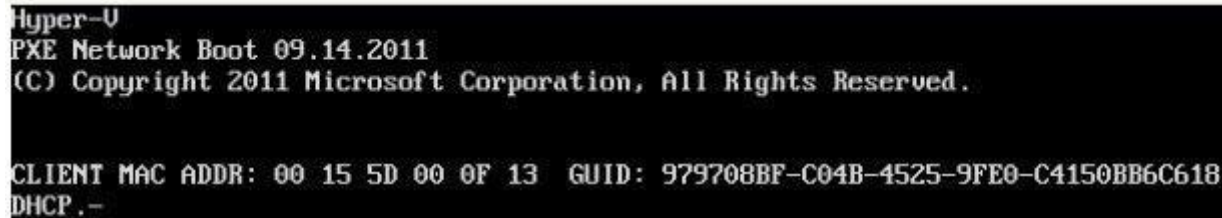
You manage a server that runs Windows Server 2012 R2. The server has the Windows Deployment Services server role installed.

You start a virtual machine named VM1 as shown in the exhibit. (Click the Exhibit button.)

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.)

**Exhibit:**



```
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.-
```

- A. 979708BFC04B45259FE0C4150BB6C618
- B. 979708BF-C04B-4525-9FE0-C4150BB6C618
- C. 00155D000F1300000000000000000000
- D. 00000000000000000000000000000000155D000F13
- E. 00000000-0000-0000-0000-C4150BB6C618

**Correct Answer:** BD

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

When a client computer attempts to boot from the network, limited data is transferred from the client to the server as part of the Pre-Boot Execution Environment (PXE) protocol. Windows Deployment Services can locate prestaged clients by using either a GUID (recommended) or a MAC address.

[https://technet.microsoft.com/en-us/library/cc772219\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772219(v=ws.10).aspx)

You can use Windows Deployment Services to link physical computers to computer account objects in Active Directory Domain Services (AD DS). This is called prestaging the client. Prestaged clients are also called known computers. Prestaging the client allows you to configure properties to control the installation for the client.

## To prestige client computers by using the Windows interface

1. On the server running Active Directory Users and Computers, open the Active Directory Users and Computers MMC snap-in (click **Start**, click **Run**, type **dsa.msc**, and then click **OK**).
2. In the console tree, right-click the organizational unit that will contain the new client computer.
3. Click **New**, and then click **Computer**.
4. Type the client computer name, click **Next**, and then click **This is a managed computer**.
5. In the text box, type the client computer's media access control (MAC) address preceded with twenty zeros or the globally unique identifier (GUID) in the format: {XXXXXXXX-XXXX-XXXX-XX-XXXXXXXXXXXX}.

[illegible]

6. Click **Next**, and click one of the following options to specify which server or servers will support this client computer:
  - **Any available remote installation server**
  - **The following remote installation server**
7. Click **Next**, and then click **Finish**.

<https://technet.microsoft.com/en-us/library/cc754469.aspx>

### QUESTION 8

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: Deploy, manage, and maintain servers**

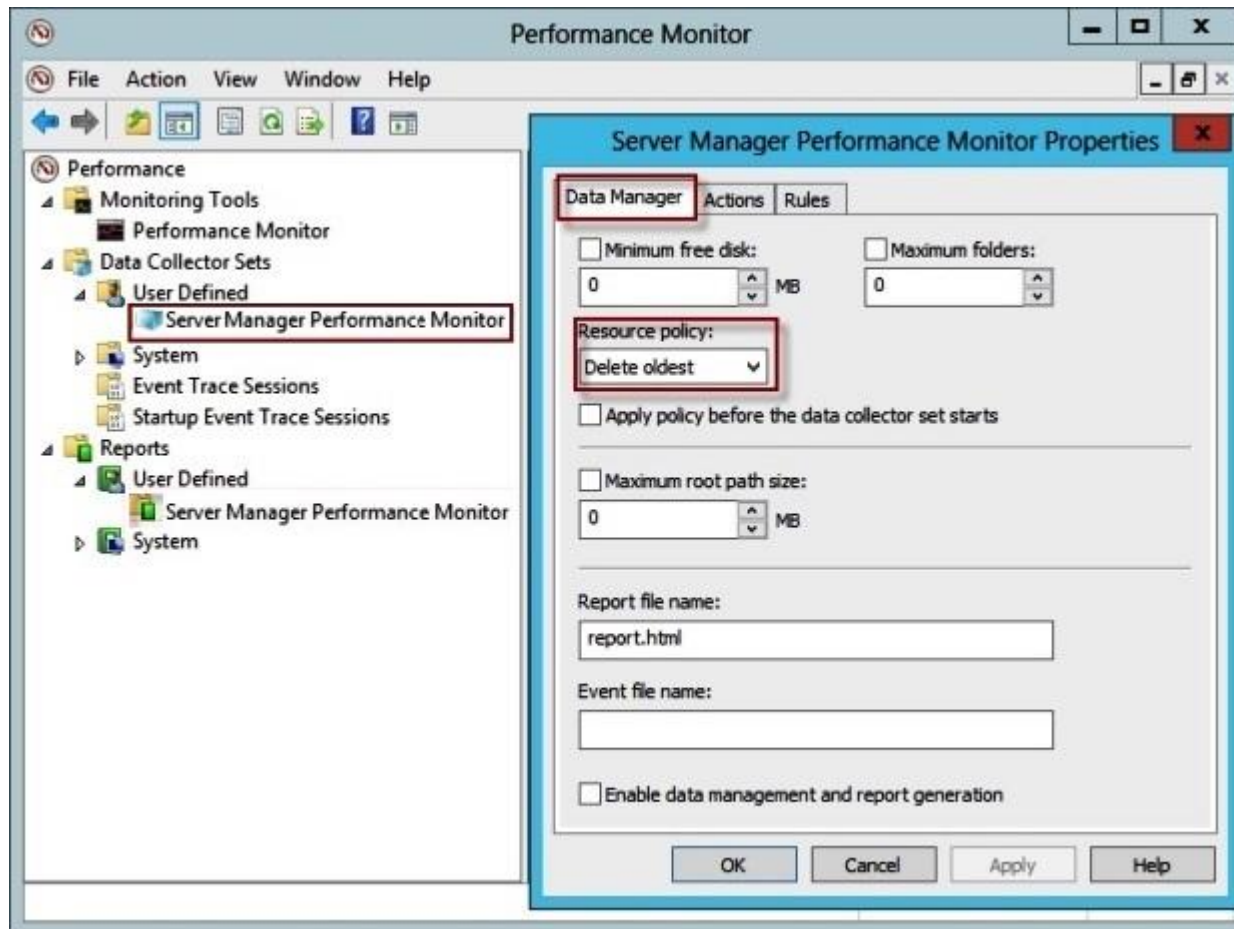
**Explanation**

**Explanation/Reference:**

Data Collector Sets create a raw log data file, in addition to optional report files. With Data Management, you can configure how log data, reports, and compressed data are stored for each Data Collector Set.

**To configure data management for a Data Collector Set**

1. In Windows Performance Monitor, expand Data Collector Sets and click **User Defined** .
2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click **Data Manager** .



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

When **Minimum free disk** or **Maximum folders** is selected, previous data will be deleted according to the **Resource policy** you choose (Delete largest or Delete oldest) when the limit is reached.

When **Apply policy before the data collector set starts** is selected, previous data will be deleted according to your selections before the data collector set creates its next log file.

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

4. Click the **Actions** tab. You can accept the default values or make changes. See the table below for details on each option.
5. When you have finished making your changes, click **OK**.

#### Data Manager Properties

Option	Definition
Minimum free disk	The amount of disk space that must be available on the drive where log data is stored. If selected, previous data will be deleted according to the Resource policy that you choose when the limit is reached.
Maximum folders	The number of subfolders that can be in the Data Collector Set data directory. If selected, previous data will be deleted according to the Resource policy that you choose when the limit is reached.
Resource policy	Specifies whether to delete the oldest or largest log file or directory when limits are reached.
Maximum root path size	The maximum size of the data directory for the Data Collector Set, including all subfolders. If selected, this maximum path size overrides the Minimum free disk and Maximum folders limits, and previous data will be deleted according to the Resource policy that you choose when the limit is reached.

#### Action Properties

Option	Definition
Age	The age in days or weeks of the data file. If the value is 0, the criterion is not used.
Size	The size in megabytes (MB) of the folder where log data is stored. If the value is 0, the criterion is not used.
Cab	A cabinet file, which is an archive file format. Cab files can be created from raw log data and extracted later when needed. Choose create or delete to take action based on the age or size criteria.
Data	Raw log data collected by the Data Collector Set. Log data can be deleted after a cab file is created to save disk space while still retaining a backup of the original data.
Report	The report file generated by Windows Performance Monitor from raw log data. Report files can be retained even after the raw data or cab file has been deleted.

<https://technet.microsoft.com/en-us/library/cc765998.aspx>

#### QUESTION 9

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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

You can gather information about all of the images in a WIM or VHD file by using the **/Get-ImageInfo** servicing command in DISM. You can also gather

information about a specific image in a WIM or VHD file, such as operating system, architecture, and settings, by specifying the name or index number of the image.

You can identify the images that are currently mounted on your computer, and you can list information about the mounted image such as read/write permissions, mount location, mounted file path, and mounted image index by using the **/Get-MountedImageInfo** servicing command.

<https://technet.microsoft.com/en-us/library/hh825042.aspx>

#### QUESTION 10

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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

Deployment Image Servicing and Management (DISM.exe) mounts a Windows image (.wim) file for servicing. The **/Apply-Image** option applies an image to a specified drive.

<https://technet.microsoft.com/en-us/library/hh825258.aspx>

#### QUESTION 11

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

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



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

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

**Correct Answer:** BC

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

### Configuring event subscriptions

Event log forwarding enables you to centralize the collection and management of events from multiple computers. Rather than having to examine the event log of each computer by making a remote connection to that computer, event log forwarding enables you to do one of the following:

- Configure a central computer to collect specific events from source computers. Use this option in environments in which you need to consolidate events from only a small number of computers.
- Configure source computers to forward specific events to a collector computer. Use this option when you have a large number of computers from which you want to consolidate events. You configure this method using Group Policy.

Event log forwarding enables you to configure the specific events that are forwarded to the central computer. This enables the computer to forward important events. It isn't necessary to forward all events from the source computer. If you discover something that warrants further investigation from the forwarded traffic, you can log on to the original source computer and view all the events from that computer in a normal manner.

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

- **Configure Forwarder Resource Usage** This policy determines the maximum event forwarding rate in events per second. If this policy is not configured, events will be transmitted as soon as they are recorded.
- **Configure Target Subscription Manager** This policy enables you to set the location of the collector computer.

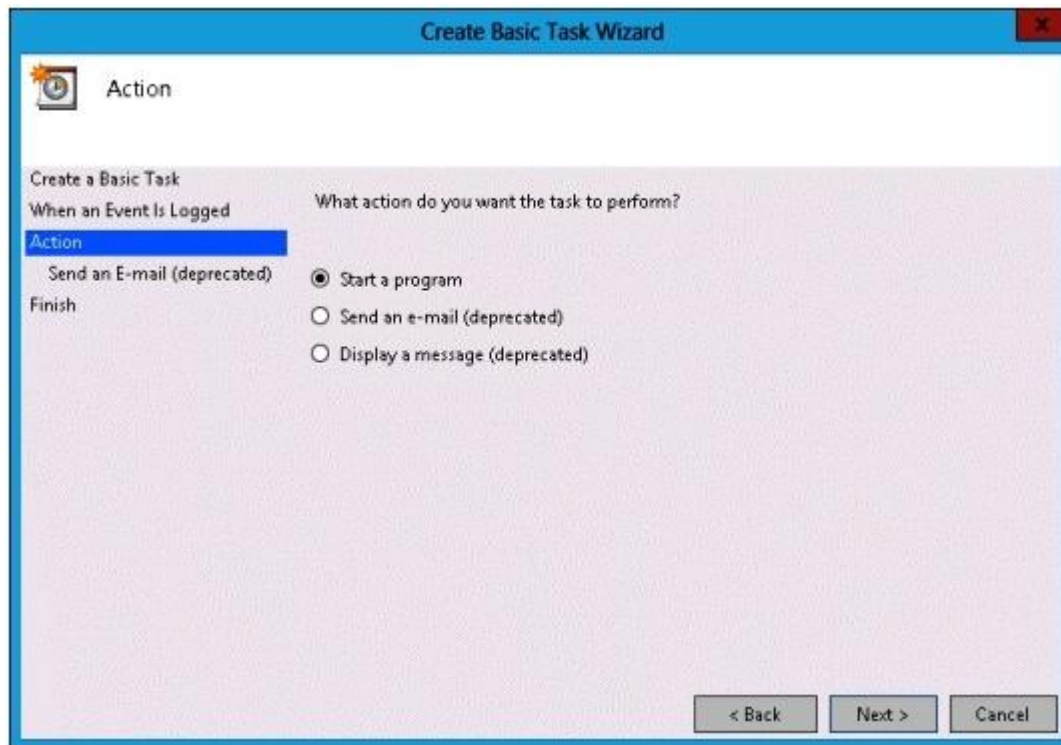
Both of these policies are located in the "Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding" node. When configuring the subscription, you must also specify the computer groups that hold the computer accounts of the computers that will be forwarding events to the collector. You do this in the Computer Groups dialog box.

### Attaching event-driven tasks

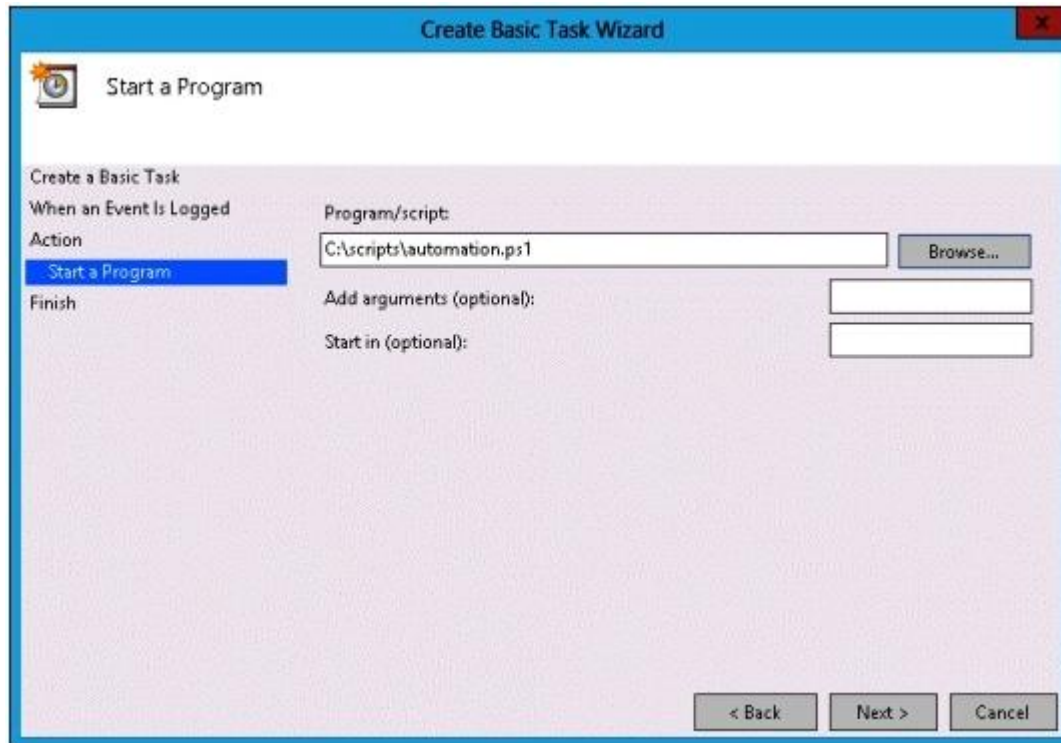
Event Viewer enables you to attach tasks to specific events. A drawback to the process of creating event-driven tasks is that you need to have an example of the event that triggers the task already present in the event log. Events are triggered based on an event having the same log, source, and event ID.

To attach a task to a specific event, perform the following steps:

1. Open Event Viewer. Locate and select the event upon which you want to base the new task.
2. On the Event Viewer Actions pane, click Attach Task To This Event. The Create Basic Task Wizard displays.
3. On the Create A Basic Task page, review the name of the task that you want to create. By default, the task is named after the event. Click Next.
4. On the When An Event Is Logged page, review the information about the event. This will list the log from which the event originates, the source of the event, and the event ID. Click Next.
5. On the Action page, shown below, you can choose the task to perform. The Send An E-Mail and Display A Message tasks are deprecated, and you get an error if you try to create a task using these actions. Click Next.



6. On the Start A Program page, shown below, specify the program or script that should be automatically triggered as well as additional arguments.



7. After you complete task creation, you can modify the task to specify the security context under which the task executes. By default, event tasks run only when the user is signed on. You can configure the task to run whether the user is signed on or not.

<https://www.microsoftpressstore.com/articles/article.aspx?p=2217266&seqNum=2>

## QUESTION 12

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

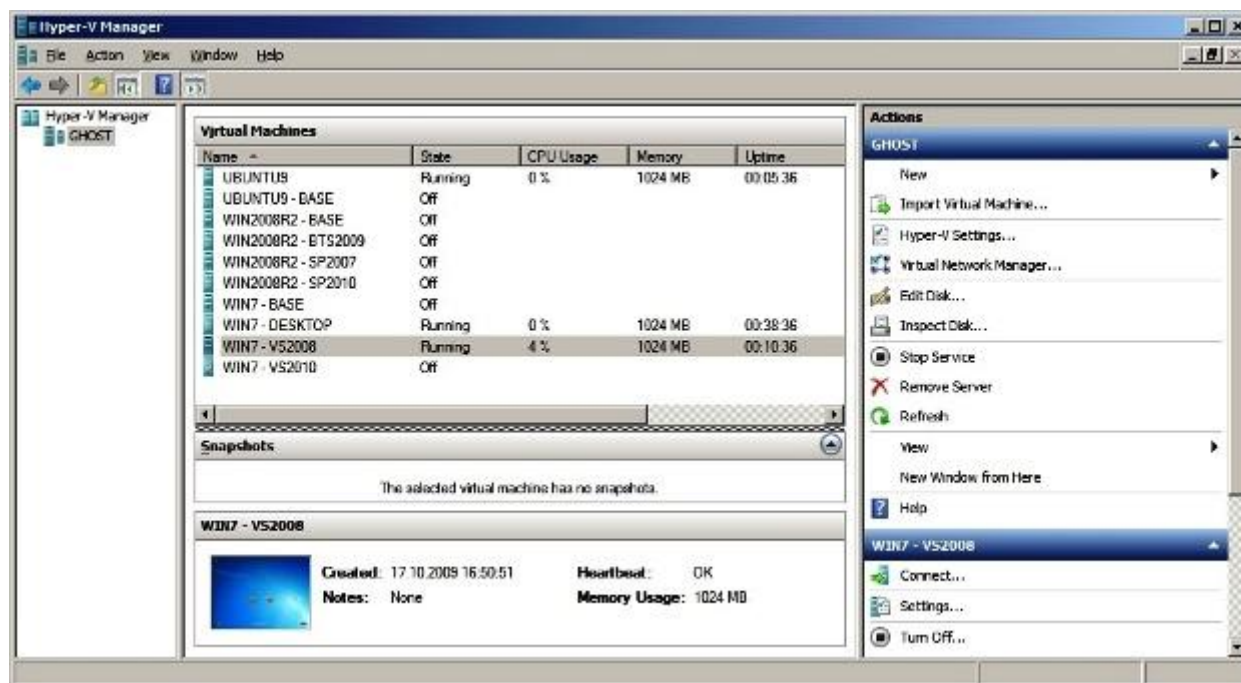
**Correct Answer:** A

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

The **Hyper-V Manager** tool is a Microsoft Management Console (MMC) snap-in that is used to manage the Hyper-V role and virtual machine configurations.



<https://technet.microsoft.com/en-us/library/dn632582.aspx>

### QUESTION 13

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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

**Local Storage Considerations**

[https://technet.microsoft.com/en-us/library/cc708480\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc708480(v=ws.10).aspx)

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.exe** tool (with the **movecontent** command) to move the update files to the new disk. For this procedure, see **Managing WSUS from the Command Line:** <https://technet.microsoft.com/en-us/library/cc720466>.

#### QUESTION 14

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 AD DS
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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

Network Unlock requires a supported version of Windows Server (Windows Server 2012 or Windows Server 2012 R2) running Windows Deployment Services (WDS) in the environment where the feature will be utilized. Configuration of the WDS installation is not required; however, the WDS service needs to be running on the server.

<https://technet.microsoft.com/en-us/library/jj574173.aspx>

The following are requirements for the default installation of the Windows Deployment Services role (both Deployment Server and Transport Server):

- Active Directory Domain Services (AD DS)
- DHCP
- DNS
- NTFS volume
- Local Administrators group credentials

<https://technet.microsoft.com/en-us/library/hh831764.aspx>

## QUESTION 15

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

You plan to apply several updates to Windows2012.vhd. You need to mount Wmdows2012.vhd to H:\Mount.

Which tool should you use?

- A. Mountvol
- B. Server Manager

- C. Diskpart
- D. Device Manager

**Correct Answer:** A

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

**Mountvol: Displays, Creates, and Deletes Volume Mount Points**

**Mountvol** is a utility that enumerates the volumes in your system. The table below describes the operations **Mountvol** can perform on a volume mount point.

Option	Description
Mountvol or Mountvol /?	Displays the name, globally unique identifier (GUID), and location of the volume.
Mountvol [drive:]path VolumeName	Creates a new volume mount point. Specify either a drive letter root directory or an existing empty NTFS directory as the source of the mount point and a volume name as the target.
Mountvol [drive:] path /D	Deletes an existing volume mount point.
Mountvol [drive:] path /L	Lists a volume name for a given volume mount point.

- 'Path' specifies the existing NTFS directory where the mount point will reside.
- 'VolumeName' specifies the name of the volume that is the mount point target.
- '/D' removes the volume mount point from the specified directory.
- '/L' Lists the mounted volume name for the specified directory.

<https://technet.microsoft.com/en-us/library/cc976820.aspx>

If you just want to mount/unmount a volume, **diskpart** can do everything that **mountvol** does. However, with **mountvol**, you can just run a simple command: `mountvol the_path_you_want_to_mount_the_volume the_volume_GUID` to mount a volume, while you have to perform many steps in **diskpart**.

Here is an example in **diskpart**:

1. `diskpart> list volume`
2. `diskpart> select volume_number`
3. `diskpart> assign mount=the_path_you_want_to_mount_the_volume`

<https://social.technet.microsoft.com/Forums/windowsserver/en-US/617e0542-03ba-468f-b13b-03f014e3daae/mountvolexe-vs-diskpart>

Bottom line: either **diskpart** or **mountvol** will satisfy the conditions of this question, but **mountvol** is the "best" answer because it solves the question with the least amount of administrative effort.

#### QUESTION 16

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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

#### **Create a Data Collector Set to Monitor Performance Counters**

You can create a custom Data Collector Set containing performance counters and configure alert activities based on the performance counters exceeding or dropping below limits you define.

After creating the Data Collector Set, you must configure the actions the system will take when the alert criteria are met.

Membership in the local **Performance Log Users** or **Administrators** group, or equivalent, is the minimum required to complete these procedures.



**To create a Data Collector Set to monitor Performance counters:**

1. In the Windows Performance Monitor navigation pane, expand **Data Collector Sets** , right-click **User Defined** , point to **New** , and click **Data Collector Set** . The Create new Data Collector Set Wizard starts.
2. Enter a name for your Data Collector Set.
3. Select the **Create manually** option and click **Next**.
4. Select the **Performance Counter Alert** option and click **Next**.
5. Click **Add** to open the **Add Counters** dialog box. When you are finished adding counters, click **OK** to return to the wizard.
6. Define alerts based on the values of performance counters you have selected.
  1. From the list of Performance counters, select the counter to monitor and trigger an alert.
  2. From the **Alert when** drop-down, choose whether to alert when the performance counter value is above or below the limit.
  3. In the **Limit** box, enter the threshold value.
7. When you are finished defining alerts, click **Next** to continue configuration or **Finish** to exit and save the current configuration.
8. After clicking **Next** , you can configure the Data Collector Set to run as a particular user. Click the **Change** button to enter the user name and password for a different user than the default listed.
9. Click **Finish** to return to Windows Performance Monitor.
  1. To view the properties of the Data Collector Set or make additional changes, select **Open properties for this data collector set**.
  2. To start the Data Collector Set immediately (and begin saving data to the location specified in Step 8), select **Start this data collector set now**.
  3. To save the Data Collector Set without starting collection, select **Save and close**.

<https://technet.microsoft.com/en-us/library/cc722414.aspx>

**QUESTION 17**

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:** CD

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

## Creating Data Collector Sets

A Data Collector Set is the building block of performance monitoring and reporting in Windows Performance Monitor. It organizes multiple data collection points into a single component that can be used to review or log performance. A Data Collector Set can be created and then recorded individually, grouped with other Data Collector Set and incorporated into logs, viewed in Performance Monitor, configured to generate alerts when thresholds are reached, or used by other non-Microsoft applications. It can be associated with rules of scheduling for data collection at specific times. Windows Management Interface (WMI) tasks can be configured to run upon the completion of Data Collector Set collection.

Data Collector Sets can contain the following types of data collectors:

- Performance counters
- Event trace data
- System configuration information (registry key values)

<https://technet.microsoft.com/en-us/library/cc749337.aspx>

## Monitoring Domain Controller Performance

- **Monitoring Active Directory replication**

Besides monitoring the domain controllers themselves, you should also monitor replication traffic between them. Problems with the network can interfere with replication. Network problems can cause replication to slow down or stop, resulting in backlogs of replication data and inconsistency among domain controllers. Regular, ongoing monitoring helps you detect problems that might occur in your Active Directory replication environment. It also gives you the opportunity to correct these problems before they affect the directory or the users.

[https://technet.microsoft.com/en-us/library/dd736504\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd736504(v=ws.10).aspx)

## QUESTION 18

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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

### **Boot Image and Install Image Priorities**

When you have multiple boot or install images available to client computers, clients will be presented with a boot and an install menu that displays the selection of images to choose from.

Windows Deployment Services allows you to set priorities to control the order that both boot and install image listings are presented to clients. This ability is integrated directly into Windows Deployment Services.

### **Steps for configuring the boot menu**

#### **To configure menu order for boot images**

1. Open the Windows Deployment Services MMC snap-in.
2. Click the **Boot Images** node. You will see your boot images appear in the right hand side of your Windows Deployment Services MMC snap-in.
3. Right-click your desired boot image from the right-hand side of your Windows Deployment Services MMC snap-in. Click **Properties**.
4. In the **Image Properties** dialog, on the **General** tab, enter in your desired priority into the Priority text box. The items that appear first on your install image menu are the ones with the lowest value.
5. Click **OK**.

#### **To configure menu order for install images**

1. Open the Windows Deployment Services MMC snap-in.
2. Double-click the **Install Images** node. You will see your image group (or image groups) appear as a sub menu item. They will also appear in the right hand side of your Windows Deployment Services MMC snap-in.

3. Click your desired **Image Group**.
4. Right-click your desired image within your image group from the right-hand side of your Windows Deployment Services MMC snap-in. Click **Properties**.
5. On the **Image Properties** dialog, in the **General** tab, enter in your desired priority into the **Priority** text box. The items that appear first on your install image menu are the ones with the lowest value.
6. Click **OK**.

When you have completed this procedure and you perform a PXE boot on a client computer, a boot or install menu with the menu order you set using priorities will appear. (if those images apply to that computer).

Priorities are pre-populated with a default value that lets you place images higher or lower on the list. The items that appear first on the list are the ones with the lowest value.

<https://technet.microsoft.com/en-us/library/jj648426.aspx>

#### QUESTION 19

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: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

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.

<https://technet.microsoft.com/en-us/library/hh847288.aspx>

#### **QUESTION 20**

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:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

#### **Configure SSL on the WSUS server**

WSUS requires two ports for SSL: one port that uses HTTPS to send encrypted metadata, and one port that uses HTTP to send updates. When you configure WSUS to use SSL, consider the following:

- You cannot configure the whole WSUS website to require SSL because all traffic to the WSUS site would have to be encrypted. WSUS encrypts update metadata only. If a computer attempts to retrieve update files on the HTTPS port, the transfer will fail.
- The certificate of the certification authority (CA) must be imported into the local computer Trusted Root CA store, or the Windows Server Update Service Trusted Root CA store on downstream WSUS servers. If the certificate is only imported to the Local User Trusted Root CA store, the downstream WSUS server will not be authenticated on the upstream server.
- You must import the certificate to all computers that will communicate with the WSUS server. This includes all client computers, downstream servers, and computers that run the WSUS Administration Console. The certificate should be imported into the local computer Trusted Root CA store or into the Windows Server Update Service Trusted Root CA store.
- You can use any port for SSL. However, the port that you set up for SSL also determines the port that WSUS uses to send clear HTTP traffic. Consider the following examples:
  - If you use the industry standard port of 443 for HTTPS traffic, WSUS uses the industry standard port 80 for clear HTTP traffic.

- If you use any port other than 443 for HTTPS traffic, WSUS will send clear HTTP traffic over the port that numerically comes before the port for HTTPS. For example, if you use port 8531 for HTTPS, WSUS will use port 8530 for HTTP.

- You must re-initialize *ClientServicingProxy* if the server name, SSL configuration, or port number are changed.

## To configure SSL on the WSUS root server

1. Log on to the WSUS server by using an account that is a member of the WSUS Administrators group or the local Administrators group.
2. Go to **Start**, type **CMD**, right-click **Command Prompt**, and then click **Run as administrator**.
3. Navigate to the *%ProgramFiles%\Update Services\Tools\* folder.
4. In the Command Prompt window, type the following command:

```
Wsusutil configuressl certificateName
```

(Where *certificateName* is the DNS name of the WSUS server.)

## Associate a server certificate with the SSL port/protocol binding in IIS

In Server 2012 R2 you need to launch IIS manager and go to the root of the WSUS site. Choose Edit Bindings and edit the HTTPS binding. If you have a valid certificate you'll be able to select it from the drop down list in here.

[https://technet.microsoft.com/en-us/library/hh852346.aspx#bkmk\\_3\\_5\\_ConfigSSL](https://technet.microsoft.com/en-us/library/hh852346.aspx#bkmk_3_5_ConfigSSL)

## QUESTION 21

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:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

#### **Total Processor % Interrupt Time (Collection Rule)**

This rule collects the Total Instance of the % Interrupt Time performance counter. By default, a sample is taken every 5 minutes. % Interrupt Time monitors the overall average processor utilization that occurred in Interrupt mode. Only interrupt service routines (ISRs), which are device driver

functions run in Interrupt mode. Excessive % Interrupt Time can identify that a device is malfunctioning and serves as a secondary indicator that a device might be contributing to a processor bottleneck.

<https://technet.microsoft.com/en-us/library/dd279711.aspx>

This monitor is disabled based on customer feedback. A majority of our customers do not monitor total percentage interrupt time performance information by default.

Enable this monitor if total percentage interrupt time performance monitoring is required.

<https://technet.microsoft.com/en-us/library/hh508967.aspx>

## QUESTION 22

Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2. Server1 and Server2 are nodes in a Hyper-V cluster named Cluster1. Cluster1 hosts 10 virtual machines. All of the virtual machines run Windows Server 2012 R2 and are members of the domain.

You need to ensure that the first time a service named Service1 fails on a virtual machine, the virtual machine is moved to a different node. You configure Service1 to be monitored from Failover Cluster Manager.

What should you configure on the virtual machine?

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

**Correct Answer: C**

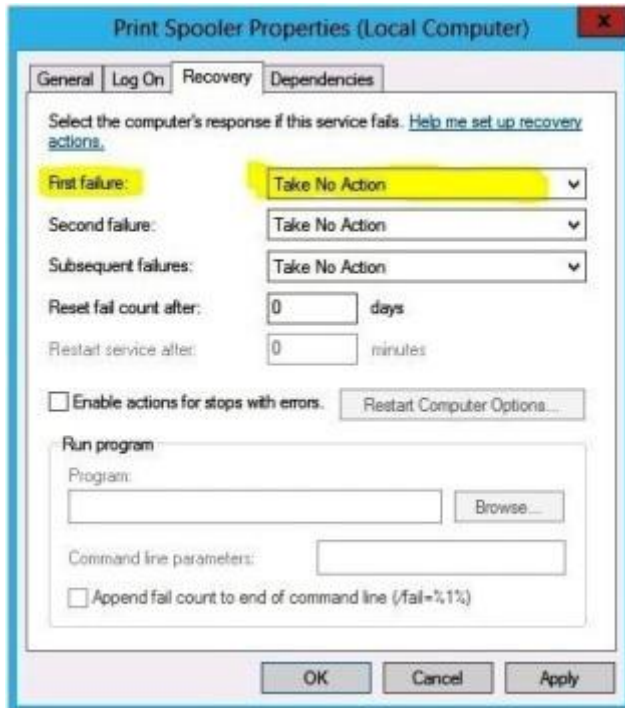
**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

When a monitored service encounters an unexpected failure, the sequence of recovery actions is determined by the Recovery actions on failure for the service. These recovery actions can be viewed and configured using Service Control Manager inside the guest. [If the properties of the service are set to 'Take No Action'] the service control manager will take no action and defer recovery actions to the cluster service running in the host.





<http://blogs.msdn.com/b/clustering/archive/2012/04/18/10295158.aspx>

### QUESTION 23

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: Deploy, manage, and maintain servers**  
**Explanation**

**Explanation/Reference:**

**Create a Data Collector Set to Monitor Performance Counters**

You can create a custom Data Collector Set containing performance counters and configure alert activities based on the performance counters exceeding or dropping below limits you define.

After creating the Data Collector Set, you must configure the actions the system will take when the alert criteria are met.

Membership in the local **Performance Log Users** or **Administrators** group, or equivalent, is the minimum required to complete these procedures.

**To create a Data Collector Set to monitor Performance counters:**

1. In the Windows Performance Monitor navigation pane, expand **Data Collector Sets** , right-click **User Defined** , point to **New** , and click **Data Collector Set** . The Create new Data Collector Set Wizard starts.
2. Enter a name for your Data Collector Set.
3. Select the **Create manually** option and click **Next**.
4. Select the **Performance Counter Alert** option and click **Next**.
5. Click **Add** to open the **Add Counters** dialog box. When you are finished adding counters, click **OK** to return to the wizard.
6. Define alerts based on the values of performance counters you have selected.
  1. From the list of Performance counters, select the counter to monitor and trigger an alert.
  2. From the **Alert when** drop-down, choose whether to alert when the performance counter value is above or below the limit.
  3. In the **Limit** box, enter the threshold value.
7. When you are finished defining alerts, click **Next** to continue configuration or **Finish** to exit and save the current configuration.
8. After clicking **Next** , you can configure the Data Collector Set to run as a particular user. Click the **Change** button to enter the user name and password for a different user than the default listed.
9. Click **Finish** to return to Windows Performance Monitor.
  1. To view the properties of the Data Collector Set or make additional changes, select **Open properties for this data collector set** . For more information about the properties of the Data Collector Set, see Data Collector Set Properties.
  2. To start the Data Collector Set immediately (and begin saving data to the location specified in Step 8), select **Start this data collector set now**.
  3. To save the Data Collector Set without starting collection, select **Save and close**.

<https://technet.microsoft.com/en-us/library/cc722414.aspx>

#### QUESTION 24

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 Update 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**

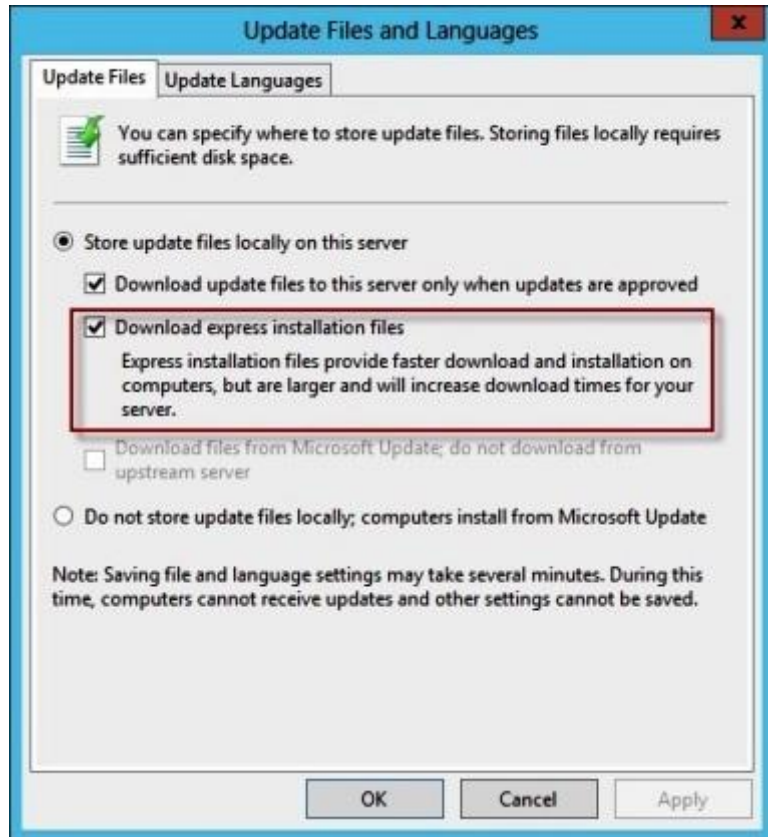
**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

**To specify whether express installation files are downloaded during synchronization**

1. In the left pane of the WSUS Administration console, click **Options**.
2. In **Update Files and Languages**, click the **Update Files** tab.
3. 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.



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

#### QUESTION 25

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2 and a server named Server2 that has the File Services server role installed.

You install the Windows Deployment Services server role on Server1. You plan to use Server2 as a reference computer. You need to create an image of Server2 by using Windows Deployment Services.

Which type of image should you add to Server1 first?

- A. Boot
- B. Discovery

- C. Install
- D. Capture

**Correct Answer:** A

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

You must add at least one boot image and one install image before you will be able to boot to the Windows Deployment Services server and install an image.

**Boot images.** Boot images are Windows PE images that you boot a client computer into to perform an operating system installation. In most scenarios, you should use the Boot.wim file from the installation media (in the \Sources folder). The Boot.wim file contains Windows PE and the Windows Deployment Services client.

**Install images.** Install images are the operating system images that you deploy to the client computer. You can also use the Install.wim file from the installation media (in the \Sources folder), or you can create your own install image.

<https://technet.microsoft.com/en-us/library/jj648426.aspx>

#### **QUESTION 26**

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

On Server1, you configure a custom Data Collector Set (DCS) named DCS1. You need to ensure that all performance log data that is older than 30 days is deleted automatically.

What should you configure?

- A. a File Server Resource Manager (FSRM) quota on the %Systemdrive%\PerfLogs folder
- B. a schedule for DCS1
- C. the Data Manager settings of DCS1
- D. a File Server Resource Manager (FSRM) file screen on the %Systemdrive%\PerfLogs folder

**Correct Answer:** C

**Section:** Deploy, manage, and maintain servers

**Explanation**

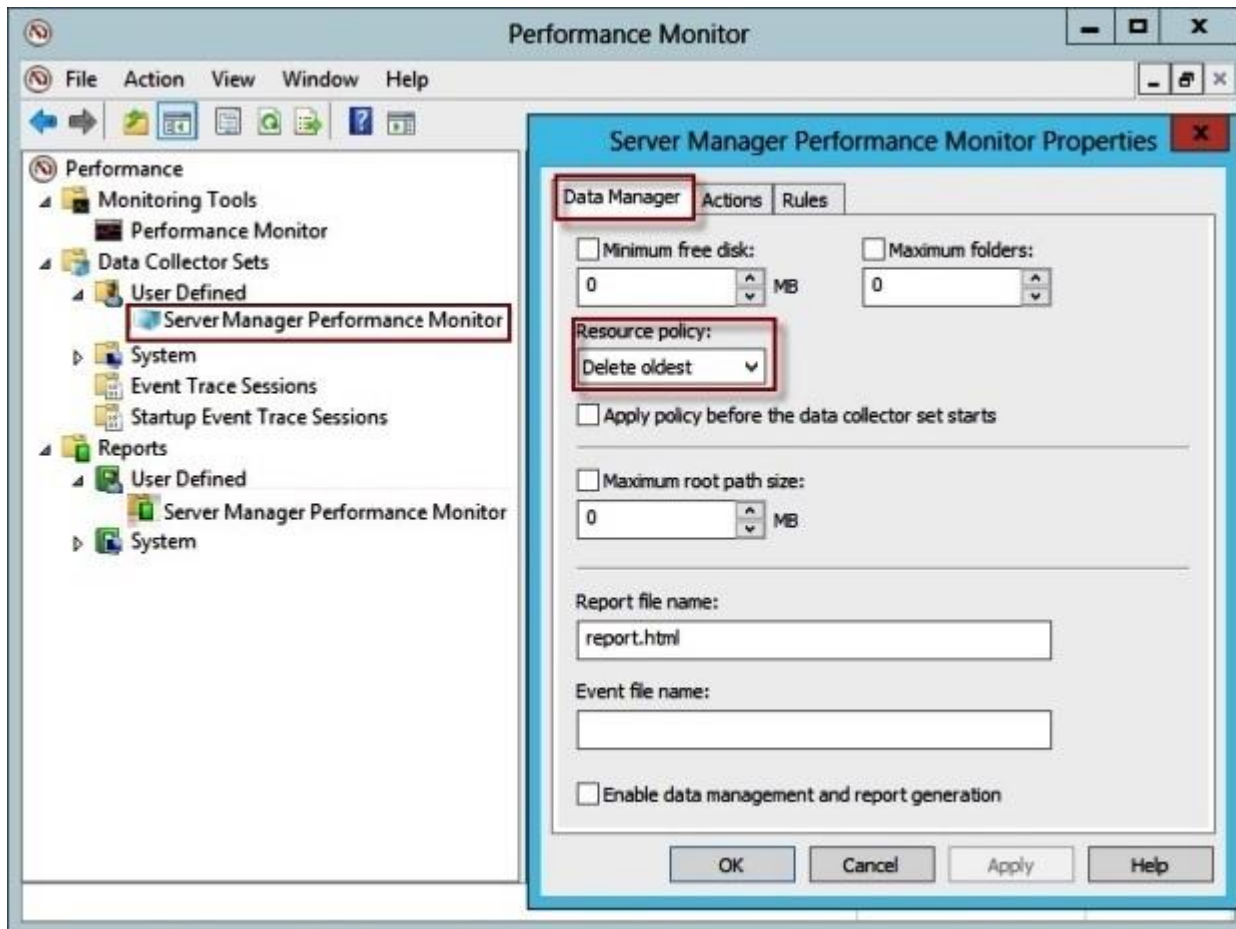
**Explanation/Reference:**

Data Collector Sets create a raw log data file, in addition to optional report files. With Data Management, you can configure how log data, reports, and

compressed data are stored for each Data Collector Set.

### To configure data management for a Data Collector Set

1. In Windows Performance Monitor, expand Data Collector Sets and click **User Defined**.
2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click **Data Manager**.



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

When **Minimum free disk** or **Maximum folders** is selected, previous data will be deleted according to the **Resource policy** you choose (Delete largest or Delete oldest) when the limit is reached.

When **Apply policy before the data collector set starts** is selected, previous data will be deleted according to your selections before the data collector set creates its next log file.

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

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

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

#### Data Manager Properties

Option	Definition
Minimum free disk	The amount of disk space that must be available on the drive where log data is stored. If selected, previous data will be deleted according to the Resource policy that you choose when the limit is reached.
Maximum folders	The number of subfolders that can be in the Data Collector Set data directory. If selected, previous data will be deleted according to the Resource policy that you choose when the limit is reached.
Resource policy	Specifies whether to delete the oldest or largest log file or directory when limits are reached.
Maximum root path size	The maximum size of the data directory for the Data Collector Set, including all subfolders. If selected, this maximum path size overrides the Minimum free disk and Maximum folders limits, and previous data will be deleted according to the Resource policy that you choose when the limit is reached.

#### Action Properties

Option	Definition
Age	The age in days or weeks of the data file. If the value is 0, the criterion is not used.
Size	The size in megabytes (MB) of the folder where log data is stored. If the value is 0, the criterion is not used.
Cab	A cabinet file, which is an archive file format. Cab files can be created from raw log data and extracted later when needed. Choose create or delete to take action based on the age or size criteria.
Data	Raw log data collected by the Data Collector Set. Log data can be deleted after a cab file is created to save disk space while still retaining a backup of the original data.
Report	The report file generated by Windows Performance Monitor from raw log data. Report files can be retained even after the raw data or cab file has been deleted.

<https://technet.microsoft.com/en-us/library/cc765998.aspx>

#### QUESTION 27

Your network contains an Active Directory domain named contoso.com. All client computers connect to the Internet by using a server that has Microsoft Forefront Threat Management Gateway (TMG) installed.

You deploy a server named Server1 that runs Windows Server 2012 R2. You install the Windows Server Update Services server role on Server1. From the Windows Server Update Services Configuration Wizard, you click **Start Connecting** and you receive an HTTP error message. You need to configure Server1 to download Windows updates from the Internet.

What should you do?

- A. From the Update Services console, modify the Synchronization Schedule options.
- B. From Windows Internet Explorer, modify the Connections settings.
- C. From Windows Internet Explorer, modify the Security settings.
- D. From the Update Services console, modify the Update Source and Proxy Server options.

**Correct Answer: D**

**Section: Deploy, manage, and maintain servers**

**Explanation**



## Explanation/Reference:

The WSUS Server Configuration Wizard allows you to configure the following areas:

### Choose the upstream server

1. On the **Choose Upstream Server** page, select the source from which this server will get its updates (Microsoft Update or another WSUS server).
2. If you choose to synchronize from Microsoft Update, you are finished with this page. Click **Next**, or select **Specify Proxy Server** from the left pane.
3. If you choose to synchronize from another WSUS server, specify the server name and the port on which this server will communicate with the upstream server.
4. To use SSL, check the **Use SSL when synchronizing update information** check box. In that case the servers will use port 443 for synchronization. (You should make sure that both this server and the upstream server support SSL.)
5. If this is a replica server, check the **This is a replica of the upstream server** check box. (For more information about replica versus autonomous downstream servers, see the [Choose a WSUS Management Style](#) section earlier in this document.)
6. At this point you are finished with upstream server configuration. Click **Next**, or select **Specify proxy server** from the left pane.

### Specify the proxy server

1. If you are setting up the root WSUS server that connects to Microsoft Update, you may wish to configure it to use a proxy server. On the **Specify Proxy Server** page of the configuration wizard, select the **Use a proxy server when synchronizing** check box, and then type the proxy server name and port number (port 80 by default) in the corresponding boxes.
2. If you want to connect to the proxy server by using specific user credentials, select the **Use user credentials to connect to the proxy server** check box, and then type the user name, domain, and password of the user in the corresponding boxes. If you want to enable basic authentication for the user connecting to the proxy server, select the **Allow basic authentication (password is sent in cleartext)** check box.
3. At this point you are finished with proxy server configuration. Click **Next** to go to the **Connect to Upstream Server** page.

### Connect to the upstream server

1. Click the **Start Connecting** button, which will save and upload your settings and then download information about available updates, products, and classifications. This initial connection will take only a few minutes.
2. While the connection is taking place, the **Stop Connecting** button will be available. If there are problems with the connection, stop the connection, fix the problems, and restart the connection.
3. After the connection has completed successfully, click **Next**. If you have chosen to store updates locally, you will go to the **Choose Languages** page, or you can select a different page from the left pane.

**Note:** If the connection to your upstream WSUS server (either Microsoft Update or an intranet WSUS server) fails, you will see a message at the bottom of the screen. Typically it will say something like "An HTTP error occurred." For more information, click the Details link.

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

Microsoft Forefront Threat Management Gateway (TMG) is irrelevant to this question. The product has not been available for purchase since 1 December 2012. Mainstream support ceases on 14 April 2015.

## QUESTION 28

You have Site1 with 400 desktop computers and Site2 with 150 desktop computers. You have a WSUS Server to deploy updates for both sites.

You need to make sure that all computers in the same site will have the same updates.

What should you configure?

- A. Computer Groups
- B. Security Groups
- C. Synchronization Options
- D. Classifications

**Correct Answer:** A

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

Windows Server Update Services (WSUS) 3.0 SP2 enables you to manage the entire process of updating your computers, including manually and automatically determining which updates they need and receive, specifying when the updates are installed, and monitoring the status of update deployments on your computers.

WSUS also allows you to target updates to groups of client computers. This capability can help you ensure that specific computers get the right updates at the most convenient times on an ongoing basis. For example, if all the computers in one department of your organization (such as all computers in the Accounting team) have a specific configuration, you can determine what updates those computers get, at what time, and then use the WSUS reporting features to evaluate the success of the update activity for that computer group.

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

## QUESTION 29

You have a WDS server named Server1 on Windows Server 2012 R2.

You need to automate the WDS deployment.

Which Tab should you configure?

- A. Boot Properties
- B. Client Properties
- C. Network Settings
- D. PXE Response Settings

**Correct Answer:** B

**Section: Deploy, manage, and maintain servers**  
**Explanation**

**Explanation/Reference:**

**Steps for performing an unattended installation**

To automate the installation, create the appropriate unattend file depending on whether you are configuring the Windows Deployment Services screens or Windows Setup. We recommend that you use Windows System Image Manager (included as part of the Windows Assessment and Deployment Kit) to author the unattend files. The Windows System Image Manager (Windows SIM) creates and manages unattended Windows Setup answer files in a graphical user interface (GUI).

You will then need to copy the unattend file to the appropriate location, and assign it for use. You can assign it at the server level or the client level. The server level assignment can further be broken down by architecture, enabling you to have different settings for x86-based and x64-based clients. Assignment at the client level overrides the server-level settings.

**To associate a client unattend file by architecture**

1. Create an Unattend.xml file with settings applicable to Windows Deployment Services.
2. Copy the client unattend file to a folder in the **RemoteInstall** folder. For example: **RemoteInstall\WDSCClientUnattend**.
3. Open the Windows Deployment Services MMC snap-in, right-click the server that contains the image that you want to associate the unattend file with, and then click **Properties**.
4. On the **Client** tab, select **Enable unattended installation**, browse to the appropriate unattend file, and then click **Open**.
5. Click **OK** to close the **Properties** page.

<https://technet.microsoft.com/en-us/library/jj648426.aspx>

**QUESTION 30**

You want to change the memory of a virtual machine that is currently powered on.

What do you need to do?

- A. Shut down the virtual machine, use the virtual machine's settings to change the memory, and start it again.
- B. Use the virtual machine's settings to change the memory.
- C. Pause the virtual machine, use the virtual machine's settings to change the memory, and resume it.
- D. Save the virtual machine, use the virtual machine's settings to change the memory, and resume it.

**Correct Answer:** A

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

**To configure memory or processors for a virtual machine**

1. Open Hyper-V Manager. Click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the results pane, under **Virtual Machines**, select the virtual machine that you want to configure.
3. In the **Action** pane, under the virtual machine name, click **Settings**. Then, in the navigation pane, click the appropriate hardware setting as described in the following steps.
4. To configure the memory, click **Memory**. On the **Memory** page, specify the new amount of memory.
5. To configure the processor, click **Processor**. If multiple processors are supported by the guest operating system, specify the number of processors to assign to the virtual machine. Then click **OK**.

**Additional considerations**

- By default, membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure. However, an administrator can use Authorization Manager to modify the authorization policy so that a user or group of users can complete this procedure.
- The virtual machine must be turned off before you can modify the memory or processor settings.

<https://technet.microsoft.com/en-us/library/cc742470.aspx>

### **QUESTION 31**

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:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

## Local Storage Considerations

[https://technet.microsoft.com/en-us/library/cc708480\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc708480(v=ws.10).aspx)

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.exe** tool (with the **movecontent** command) to move the update files to the new disk. For this procedure, see **Managing WSUS from the Command Line:** <https://technet.microsoft.com/en-us/library/cc720466>.

## QUESTION 32

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

You have a desktop computer that has the following configuration:

- Computer name: Computer1
- Operating system: Windows 8
- MAC address: 20-CF-30-65-D0-87
- GUID: 979708BF-C04B-4525-9FE0-C4150BB6C618

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

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

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

**Correct Answer:** CD

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

When a client computer attempts to boot from the network, limited data is transferred from the client to the server as part of the Pre-Boot Execution

[https://technet.microsoft.com/en-us/library/cc772219\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772219(v=ws.10).aspx)

## To prestige client computers by using the Windows interface

- [illegible]

- www.vceplus.com - Website designed to help IT pros advance their careers - Born to Learn

7. Click **Next**, and then click **Finish**.

<https://technet.microsoft.com/en-us/library/cc754469.aspx>

### QUESTION 33

You have five servers that run Windows Server 2012 R2. The servers have the Failover Clustering feature installed.

You deploy a new cluster named Cluster1. Cluster1 is configured as shown in the following table.

Site name	Server name
Site1	Server1 Server2 Server3
Site2	Server4 Server5

Server1, Server2, and Server3 are configured as the preferred owners of the cluster roles. Dynamic quorum management is disabled.

You plan to perform hardware maintenance on Server3. You need to ensure that if the WAN link between Site1 and Site2 fails while you are performing maintenance on Servers, the cluster resource will remain available in Site1.

What should you do?

- A. Add a file share witness in Site1
- B. Remove the node vote for Server3
- C. Remove the node vote for Server4 and Server5
- D. Enable dynamic quorum management

**Correct Answer: C**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

In Windows Server 2012, as an advanced quorum configuration option, you can choose to assign or remove quorum votes on a per-node basis. By default, all nodes are assigned votes. Regardless of vote assignment, all nodes continue to function in the cluster, receive cluster database updates, and can host applications.

You might want to remove votes from nodes in certain disaster recovery configurations. For example, in a multisite cluster, you could remove votes from the nodes in a backup site so that those nodes do not affect quorum calculations. This configuration is recommended only for manual failover across sites.

<https://technet.microsoft.com/en-us/library/jj612870.aspx>

#### **QUESTION 34**

Your network contains an Active Directory domain named adatum.com. Client computers are deployed by using Windows Deployment Services (WDS).

From Active Directory Users and Computers on a domain controller named DC1, you attempt to create a new computer account as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that you configure computer accounts as managed accounts when you create the computer accounts from Active Directory Users and Computers.

What should you do on DC1?

**Exhibit:**





- A. Install the User Interfaces and Infrastructure feature
- B. From the View menu in Active Directory Users and Computers, select Users, Contacts, Groups, and Computers as containers.
- C. Install the Windows Deployment Services Tools role administration tool
- D. From the View menu in Active Directory Users and Computers, select Advanced Features

**Correct Answer: C**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

You can use Windows Deployment Services to link physical computers to computer account objects in Active Directory Domain Services (AD DS). This is called prestaging the client. Prestaged clients are also called known computers. Prestaging the client allows you to configure properties to control the

installation for the client. For example, you can configure the network boot program and the unattend file that the client should receive, as well as the server from which the client should download the network boot program.

Using the Active Directory Users and Computers snap-in, you can prestage client computers before they have attempted a network boot using AD DS.

<https://technet.microsoft.com/en-us/library/cc754469.aspx>

### QUESTION 35

You have a VHD that contains an image of Windows Server 2012 R2.

You plan to apply updates to the image. You need to ensure that only updates that can install without requiring a restart are installed.

Which DISM option should you use?

- A. /PreventPending
- B. /Apply-Unattend
- C. /Cleanup-Image
- D. /Add-ProvisionedAppxPackage

**Correct Answer: A**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

Use the **/PreventPending** option to skip the installation of the package if the package or Windows image has pending online actions. This option can only be used when servicing Windows 8, Windows Server 2012, or Windows® Preinstallation Environment (Windows PE) 4.0 images.

<https://technet.microsoft.com/en-us/library/hh825265.aspx>

### QUESTION 36

Your network contains an Active Directory domain named adatum.com. The domain contains a server named WDS1 that runs Windows Server 2012 R2.

You install the Windows Deployment Services server role on WDS1. You have a virtual machine named VM1 that runs Windows Server 2012 R2. VM1 has several line-of-business applications installed.

You need to create an image of VM1 by using Windows Deployment Services.

Which type of image should you add to VM1 first?

- A. Capture
- B. Install
- C. Discovery
- D. Boot

**Correct Answer:** D

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

Windows Deployment Services uses two basic image types, both of which use the Windows Image (.wim) file format:

- **Install image:** The operating system image that you deploy to the client computer. To create install images using Windows Deployment Services, you must first create a capture image.
- **Boot image:** The Microsoft Windows Preinstallation Environment (Windows PE) image that you boot a client into before you install the install image. To install an operating system, you first boot the computer into the boot image, and then you select the install image to install. You can also create two additional types of boot images:

**Capture image:** A type of boot image that you boot a client computer into to capture the operating system as a .wim file. You must first create a capture image when you are creating custom install images.

**Discover image:** A type of boot image that you can use to install an operating system on a computer that is not Pre-Boot Execution Environment (PXE) enabled. When you boot a computer into a discover image, a Windows Deployment Services server will be located, and then you can choose the install image you want to install.

<https://technet.microsoft.com/en-us/library/cc730907>

### QUESTION 37

You have a VHD that contains an image of Windows Server 2012 R2.

You need to apply an update package to the image.

Which DISM option should you use?

- A. /Add-ProvisionedAppxPackage
- B. /Cleanup-Image
- C. /Add-Package

D. /Apply-Unattend

**Correct Answer: C**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

**/Add-Package** installs a specified .cab or .msu package in the image. Multiple packages can be added on one command line. The applicability of each package will be checked. If the package is cannot be applied to the specified image, you will receive an error message.

<https://technet.microsoft.com/en-us/library/hh825265.aspx>

### QUESTION 38

Which WDSUTIL parameter do you need to use to import GUID and MAC address?

A. /get-AutoAddDevices

B. /get-Device

C. /add

D. /enable

**Correct Answer: B**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

**/get-Device** retrieves Windows Deployment Services information about a prestaged computer (that is, a physical computer that has been lined to a computer account in Active Directory Domain Services).

```
WDSUTIL /Get-Device {/Device:<Device name> | /ID:<MAC or UUID>} [/Domain:<Domain>] [/Forest:{Yes | No}]
```

<https://technet.microsoft.com/en-us/library/cc742044.aspx>

### QUESTION 39

Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 runs Windows Server 2012 and has the Windows Deployment Services (WDS) server role installed.

You need to use WDS to deploy an image to a client computer that does not support PXE.

Which type of image should you use to start the computer?

- A. Capture
- B. Install
- C. Discovery
- D. Boot

**Correct Answer: C**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

Windows Deployment Services uses two basic image types, both of which use the Windows Image (.wim) file format:

- **Install image:** The operating system image that you deploy to the client computer. To create install images using Windows Deployment Services, you must first create a capture image.
- **Boot image:** The Microsoft Windows Preinstallation Environment (Windows PE) image that you boot a client into before you install the install image. To install an operating system, you first boot the computer into the boot image, and then you select the install image to install. You can also create two additional types of boot images:

**Capture image:** A type of boot image that you boot a client computer into to capture the operating system as a .wim file. You must first create a capture image when you are creating custom install images.

**Discover image:** A type of boot image that you can use to install an operating system on a computer that is not Pre-Boot Execution Environment (PXE) enabled. When you boot a computer into a discover image, a Windows Deployment Services server will be located, and then you can choose the install image you want to install.

<https://technet.microsoft.com/en-us/library/cc730907>

#### **QUESTION 40**

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

You plan to create an image of Server1. You need to remove the source files for all server roles that are not installed on Server1.

Which tool should you use?

- A. Ocsetup.exe
- B. Servermanagercmd.exe
- C. ImageX.exe

D. Dism.exe

**Correct Answer:** D

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

The Deployment Image Servicing and Management (DISM) tool is a command-line tool that is used to modify Windows® images. You can use DISM to enable or disable Windows features directly from the command prompt, or by applying an answer file to the image. You can enable or disable Windows features offline on a WIM or VHD file, or online on a running operating system.

<https://technet.microsoft.com/en-us/library/hh824822.aspx>

#### **QUESTION 41**

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 has the Windows Server Update Services (WSUS) server role installed. WSUS is configured to use a Windows Internal Database. Server2 has Microsoft SQL Server 2008 R2 Standard deployed.

You detach the SUSDB database from Server1 and attach the database to Server2.

You need to ensure that Windows Deployment Services (WDS) on Server1 uses the database hosted on Server2.

What should you do on Server1?

- A. Configure an ODBC file data source
- B. Run the wsusutil command
- C. Edit the registry
- D. Configure an ODBC system data source

**Correct Answer:** C

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

#### **Migrating the WSUS database if it is running on the WSUS server**

1. Install SQL Server by using the **Server and Client Tools** option on your WSUS server.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.

3. Right-click **IIS Admin Service**, and then click **Stop**.
4. Right-click **Update Services**, and then click **Stop**.
5. Run the following SQL command to detach the WSUS database (SUSDB) from the Windows Internal Database instance by using the **sqlcmd** utility.
6. In SQL Server Management Studio, under the **Instance** node, right-click **Databases**, select **Properties**, and then click **Attach**.
7. In this step, you will verify that NT AUTHORITY\NETWORK SERVICE has login permissions to the instance of SQL Server and to the WSUS database. If it does not, you will have to add it to both locations. This account should also be a member of the **webService** role on the WSUS database.
8. In the **Attach Databases** box, under **Databases to attach**, locate the susdb.mdf file, and then click **OK**.
9. In this step, you will edit the registry to point WSUS to the instance of SQL Server that now holds the WSUS database and to recognize the new database for future WSUS updates. If you have not already done so, export the keys in the registry that you plan to edit or back up the whole registry.
  - a. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
  - b. Locate the following key:  
  
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\UpdateServices\Server\Setup\SqlServerName`  
  
In the **Value** text box, type `[ServerName]\[InstanceName]`, and then click **OK**. If the instance name is the default instance, type `[ServerName]`.
  - c. Find the following key:  
  
`HKEY_LOCAL_MACHINE\Software\Microsoft\Update Services\Server\Setup\wYukonInstalled`  
  
In the **Value** text box, type 0, and then click **OK**.
10. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
11. Right-click **IIS Admin Service**, and then click **Start**.
12. Right-click **Update Services**, and then click **Start**.
13. Verify that the database migration was successful by opening the WSUS administrative console.

[https://technet.microsoft.com/en-us/library/Dd939918\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Dd939918(v=WS.10).aspx)

#### QUESTION 42

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

The domain contains a server named Server1. You install the Windows PowerShell Web Access gateway on Server1.

You need to provide administrators with the ability to manage the servers in the domain by using the Windows PowerShell Web Access gateway.

Which two cmdlets should you run on Server1? (Each correct answer presents part of the solution. Choose two.)

- A. Set-WSManQuickConfig
- B. Set-WSManInstance
- C. Add-PswaAuthorizationRule
- D. Set-BCAAuthentication
- E. Install-PswaWebApplication

**Correct Answer: CE**

**Section: Deploy, manage, and maintain servers**

**Explanation**

**Explanation/Reference:**

The **Install-PswaWebApplication** cmdlet is a quick way to get Windows PowerShell Web Access configured.

After Windows PowerShell Web Access is installed and the gateway is configured, users can open the sign-in page in a browser, but they cannot sign in until the Windows PowerShell Web Access administrator grants users access explicitly. Windows PowerShell Web Access access control is managed by using the set of Windows PowerShell cmdlets described below. There is no comparable GUI for adding or managing authorization rules.

To add a restrictive authorization rule

**Add-PswaAuthorizationRule** -UserName Contoso\JSmith -ComputerName Contoso\_214 -ConfigurationName NewAdminsOnly

<https://technet.microsoft.com/en-us/library/Hh831611.aspx>

#### QUESTION 43

Your network contains an Active Directory forest named contoso.com. The forest contains two sites named Main and Branch. The Main site contains 400 desktop computers and the Branch site contains 150 desktop computers. All of the desktop computers run Windows 8.

In Main, the network contains a member server named Server1 that runs Windows Server 2012 R2. You install the Windows Server Update Services server role on Server1.

You need to ensure that Windows updates obtained from Windows Server Update Services (WSUS) are the same for the computers in each site. You



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

What should you do?

- A. From the Update Services console, create computer groups.
- B. From the Update Services console, configure the Computers options.
- C. From the Group Policy Management console, configure the Windows Update settings.
- D. From the Group Policy Management console, configure the Windows Anytime Upgrade settings.
- E. From the Update Services console, configure the Synchronization Schedule options.

**Correct Answer:** A

**Section:** Deploy, manage, and maintain servers

**Explanation**

**Explanation/Reference:**

Windows Server Update Services (WSUS) 3.0 SP2 enables you to manage the entire process of updating your computers, including manually and automatically determining which updates they need and receive, specifying when the updates are installed, and monitoring the status of update deployments on your computers.

WSUS also allows you to target updates to groups of client computers. This capability can help you ensure that specific computers get the right updates at the most convenient times on an ongoing basis. For example, if all the computers in one department of your organization (such as all computers in the Accounting team) have a specific configuration, you can determine what updates those computers get, at what time, and then use the WSUS reporting features to evaluate the success of the update activity for that computer group.

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

#### **QUESTION 44**

You have a WIM file that contains an image of Windows Server 2012 R2.

Recently, a technician applied a Microsoft Standalone Update Package (MSU) to the image. You need to remove the MSU package from the image.

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

**Select and Place:**

	Answer Area
Run <b>dism.exe</b> and specify the <i>/Capture-Image</i> parameter.	
Run <b>dism.exe</b> and specify the <i>/Apply-Image</i> parameter.	
Run <b>wusa.exe</b> and specify the <i>/uninstall</i> parameter.	
Run <b>dism.exe</b> and specify the <i>/RemovePackage</i> parameter.	
Run <b>dism.exe</b> and specify the <i>/Cleanup-Image</i> parameter.	

Correct Answer:

	Answer Area
	Run <b>dism.exe</b> and specify the <i>/Apply-Image</i> parameter.
	Run <b>wusa.exe</b> and specify the <i>/uninstall</i> parameter.
	Run <b>dism.exe</b> and specify the <i>/Capture-Image</i> parameter.
Run <b>dism.exe</b> and specify the <i>/RemovePackage</i> parameter.	
Run <b>dism.exe</b> and specify the <i>/Cleanup-Image</i> parameter.	

Section: Deploy, manage, and maintain servers

Explanation

## Explanation/Reference:

### DISM Image Management Command-Line Options

Deployment Image Servicing and Management (DISM.exe) mounts a Windows image (.wim) file or virtual hard disk (.vhd or .vhdx) for servicing. You can also use the DISM image management command to list the image index numbers, to verify the architecture for the image that you are mounting, append an image, apply an image, capture an image and delete an image. After you update the image, you must unmount it and either commit or discard the changes that you have made.

Option: **/Apply-Image** Applies an image to a specified drive.

Option: **/Capture-Image** Captures an image of a drive to a new .wim file. Captured directories include all subfolders and data. You cannot capture an empty directory. A directory must contain at least one file.

<https://technet.microsoft.com/en-us/library/hh825258.aspx>

### Description of the Windows Update Standalone Installer in Windows

The Wusa.exe file is in the %windir%\System32 folder. The Windows Update Standalone Installer uses the Windows Update Agent API to install update packages. Update packages have an .msu file name extension. The .msu file name extension is associated with the Windows Update Standalone Installer.

You can use Wusa.exe to uninstall an update in Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012. You can use the following switches together with Wusa.exe:

**/uninstall** Uninstalls the specified package or KB number.

<http://support.microsoft.com/kb/934307>

### QUESTION 45

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.

You generalize Server2. You install the Windows Deployment Services (WDS) server role on Server1. You need to capture an image of Server2 on Server1.

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

### Select and Place:

Actions	Answer Area
Add an install image to Server1.	
Start Server2 by using PXE.	
Add a boot image to Server1.	
Add a capture image to Server1.	
Add a prestaged device to Server1.	
Start Server2 by using a Windows To Go image.	

**Correct Answer:**

Actions	Answer Area
	Start Server2 by using PXE.
	Add a capture image to Server1.
Add a boot image to Server1.	Add an install image to Server1.
Add a prestaged device to Server1.	
Start Server2 by using a Windows To Go image.	

**Section: Deploy, manage, and maintain servers**

## Explanation

### Explanation/Reference:

#### Steps for creating a capture image

To create an install image, you must first create a capture image. Capture images are boot images that you boot a client computer into to capture the operating system into a .wim file. You can also create media (a CD, DVD, USB drive, or other type of media) that contains a capture image, and then boot a computer from the media. These images provide an alternative to the command-line utility, ImageX.exe. Except in advanced scenarios, you can create a capture image by using the Boot.wim file from the Windows installation media.

#### To create a capture image

1. In the Windows Deployment Services MMC snap-in, expand the **Boot Images** node.
2. Right-click the image to use it as a capture image. In most cases, you can just use the Boot.wim file from the installation media.
3. Click **Create Capture Image**.
4. Type in your Image Name, Image Description, and the location and file name where you want to save a local copy of the file. You must specify a location in case there is a problem with the network when you deploy the capture image. Click **Next**.
5. Allow the Create Capture Image Wizard to complete.
6. Tick **Add Image to the Windows Deployment Server now**. Click **Next**
7. Enter the location of the Windows Image file that contains the images. Click **Next**.
8. Enter your **Image Name** and **Image Description**. Click **Next**.
9. On the **Summary** page, click **Next**.
10. Click **Finish**.

After you have created the capture image, follow the instructions in the next section to boot a computer into the capture image and capture the operating system.

#### Steps for creating an install image

Now that you have a capture image, you need to prepare a reference computer and then create the install image. The reference computer can be a computer with a standard Windows installation or a Windows installation that has been configured for your environment. First, you boot a computer (which has been prepared with Sysprep) into the capture image. Then a wizard creates an install image of the reference computer and saves it as a .wim file. After that, you can deploy the .wim file to a computer.

## To create a custom install image

1. Create a reference computer (install the operating system, applications, and make any other changes that you want).
2. Ensure that you have the correct version of Sysprep.exe on the computer.
3. At a command prompt on the reference computer, change folders to \Windows\System32\Sysprep or the folder that contains Sysprep.exe and Setupcl.exe.
4. Type one of the following:

On computers running Windows 8.1, Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 run the command:

```
sysprep /oobe /generalize /reboot
```

If you prefer, you can also use the **Sysprep** graphical user interface by double-clicking **Sysprep.exe**.

5. When the computer restarts, perform a network boot on the computer by pressing F12.
6. In the boot menu, select the capture boot image that you created in the preceding procedure, and then press ENTER.
7. You will be presented with the Windows Deployment Services Image Capture Wizard. Click **Next**.
8. On the **Directory to Capture** page, select **Volume to capture**, enter your **Image name** and **Image description**. Click **Next**.
9. Click **Browse** next to Name and location and browse to a local folder where you want to store the captured install image. Type a name for the image, using the .wim file name extension, and then click **Save**. Note that this location can be a mapped network drive.
10. Select the **Upload Image to a Windows Deployment Services** check box.
11. Click **Connect**. If prompted for credentials, provide a user name and password for an account with permissions to connect to the Windows Deployment Services server.
12. Select your **Image Group Name**. Click **Next**. The wizard will now complete and create a custom installation image and store it in the Windows Deployment Services store.
13. Click **Finish**.

When this process is complete, you can PXE boot a client computer to install this image. The image will be listed in the installation option.

<https://technet.microsoft.com/en-us/library/jj648426.aspx>

**QUESTION 46**

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 Server3 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	<div><div></div><div>set-wsuserversynchronization -syncfrommu</div><div>set-wsuserversynchronization -ussservername server1</div><div>set-wsuserversynchronization -ussservername server2</div><div>wsusutil.exe movecontent \\server1\c\$</div><div>wsusutil.exe movecontent \\server2\c\$</div></div>
Server2	<div><div></div><div>set-wsuserversynchronization -syncfrommu</div><div>set-wsuserversynchronization -ussservername server1</div><div>set-wsuserversynchronization -ussservername server2</div><div>wsusutil.exe movecontent \\server1\c\$</div><div>wsusutil.exe movecontent \\server2\c\$</div></div>

**Correct Answer:**

Server1	<input type="text"/> set-wsuserversynchronization -syncfrommu set-wsuserversynchronization -ussservername server1 set-wsuserversynchronization -ussservername server2 wsusutil.exe movecontent \\server1\c\$\ wsusutil.exe movecontent \\server2\c\$\
Server2	<input type="text"/> set-wsuserversynchronization -syncfrommu set-wsuserversynchronization -ussservername server1 set-wsuserversynchronization -ussservername server2 wsusutil.exe movecontent \\server1\c\$\ wsusutil.exe movecontent \\server2\c\$\

## Section: Deploy, manage, and maintain servers

### Explanation

#### Explanation/Reference:

The **Set-WsusServerSynchronization** cmdlet 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).

#### **-SyncFromMU**

Specifies that the WSUS server synchronizes updates from Microsoft Update.

#### **-UssServerName<String>**

Specifies the name of a local server from which to synchronize updates.

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

### QUESTION 47

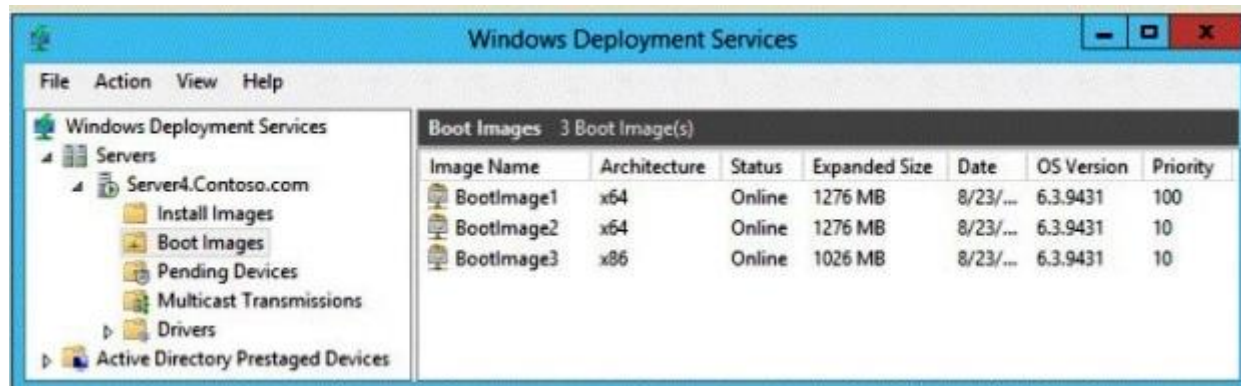
You have a server named Server4 that runs Windows Server 2012 R2. Server4 has the Windows Deployment Services server role installed.

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

Complete each statement in the answer are according to the information presented in the exhibit. Each correct selection is worth one point.

#### Exhibit:





Hot Area:

#### Answer Area

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

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

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

- BootImage1.
- BootImage2.
- BootImage3.

Correct Answer:

#### Answer Area

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

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

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

- BootImage1.
- BootImage2.
- BootImage3.

#### Section: Deploy, manage, and maintain servers

##### Explanation

##### Explanation/Reference:

To configure menu order for boot images, in the **Image Properties** dialog, on the **General** tab, enter in your desired priority into the Priority text box. The items that appear first on your install image menu are the ones with the lowest value. (i.e., the image with the smallest assigned priority number is the highest priority image.)

<https://technet.microsoft.com/en-us/library/jj648426.aspx>

The boot menu on x86-based computers will display only x86 boot images (because x86-based computers cannot run x64 boot images); however, if you boot into an x86-based boot image from an x64-based computer, x86-based and x64-based install images will be displayed. If you boot into an x64-based boot image from an x64-based computer, only x64-based boot images will be displayed.

[https://technet.microsoft.com/en-us/library/cc730907\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc730907(v=ws.10).aspx)

#### QUESTION 48

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

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

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

Hot Area:

Answer Area		
<div><div></div><div>Add-WsusComputer Approve-WsusUpdate Set-WsusClassification Set-WsusProduct Set-WsusServerSynchronizatio</div></div>	<div><div></div><div>-ServerName Server1 -UpdateServer Server1 -UssServerName Server1</div></div>	<div><div></div><div>-Replica -SyncFromMu -UseSsl</div></div>

Correct Answer:

Answer Area		
<div><div></div><div>Add-WsusComputer Approve-WsusUpdate Set-WsusClassification Set-WsusProduct Set-WsusServerSynchronizatio</div></div>	<div><div></div><div>-ServerName Server1 -UpdateServer Server1 -UssServerName Server1</div></div>	<div><div></div><div>-Replica -SyncFromMu -UseSsl</div></div>

Section: Deploy, manage, and maintain servers

Explanation

Explanation/Reference:

The **Set-WsusServerSynchronization** cmdlet 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).

**-UssServerName<String>**

Specifies the name of a local server from which to synchronize updates.

**-Replica**

Specifies whether the WSUS server is a replica server.

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

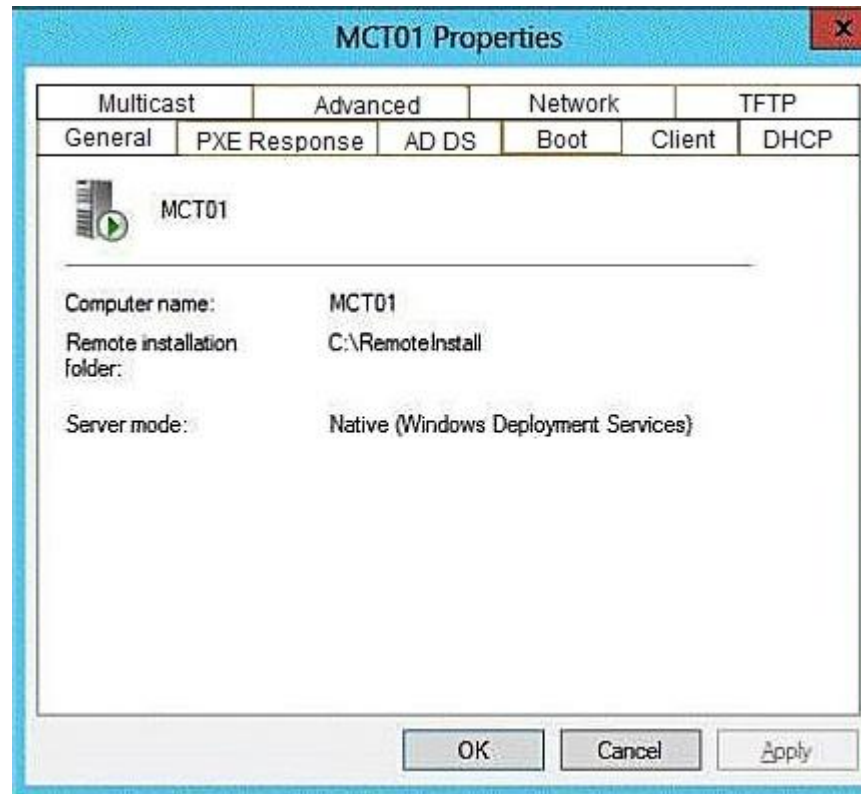
#### QUESTION 49

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

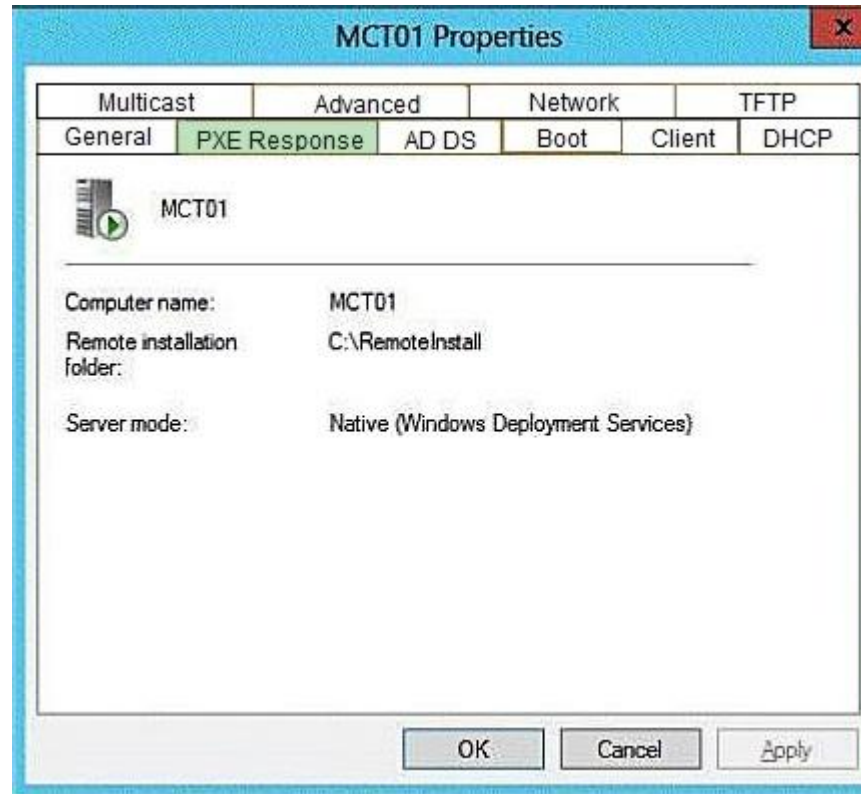
You create a new multicast session in WDS and connect 50 client computers to the session. When you open the Windows Deployment Services console, you discover that all of the computers are listed as pending devices. You need to ensure that any of the computers on the network can join a multicast transmission without requiring administrator approval.

What should you configure? To answer, select the appropriate tab in the answer area.

**Hot Area:**



**Correct Answer:**



## Section: Deploy, manage, and maintain servers

### Explanation

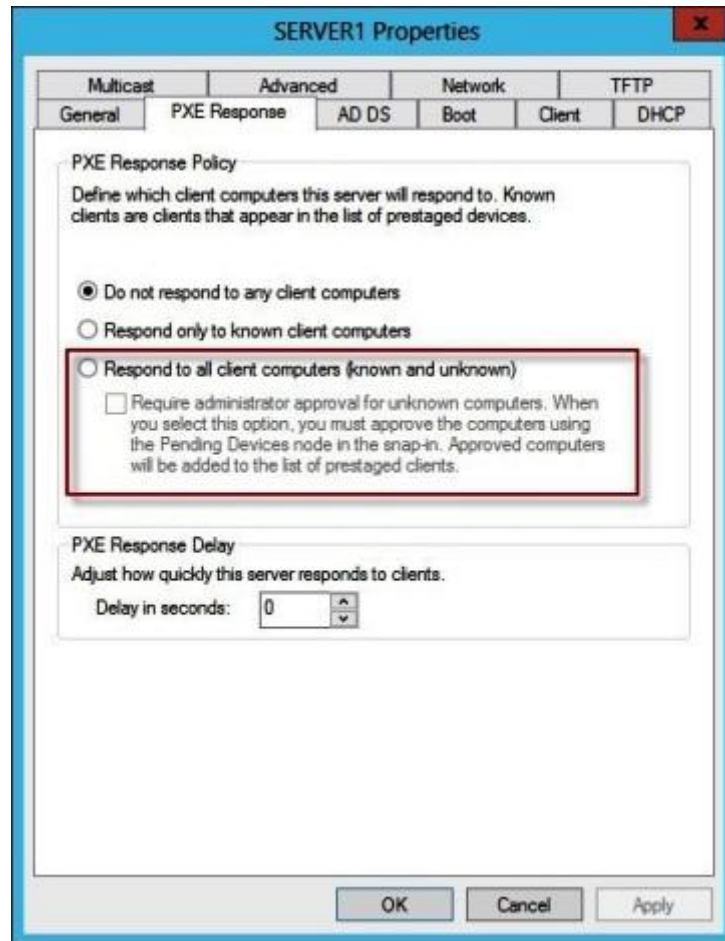
#### Explanation/Reference:

The settings on the **PXE Response** tab determine which clients Windows Deployment Services responds to, what action is taken when responding to an unknown client, and how long to wait before responding to a client. To view this tab, right-click the server in the MMC-snap in, and then click **Properties**.

The following options specify how the Windows Deployment Services server responds to incoming Pre-Boot Execution Environment (PXE) requests from client computers.

- **Do not respond to any client computers.** Note that this option will only work if Windows Deployment Services and DHCP are running on different servers. This is because although Windows Deployment Services will not respond, DHCP will. You can try to work around this issue by disabling DHCP option 60 on the DHCP Tab.

- **Respond only to known client computers.** Choose this option if you have prestaged clients in Active Directory Domain Services. When you select this option, clients that are not prestaged (unknown) will not be able to PXE boot to the Windows Deployment Services server.
- **Respond to all client computers (known and unknown).** Choose this option to allow all clients to PXE boot to the Windows Deployment Services server. The check box labeled **Require administrator approval for unknown computers** is called the Auto-Add policy. Choose this option if you want to approve new clients using the **Pending Devices** node in the MMC snap-in before allowing them to PXE boot.



<https://technet.microsoft.com/en-us/library/cc732360.aspx>

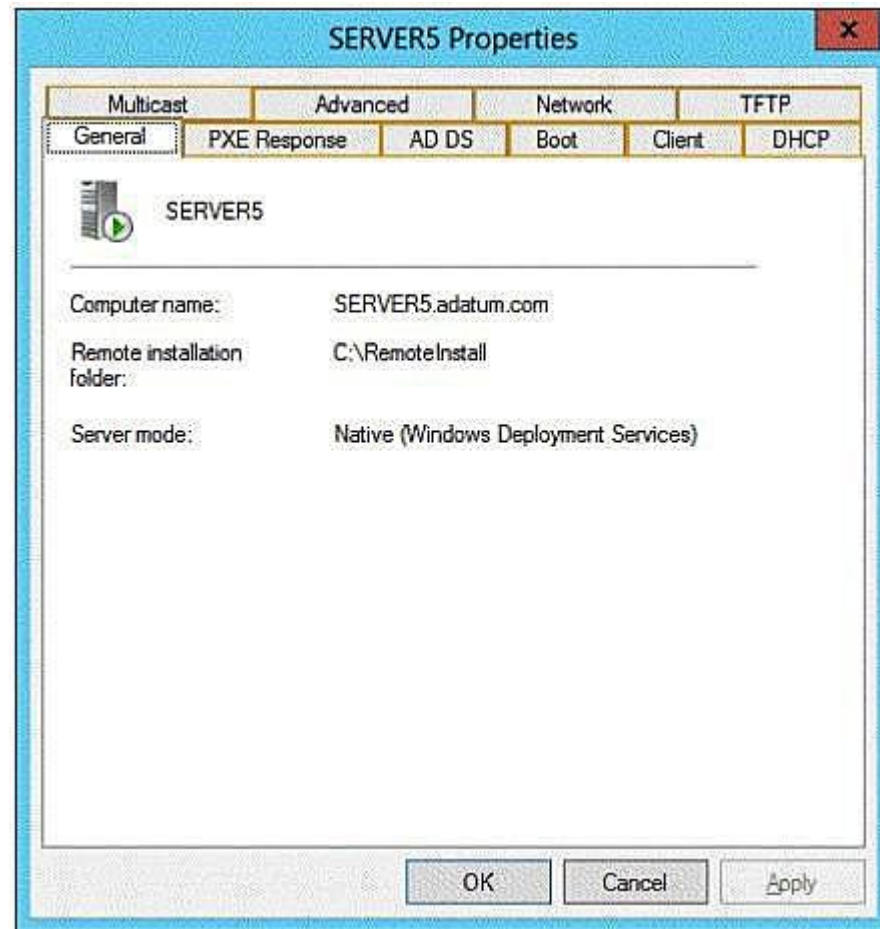
## QUESTION 50

You have a server named Server5 that runs Windows Server 2012 R2. Server5 has the Windows Deployment Services server role installed. Server5 contains several custom images of Windows 8.

You need to ensure that when 32-bit client computers start by using PXE, the computers automatically install an image named Image1.

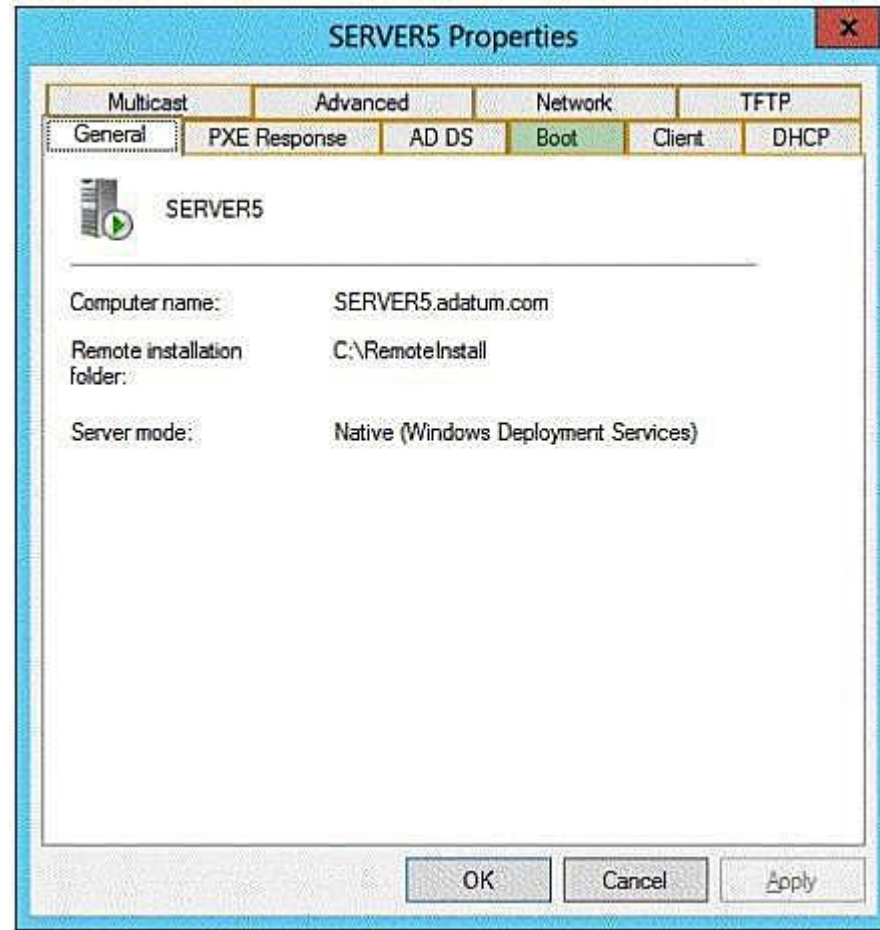
What should you configure? To answer, select the appropriate tab in the answer area.

**Hot Area:**



**Correct Answer:**





### Section: Deploy, manage, and maintain servers

#### Explanation

#### Explanation/Reference:

#### Automating the Selection of the Boot Image

Windows Deployment Services displays a menu that enables users to select a boot image. This menu is always automated, and when there are multiple boot images, one will be selected by default when the time-out value expires (which is configurable by using the Bcdedit tool). However, if there is only one boot image available to the client computer, it will be selected immediately. Because the boot menu selection does not require user action, the only configuration task that you need to complete is to ensure that clients are directed to the correct boot image. There are two methods for doing



this:

Configure the default boot image on the server (on the **Boot** tab of the server's properties). This setting applies to all clients of a particular architecture (both prestaged and unknown computers) that connect to the server.

Configure the default boot image for a prestaged computer by running the command **WDSUTIL /Set-Device /Device:<name> /BootImagePath:<Relative path>**, where <path> is the relative path to the RemoteInstall folder.

[https://technet.microsoft.com/en-us/library/cc771788\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771788(v=ws.10).aspx)

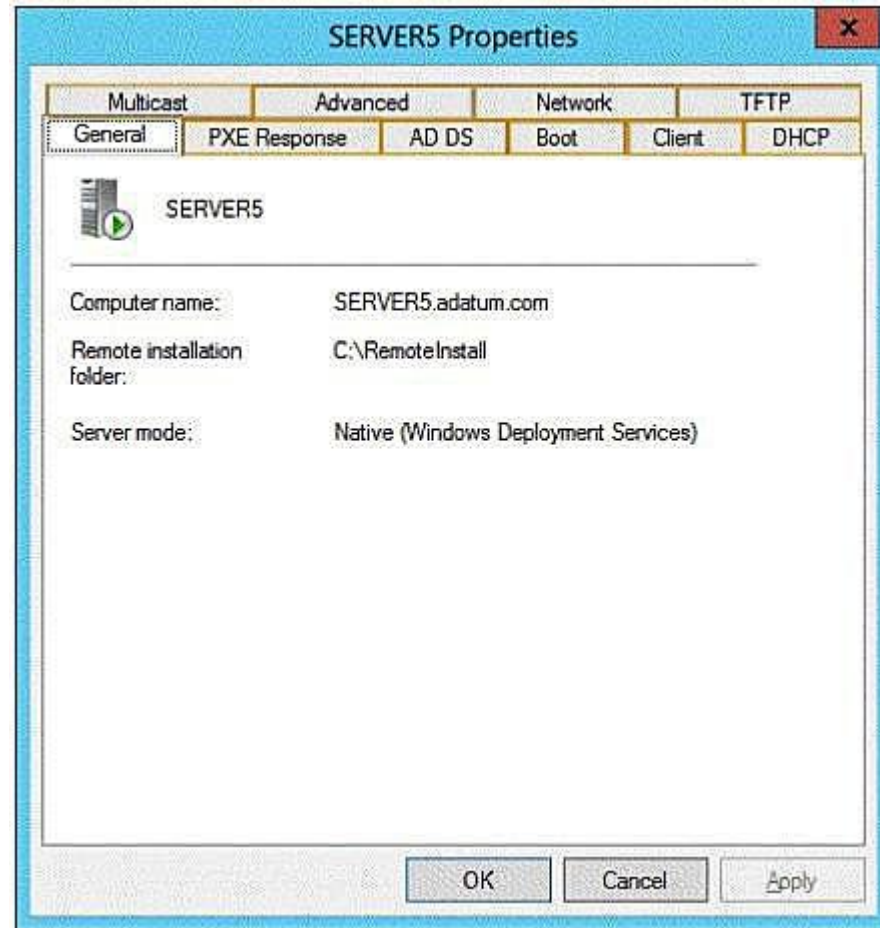
#### **QUESTION 51**

You have a server named Server5 that runs Windows Server 2012 R2. Servers has the Windows Deployment Services server role installed.

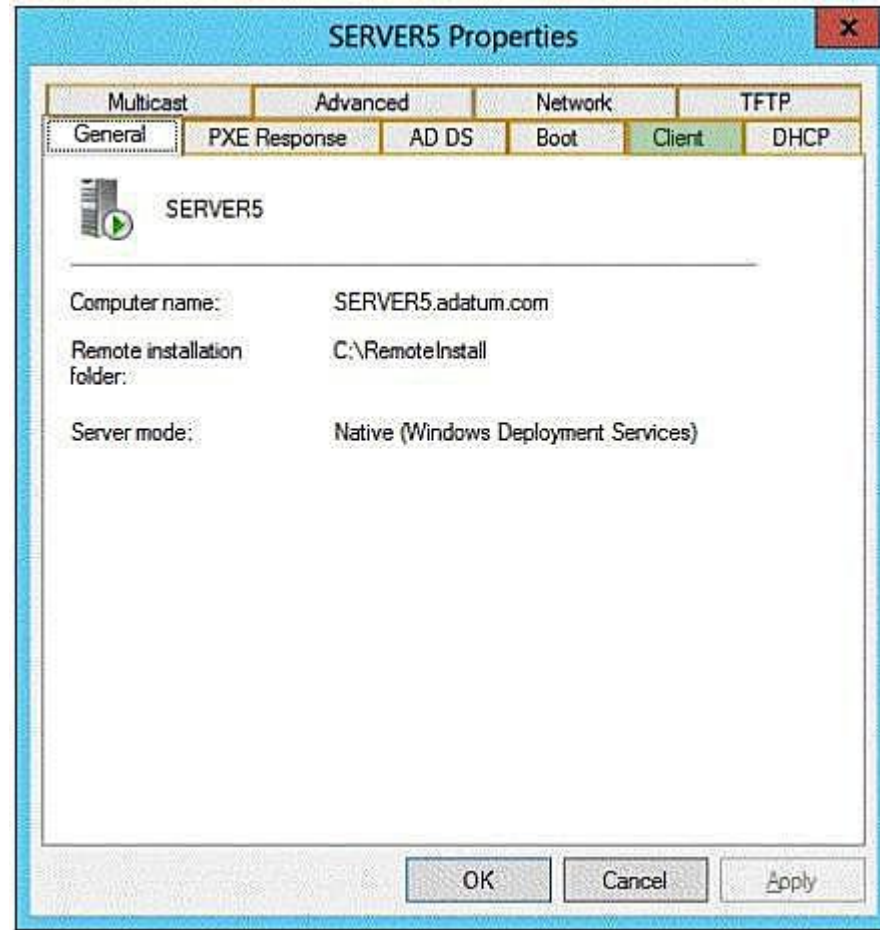
You need to ensure that when client computers connect to Server5 by using PXE, the computers use an unattended file.

What should you configure? To answer, select the appropriate tab in the answer area.

**Hot Area:**



**Correct Answer:**



### Section: Deploy, manage, and maintain servers

#### Explanation

#### Explanation/Reference:

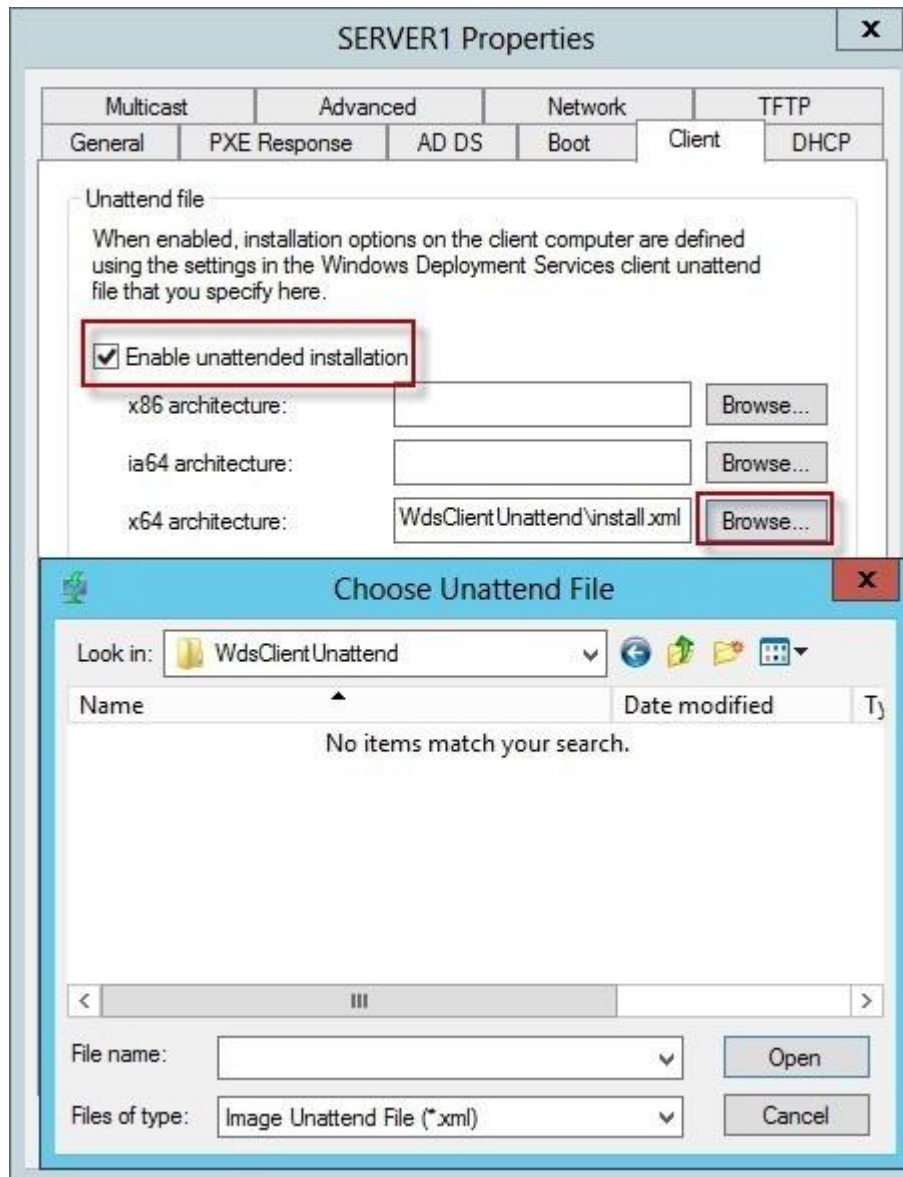
To automate the installation, create the appropriate unattend file depending on whether you are configuring the Windows Deployment Services screens or Windows Setup. We recommend that you use Windows System Image Manager (included as part of the Windows Assessment and Deployment Kit) to author the unattend files. The Windows System Image Manager (Windows SIM) creates and manages unattended Windows Setup answer files in a graphical user interface (GUI).

You will then need to copy the unattend file to the appropriate location, and assign it for use. You can assign it at the server level or the client level. The

server level assignment can further be broken down by architecture, enabling you to have different settings for x86-based and x64-based clients. Assignment at the client level overrides the server-level settings.

#### **To associate a client unattend file by architecture**

1. Create an Unattend.xml file with settings applicable to Windows Deployment Services.
2. Copy the client unattend file to a folder in the **RemoteInstall** folder. For example: **RemoteInstall\WDSCientUnattend**.
3. Open the Windows Deployment Services MMC snap-in, right-click the server that contains the image that you want to associate the unattend file with, and then click **Properties**.
4. On the **Client** tab, select **Enable unattended installation**, browse to the appropriate unattend file, and then click **Open**.
5. Click **OK** to close the **Properties** page.



<https://technet.microsoft.com/en-us/library/jj648426.aspx>

## QUESTION 52

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?

**Exhibit:**



- 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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

Access-based enumeration hides files and folders that users do not have permission to access. By default, this feature is not enabled for DFS namespaces. You can enable access-based enumeration of DFS folders by using DFS Management. To control access-based enumeration of files and folders in folder targets, you must enable access-based enumeration on each shared folder by using Share and Storage Management.

To enable access-based enumeration on a namespace, all namespace servers must be running Windows Server 2008 or newer. Additionally, domain-based namespaces must use the Windows Server 2008 mode.

If you upgrade the domain functional level to Windows Server 2008 while there are existing domain-based namespaces, DFS Management will allow you to enable access-based enumeration on these namespaces. However, you will not be able to edit permissions to hide folders from any groups or users unless you migrate the namespaces to the Windows Server 2008 mode. For more information, see **Migrate a Domain-based Namespace to Windows Server 2008 Mode**.

<https://technet.microsoft.com/en-us/library/dd759150.aspx>

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.

<https://technet.microsoft.com/en-us/library/cc753875.aspx>

### QUESTION 53

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

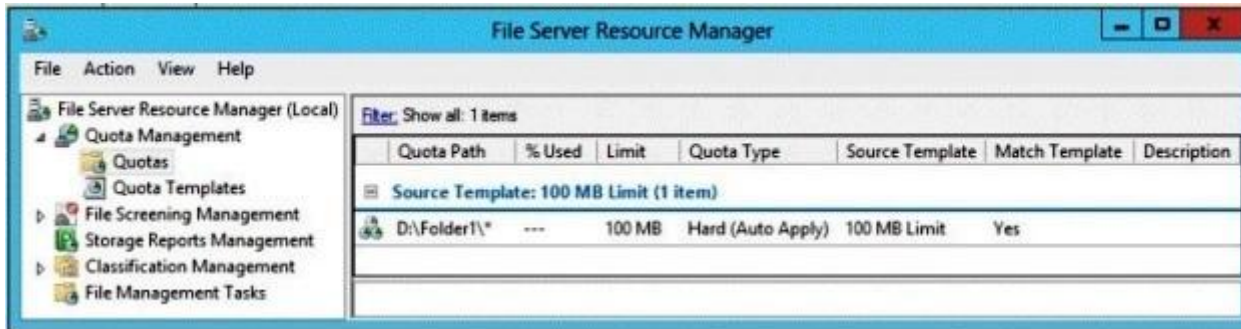
An administrator creates a quota as shown in the Quota exhibit. (Click the Exhibit button.)

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

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

What should you do?

**Exhibit 1 (exhibit):**



**Exhibit 2 (exhibit):**

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

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>
```

- 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**

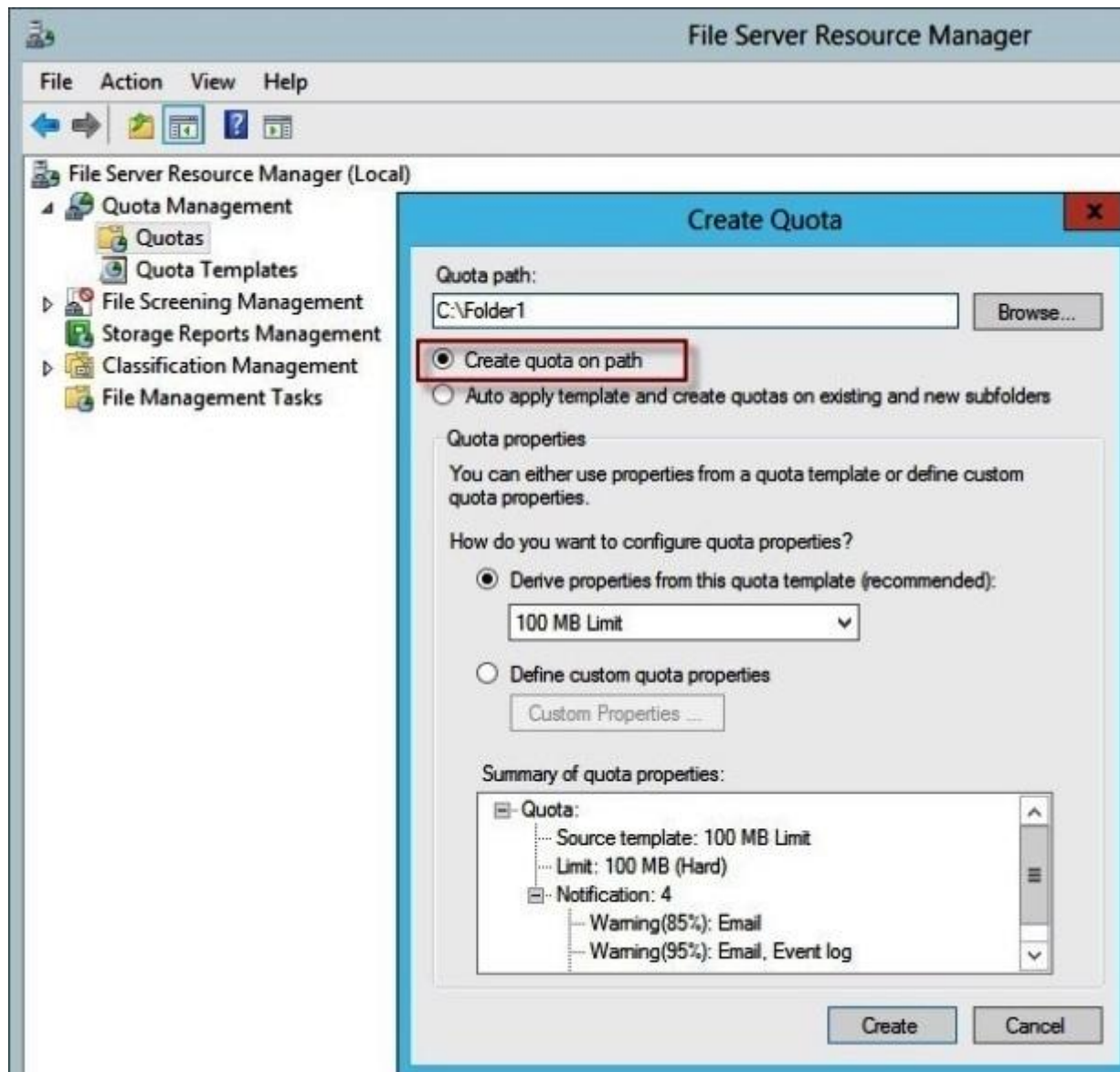
**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

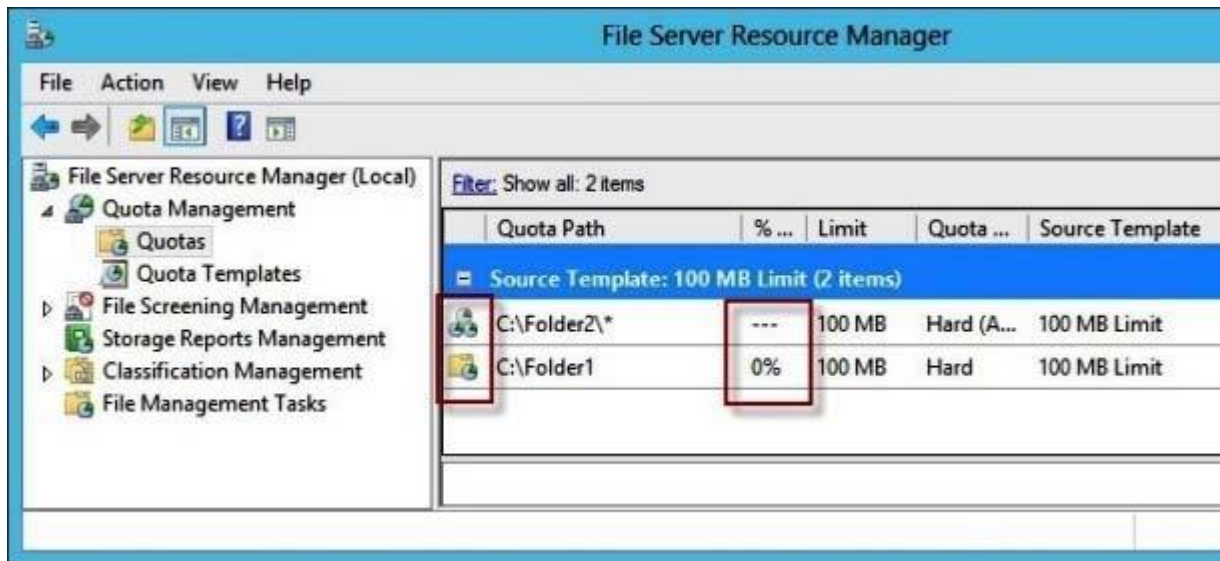
Quotas can be created from a template or with custom properties. The following procedure describes how to create a quota that is based on a template (recommended). If you need to create a quota with custom properties, you can save these properties as a template to reuse at a later date.





When you create a quota, you choose a quota path, which is a volume or folder that the storage limit applies to. On a given quota path, you can use a template to create one of the following types of quota:

- A single quota that limits the space for an entire volume or folder.
- An auto apply quota, which assigns the quota template to a folder or volume. Quotas based on this template are automatically generated and applied to all subfolders.



```
Administrator: Command Prompt

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

Directory of C:\Folder1

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

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

Directory of C:\Folder2

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

<https://technet.microsoft.com/en-us/library/cc771467.aspx>

#### QUESTION 54

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

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

You implement a Distributed File System (DFS) replication group named ReplGroup. ReplGroup is used to replicate a folder on each file server. ReplGroup uses a hub and spoke topology. NYC-SVR1 is configured as the hub server.

You need to ensure that replication can occur if NYC-SVR1 fails.

What should you do?

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

**Correct Answer: D**

**Section: Configure File and Print Services**

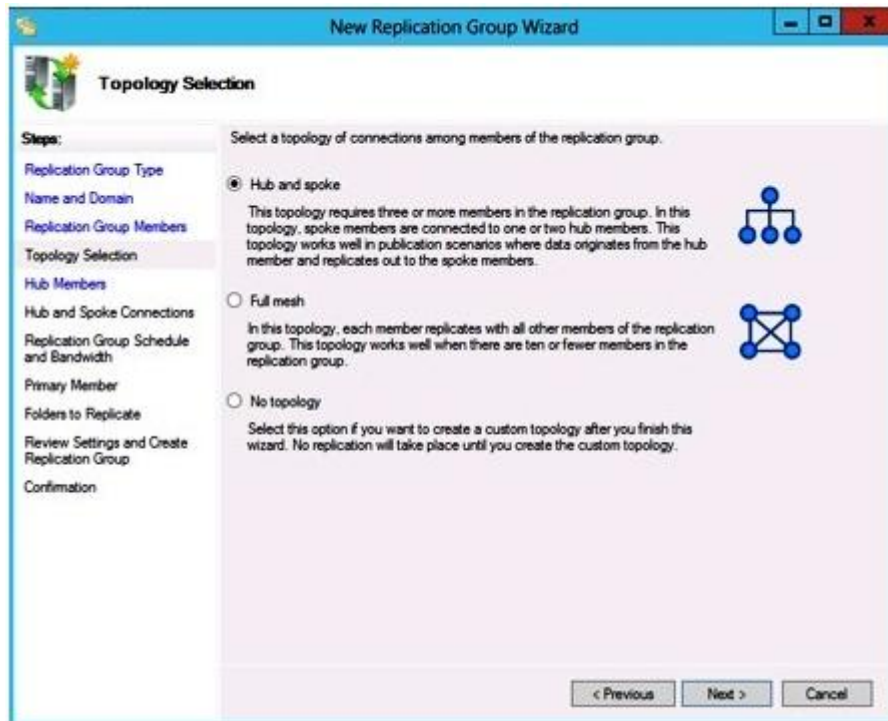
**Explanation**

**Explanation/Reference:**

The replication topology consists of the logical connections that DFS Replication uses to replicate files among servers. When you set up a replication group, you can choose from three topologies:

- **Hub and spoke.** This topology requires three or more members; otherwise this option is unavailable. For each spoke member, you can choose a required hub member and an optional second hub member for redundancy. This optional hub ensures that a spoke member can still replicate if one of the hub members is unavailable. If you specify two hub members, the hub members will have a full-mesh topology between them.
- **Full mesh.** In this topology, every member replicates with all other members of the replication group. This topology works well when there are ten or fewer members in the replication group. We recommend against using a full mesh topology if you have more than ten members in the replication group.
- **No topology.** Choose this option if you want to create connections yourself after you finish the New Replication Group Wizard or the Replicate Folder Wizard. No replication will take place until you create the connections.

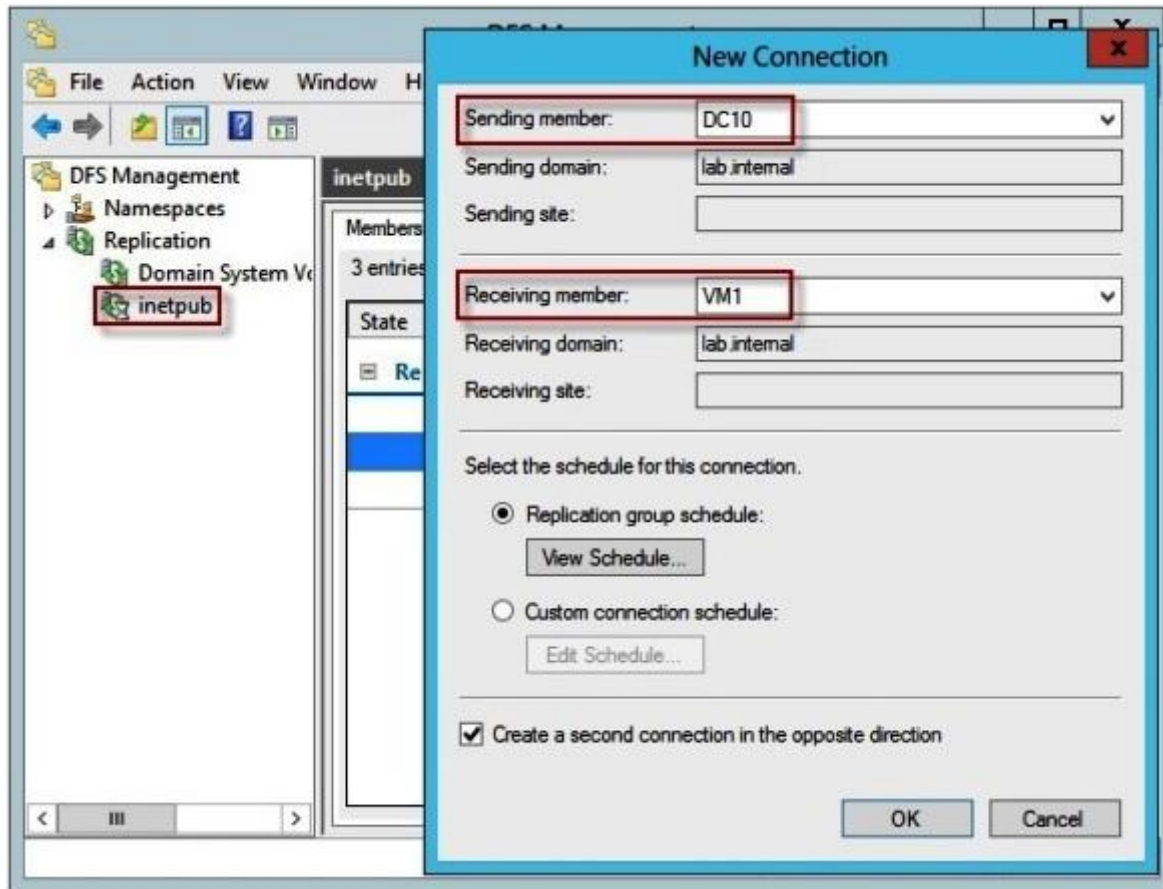
When choosing a topology, keep in mind that two one-way connections are created between the members you choose. These two connections allow data to flow in both directions. For example, in a hub and spoke topology, data will flow from the hub members to the spoke members and from the spoke members to the hub members.



[https://technet.microsoft.com/en-us/library/cc757769\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc757769(v=ws.10).aspx)

### To create a connection

1. Click **Start** , point to **Administrative Tools** , and then click **DFS Management** .
2. In the console tree, under the **Replication** node, right-click the replication group that you want to create a new connection in, and then click **New Connection** .
3. Specify the sending and receiving members, and specify the schedule to use for the connection. At this point, replication is one-way.
4. Select **Create a second connection in the opposite direction** to create a second connection for two-way replication between the sending and receiving members. All members must have two-way connections.



Configuration changes are not applied immediately to all members except when using the `Suspend-DfsReplicationGroup` and `Sync-DfsReplicationGroup` cmdlets. The new configuration must be replicated to all domain controllers, and each member in the replication group must poll its closest domain controller to obtain the changes. The amount of time this takes depends on AD DS replication latency and the long polling interval (60 minutes) on each member.

To poll immediately for configuration changes, open a command prompt window and then type the following command once for each member of the replication group:

```
dfsrdiag.exe PollAD /Member:DOMAIN\Server1
```

To do so from a Windows PowerShell session, use the `Update-DfsrConfigurationFromAD` cmdlet, which was introduced on Windows Server 2012 R2.

<https://technet.microsoft.com/en-us/library/cc771941.aspx>

#### QUESTION 55

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?

**Exhibit:**



- 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:** Configure File and Print Services

**Explanation**

**Explanation/Reference:**

You can configure access-denied assistance within a domain by using Group Policy, or you can configure the assistance individually on each file server by using the **File Server Resource Manager** console. You can also change the access-denied message for a specific shared folder on a file server.

<https://technet.microsoft.com/en-us/library/hh831402.aspx>

## QUESTION 56

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:** Configure File and Print Services

**Explanation**

**Explanation/Reference:**

There are a few considerations and decisions that should be made before you deploy access-denied assistance.

Use the following table to plan your access-denied assistance deployment in your organization.



Task	Description
1.1 Determine the access-denied assistance model	Determine whether your organization should use an email model or a Web services model for access-denied assistance.
1.2. Determine who should handle access requests	You can assign each file share an owner distribution list that will receive access requests.
1.3. Customize the access-denied assistance message	The access-denied assistance message should be customized for your organization. The included message is only a sample.
1.4. Plan for exceptions	Exceptions happen when a user account needs access to a specific file share but they do not need access to everything that the security group has.
1.5. Determine how access-denied assistance is deployed	Access-denied assistance can be configured at the file server level or at the file share level.

## 1.2. Determine who should handle access requests

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.

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

<https://technet.microsoft.com/en-us/library/jj574182.aspx>

## QUESTION 57

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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

### **Target priority**

You can assign a priority to individual targets for a given namespace root or folder. This priority determines how the target is ordered in a referral. The options are:

- First among all targets
- Last among all targets
- First among targets of equal cost
- Last among targets of equal cost

It is important to note that setting target priority on a target will result in that target always being present in a referral, even in cases where you set the **Exclude targets outside of the client's site** option on the folder associated with the target.

If you want clients to always fail over to a particular server in the hub site, you can configure that hub server's target priority as **first among targets of equal cost**.

### **Referral ordering**

A referral is an ordered list of targets, transparent to the user, that a client receives from a domain controller or namespace server when the user accesses the namespace root or a folder with targets in the namespace. The client caches the referral for a configurable period of time.

Targets in the client's Active Directory site are listed first in a referral. (Targets given the target priority "first among all targets" will be listed before targets in the client's site.) The order in which targets outside of the client's site appear in a referral is determined by one of the following referral ordering methods:

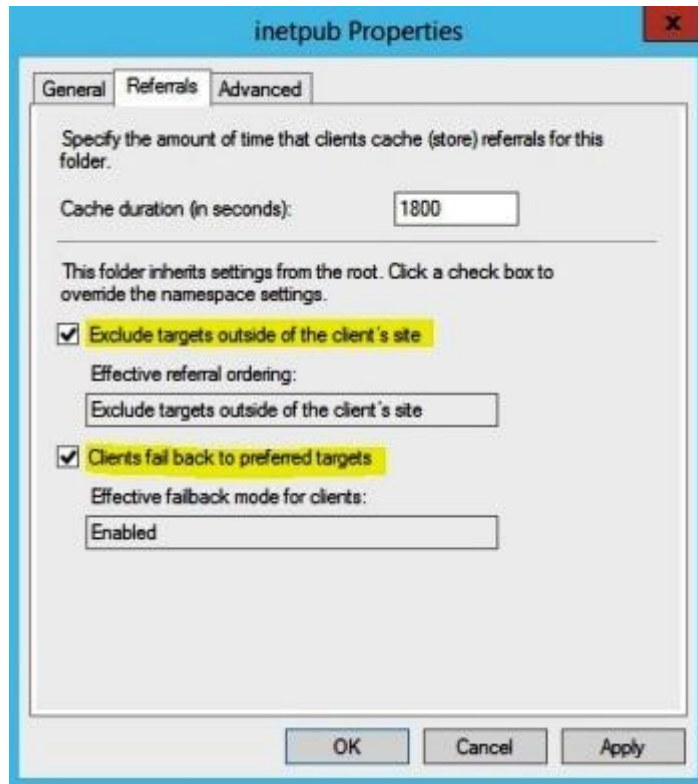
- Lowest cost
- Random order

- Exclude targets outside of the client's site

You can set referral ordering on the namespace root, and the ordering method applies to all folders with targets in the namespace. You can also override the namespace root's ordering method for individual folders with targets.

[https://technet.microsoft.com/en-us/library/cc772778\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772778(v=ws.10).aspx)

If you do not want clients to access folder targets outside of their site, you can override the ordering method for individual folders. To do this, right-click a folder with targets in the console tree, click **Properties**, click the **Referrals** tab, and then click **Exclude targets outside of the client's site**. Note that if no same-site targets are available, the client fails to access the folder because no folder targets are returned in the referral.



[https://technet.microsoft.com/en-us/library/cc732863\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732863(v=ws.10).aspx)

## QUESTION 58

You have a server named Server1.

You enable BitLocker Drive Encryption (BitLocker) on Server1. 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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

The **Set-TpmOwnerAuth** cmdlet 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.

<https://technet.microsoft.com/en-us/library/jj603120.aspx>

An owner authorization file is not simply a password. It is generated for a specific system. For more information on TPM, see the **Trusted Platform Module Technology Overview** in the TechNet library at:

<http://technet.microsoft.com/en-us/library/jj131725.aspx>

#### **QUESTION 59**

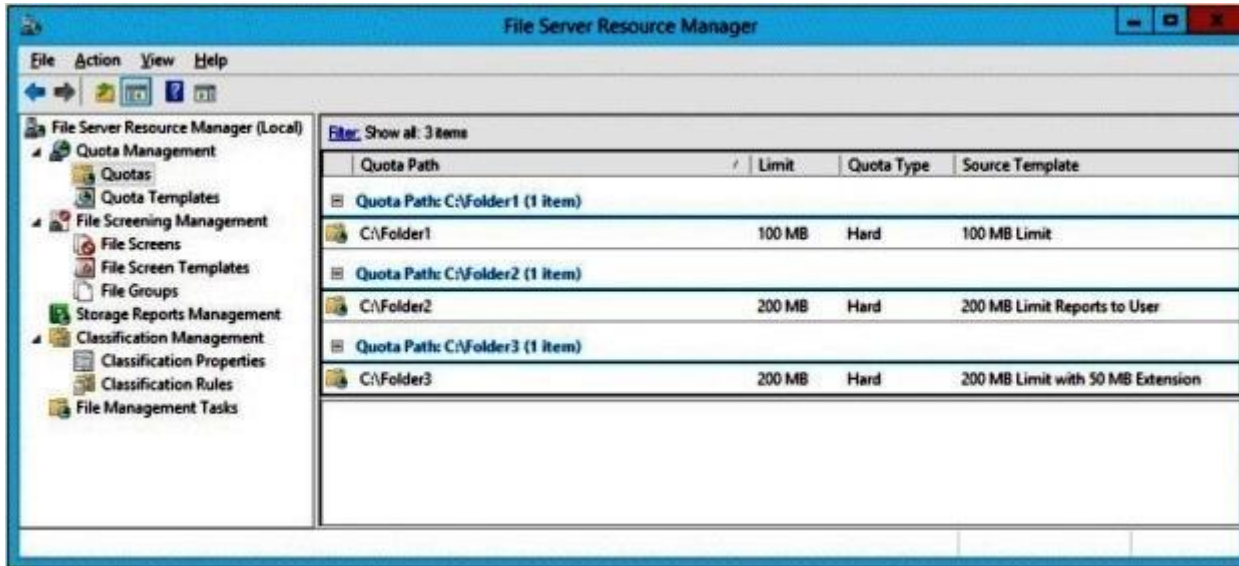
You have a file server that has the File Server Resource Manager role service installed.

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

You need to ensure that all of the folders in Folder1 have a 100-MB quota limit.

What should you do?

**Exhibit:**



- A. Run the Update-FsrmQuota cmdlet.
- B. Run the Update-FsrmAutoQuota cmdlet.
- C. Create a new quota for Folder1.
- D. Modify the quota properties of Folder1.

**Correct Answer: B**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

The **Update-FsrmAutoQuota** cmdlet updates the properties of an auto apply quota and the quotas that derive from the automatic quota. To change the properties of an auto apply quota, change the properties of the template from which the automatic quota is derived, and then use this cmdlet to update the properties of the auto apply quota.

Updating the properties of an auto apply quota is a long-running process. Update an auto apply quota only when you have changed the properties of the template from which the auto apply quota is derived.

<https://technet.microsoft.com/en-us/library/jj900582.aspx>

**QUESTION 60**

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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

Network Unlock must meet mandatory hardware and software requirements before the feature can automatically unlock domain joined systems. These requirements include:

- Supported Windows operating systems: Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2.
- Any supported operating system with UEFI DHCP drivers can be Network Unlock clients.
- **A server running the Windows Deployment Services (WDS) role on any supported server operating system.**

- BitLocker Network Unlock optional feature installed on any supported server operating system.
- A DHCP server, separate from the WDS server.
- Properly configured public/private key pairing.
- Network Unlock Group Policy settings configured.

<https://technet.microsoft.com/en-us/library/jj574173.aspx>

## QUESTION 61

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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

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.

[https://technet.microsoft.com/en-us/library/cc734419\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc734419(v=ws.10).aspx)

A *file screen template* defines a set of file groups to screen, the type of screening to perform (active or passive), and (optionally) a set of notifications that will be generated automatically when a user saves, or attempts to save, an unauthorized file.

File Server Resource Manager can send e-mail messages to administrators or specific users, log an event, execute a command or a script, or generate

reports. You can configure more than one type of notification for a file screen event.

By creating file screens exclusively from templates, you can centrally manage your file screens by updating the templates instead of replicating changes in each file screen. This feature simplifies the implementation of storage policy changes by providing one central point where you can make all updates.

<https://technet.microsoft.com/en-us/library/cc731318.aspx>

#### QUESTION 62

Your network contains an Active Directory domain named contoso.com. The domain contains a virtual machine named Server1 that runs Windows Server 2012 R2. Server1 has a dynamically expanding virtual hard disk that is mounted to drive E.

You need to ensure that you can enable BitLocker Drive Encryption (BitLocker) on drive E.

Which command should you run?

- A. `manage-bde -protectors -add c: -startup e:`
- B. `manage-bde -lock e:`
- C. `manage-bde -protectors -add e: -startupkey c:`
- D. `manage-bde -on e:`

**Correct Answer: C**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

#### **Manage-bde.exe**

Used to turn on or turn off BitLocker, specify unlock mechanisms, update recovery methods, and unlock BitLocker-protected data drives. This command-line tool can be used in place of the **BitLocker Drive Encryption** Control Panel item.

<https://technet.microsoft.com/en-us/library/ff829849.aspx>

#### **-protectors**

Manages the protection methods used for the BitLocker encryption key.

#### **-add**

Adds key protection methods as specified by using additional -add syntax and parameters.

#### **-startupkey**

Adds an external key protector for startup. You can also use **-sk** as an abbreviated version of this command.



<https://technet.microsoft.com/en-us/library/ff829848.aspx>

For thinly provisioned storage, such as a Dynamic Virtual Hard Disk (VHD), BitLocker runs in Used Disk Space Only encryption mode. Full Encryption requires an end marker for the volume and dynamically expanding VHDs do not have a static end of volume marker.

<https://technet.microsoft.com/en-us/library/dn383585.aspx>

The following example illustrates enabling BitLocker on a computer without a TPM chip. Before beginning the encryption process you must create the startup key needed for BitLocker and save it to the USB drive. When BitLocker is enabled for the operating system volume, the BitLocker will need to access the USB flash drive to obtain the encryption key (in this example, the drive letter E represents the USB drive). You will be prompted to reboot to complete the encryption process.

```
manage-bde -protectors -add C: -startupkey E:
manage-bde -on C:
```

<https://technet.microsoft.com/en-us/library/jj647767.aspx>

### QUESTION 63

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

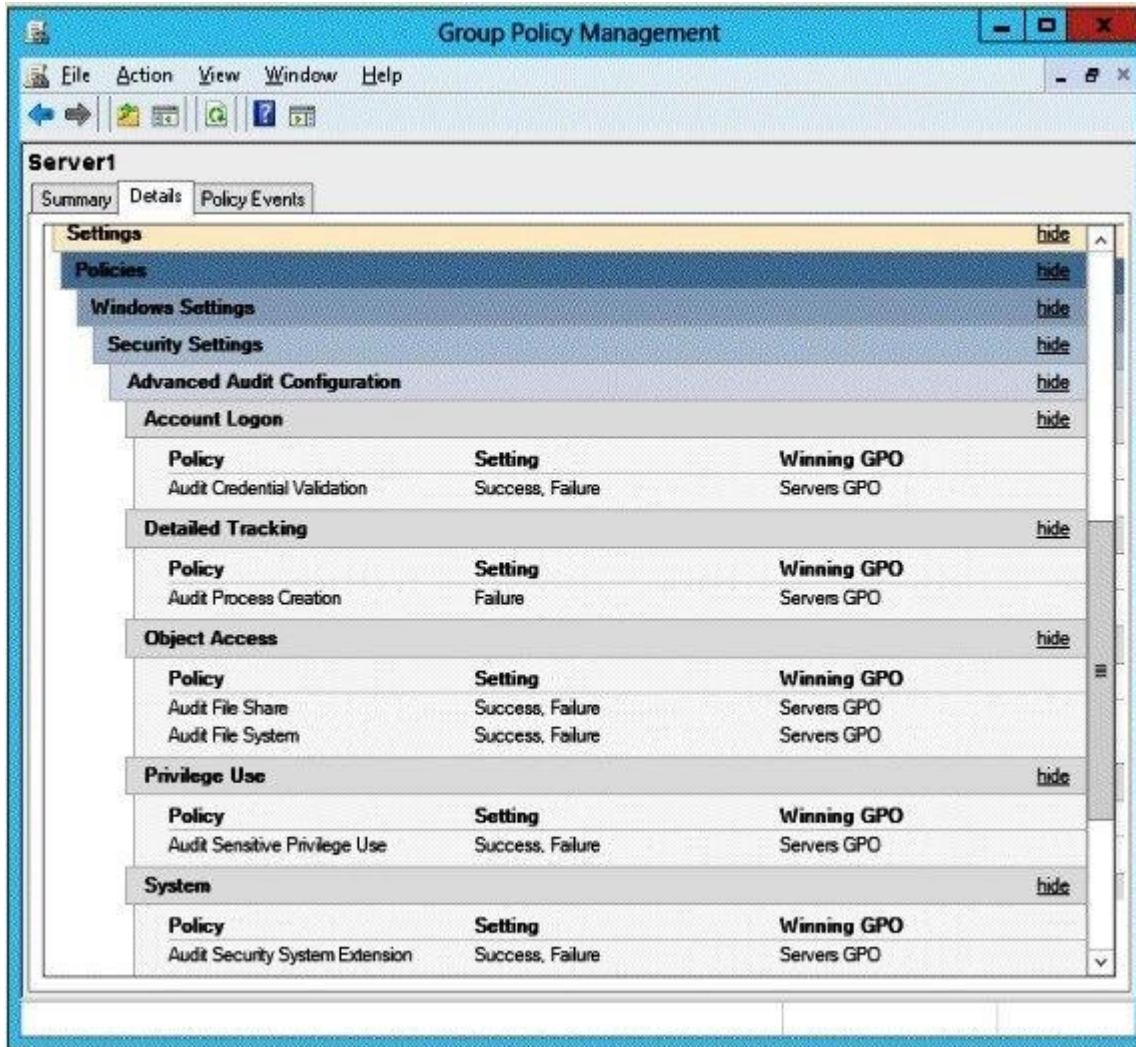
You view the effective policy settings of Server1 as shown in the exhibit. (Click the Exhibit button.)

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?

**Exhibit:**



- 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: Configure File and Print Services

### Explanation

#### Explanation/Reference:

#### Create and verify an audit policy that provides the reason for object access

One of the most common auditing needs is to track access to a particular file or folder. For example, you might need to identify an activity such as users writing to files that they should not have had access to. By enabling "reason for access" auditing, not only will you be able to track this type of activity, but you will also be able to identify the exact access control entry that allowed the undesired access, which can significantly simplify the task of modifying access control settings to prevent similar undesired object access in the future.

To configure, apply, and validate a reason for object access policy, you must:

- Configure the file system audit policy
- Enable auditing for a file or folder
- Enable the handle manipulation audit policy
- Ensure that Advanced Audit Policy Configuration settings are not overwritten
- Update Group Policy settings
- Review and verify the reason for access auditing data

#### To enable auditing for a file or folder

1. Log on to CONTOSO-CLNT as a member of the local **Administrators** group.
2. Create a new folder or .txt document.
3. Right-click the new object, click **Properties**, and click the **Security** tab.



4. Click **Advanced**, and then click the **Auditing** tab.



5. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
6. Click **Add**, type a user name or computer name in the format **contoso\user1**, and then click **OK**.
7. In the **Auditing Entries for** dialog box, select the permissions that you want to audit, such as **Full Control** or **Delete**.
8. Click **OK** four times to complete configuration of the object SACL.

In Windows 7 and Windows Server 2008 R2, the reason that someone is granted or denied access is added to the open handle event. This makes it possible for administrators to understand why someone was able to open a file, folder, or file share for a specific access. To enable this functionality, the handle manipulation audit policy also needs to be enabled to show **Success** access attempts that were allowed and **Failure** access attempts that were denied.

<https://technet.microsoft.com/en-us/library/dn311488.aspx>

## QUESTION 64

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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

### **Using BitLocker with Clustered Volumes**

BitLocker on volumes within a cluster are managed based on how the cluster service "views" the volume to be protected. The volume can be a physical disk resource such as a logical unit number (LUN) on a storage area network (SAN) or network attached storage (NAS).

Alternatively, the volume can be a cluster-shared volume, a shared namespace, within the cluster. Windows Server 2012 has expanded the CSV architecture, now known as CSV2.0, to enable support for BitLocker. When using BitLocker with volumes designated for a cluster, the volume will need to turn on BitLocker before its addition to the storage pool within cluster or put the resource into maintenance mode before BitLocker operations will complete.

Windows PowerShell or the manage-bde command line interface is the preferred method to manage BitLocker on CSV2.0 volumes. This is recommended over the BitLocker Control Panel item because CSV2.0 volumes are mount points. Mount points are an NTFS object that is used to provide an entry point to other volumes. Mount points do not require the use of a drive letter. Volumes that lack drive letters do not appear in the BitLocker Control Panel item. Additionally, the new Active Directory-based protector option required for cluster disk resource or CSV2.0 resources is not available in the Control Panel item.

<https://technet.microsoft.com/en-us/library/dn383585.aspx>

The **Add-BitLockerKeyProtector** cmdlet adds a protector for the volume key of the volume protected with BitLocker Drive Encryption.

**-MountPoint<String[]>**

Specifies an array of drive letters or BitLocker volume objects. This cmdlet adds a key protector to the volumes specified. To obtain a BitLocker volume object, use the Get-BitLockerVolume cmdlet.

**-ADAccountOrGroupProtector**

Indicates that BitLocker uses an AD DS account as a protector for the volume encryption key.

**-Service**

Indicates that the system account for this computer unlocks the encrypted volume.

<https://technet.microsoft.com/en-us/library/jj649835.aspx>

**QUESTION 65**

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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

Consider the following scenario:

You want to force the non-authoritative synchronization of SYSVOL on a domain controller. In the File Replication Service (FRS), this was controlled through the **D2** and **D4** data values for the **Burflags** registry values, but these values do not exist for the Distributed File System Replication (DFSR) service. You cannot use the DFS Management snap-in (Dfsmgmt.msc) or the Dfsradmin.exe command-line tool to achieve this. Unlike custom DFSR replicated folders, SYSVOL is intentionally protected from any editing through its management interfaces to prevent accidents.

**How to perform a non-authoritative synchronization of DFSR-replicated SYSVOL (like "D2" for FRS)**

1. In the **ADSIEDIT.MSC** tool modify the following distinguished name (DN) value and attribute on each of the domain controllers that you want to make non-authoritative:

CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain>

msDFSR-Enabled=**FALSE**

2. Force Active Directory replication throughout the domain.
3. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:

**DFSRDIAG POLLAD**

4. You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated.
5. On the same DN from Step 1, set:

msDFSR-Enabled=**TRUE**

6. Force Active Directory replication throughout the domain.
7. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:

**DFSRDIAG POLLAD**

8. 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.

<http://support.microsoft.com/kb/2218556>

## QUESTION 66

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-DfsrClone cmdlets.

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: Configure File and Print Services**

**Explanation**



## Explanation/Reference:

### To export a clone of a DFS Replication database

1. Validate that all the existing replicated folders on the volume that stores the replicated folder that you want to preseed are in the **Normal**, noninitial sync state. Replicated folders in other states are skipped during cloning.

To validate the state, examine the DFS Replication event log to ensure that all replicated folders have a 4112 or 4104 event.

All replicated folders listed for that computer will show state 4 (that is, **Normal**) if they have completed the initial build or initial sync, and they are ready to clone.

2. Export the cloned database and volume configuration XML by running the following sample command from an elevated Windows PowerShell session:

```
$DfsrCloneVolume = "H:"  
$DfsrCloneDir = "\DfsrClone"  
  
New-Item -Path $DfsrCloneVolume\$DfsrCloneDir -Type Directory  
Export-DfsrClone -Volume $DfsrCloneVolume -Path $DfsrCloneVolume\$DfsrCloneDir
```

Although the **Export-DfsrClone** cmdlet does not return any output until cloning completes, you can safely close the Windows PowerShell session after running the command. The DFS Replication service performs the processing while the command synchronously waits for the result. If you close the Windows PowerShell console or exit the command, you can continue to see progress by examining the DFS Replication event log, the DFS Replication debug logs, or by using the **Get-DfsrCloneState** cmdlet.

3. After completion, make a note of the **Robocopy** sample commands that are displayed by the **Export-DfsrClone** cmdlet. You can later use these commands to copy the data to the destination server. You can also use **Export-DfsrClone** with the **-WhatIf** parameter to see the Robocopy samples without performing cloning, for example:

```
Robocopy.exe "H:\DfsrClone" "<destination path>" /B  
Robocopy.exe "H:\RF01" "<destination path>" /E /B /COPYALL /R:6 /W:5 /MT:64 /XD DfsrPrivate /TEE /LOG  
+:preseed.log
```

4. Wait for a DFS Replication Event 2402 in the DFS Replication event log, which indicates that the export completed successfully. You can also use the **Get-DfsrCloneState** cmdlet to see the export status. The cmdlet returns **Ready** when the export process completes.

<https://technet.microsoft.com/en-us/library/dn482443.aspx>

### QUESTION 67

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

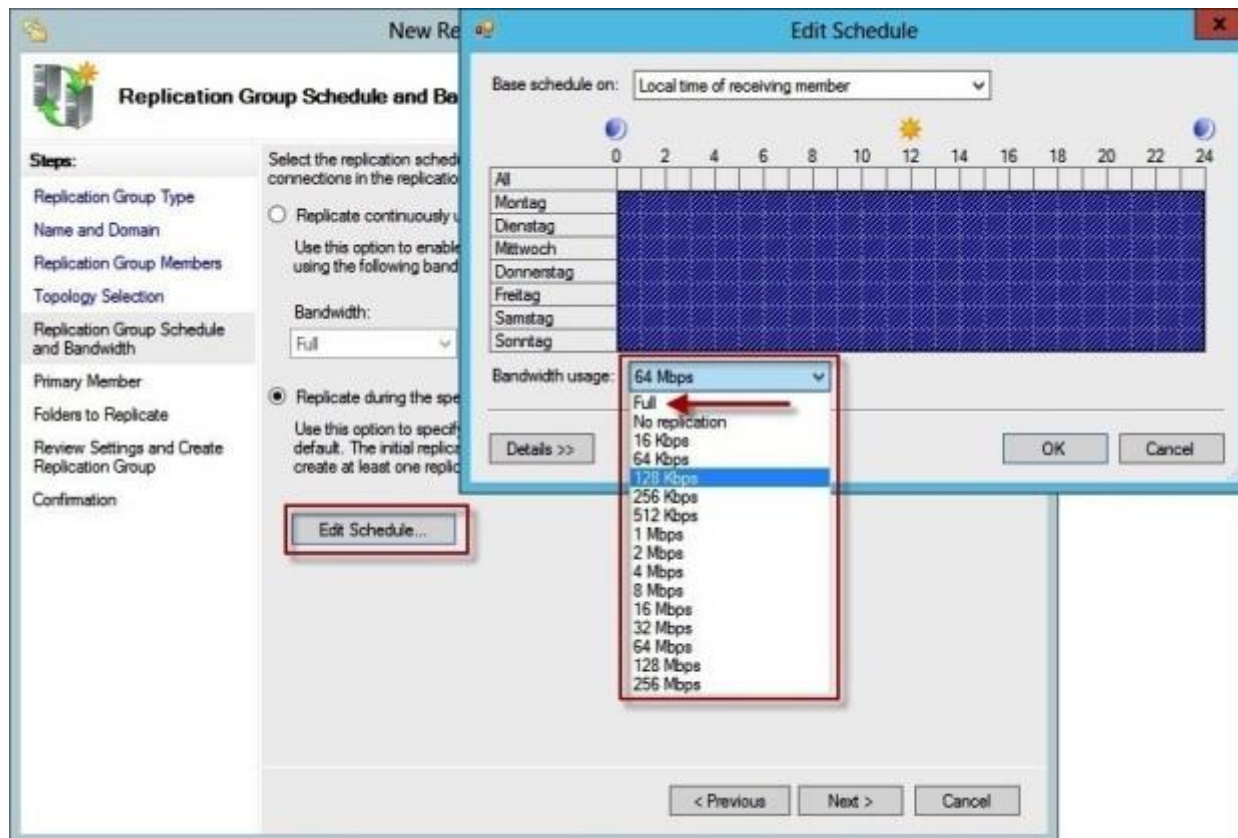
**Correct Answer: D**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

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.



[https://technet.microsoft.com/en-us/library/cc773238\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc773238(v=ws.10).aspx)

#### QUESTION 68

You have a file server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed. Files created by users in the human resources department are assigned the Department classification property automatically.

You are configuring a file management task named Task1 to remove user files that have not been accessed for 60 days or more. You need to ensure that Task1 only removes files that have a Department classification property of human resources. The solution must minimize administrative effort.

What should you configure on Task1?

- A. Configure a file screen.
- B. Create a condition.

- C. Create a classification rule.
- D. Create a custom action.

**Correct Answer: B**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

## **Create a File Expiration Task**

The following procedure guides you through the process of creating a file management task for expiring files. File expiration tasks are used to automatically move all files that match certain criteria to a specified expiration directory, where an administrator can then back those files up and delete them.

When a file expiration task is run, a new directory is created within the expiration directory, grouped by the server name on which the task was run.

The new directory name is based on the name of the file management task and the time it was run. When an expired file is found it is moved into the new directory, while preserving its original directory structure.

### **To create a file expiration task**

1. Click the **File Management Tasks** node.
2. Right-click **File Management Tasks**, and then click **Create File Management Task** (or click **Create File Management Task** in the **Actions** pane). This opens the **Create File Management Task** dialog box.
3. On the **General** tab, enter the following information:
  - **Name.** Enter a name for the new task.
  - **Description.** Enter an optional descriptive label for this task.
  - **Scope.** Add the directories that this task should operate on by using the **Add** button. Optionally, directories can be removed from the list using the **Remove** button. The file management task will apply to all folders and their subfolders in this list.
4. On the **Action** tab, enter the following information:
  - **Type.** Select **File Expiration** from the drop-down box.
  - **Expiration Directory.** Select a directory where files will be expired to.
5. Optionally, on the **Notification** tab, click **Add** to send e-mail notifications, log an event, or run a command or script a specified minimum number of

days before the task performs an action on a file.

6. Optionally, use the **Report** tab to generate one or more logs or storage reports.

7. Optionally, use the **Condition** tab to run this task only on files that match a defined set of conditions. The following settings are available:

- **Property conditions.** Click **Add** to create a new condition based on the file's classification. This will open the Property Condition dialog box, which allows you to select a property, an operator to perform on the property, and the value to compare the property against. After clicking **OK**, you can then create additional conditions, or edit or remove an existing condition.
- **Days since file was last modified.** Click the check box and then enter a number of days into the spin box. This will result in the file management task only being applied to files that have not been modified for more than the specified number of days.
- **Days since file was last accessed.** Click the check box and then enter a number of days into the spin box. If the server is configured to track timestamps for when files were last accessed, this will result in the file management task only being applied to files that have not been accessed for more than the specified number of days. If the server is not configured to track accessed times, this condition will be ineffective.
- **Days since file was created.** Click the check box and then enter a number of days into the spin box. This will result in the task only being applied to files that were created at least the specified number of days ago.
- **Effective starting.** Set a date when this file management task should start processing files. This option is useful for delaying the task until you have had a chance to notify users or make other preparations in advance.

8. On the **Schedule** tab, click **Create Schedule**, and then in the **Schedule** dialog box, click **New**. This displays a default schedule set for 9:00 A.M. daily, but you can modify the default schedule. When you have finished configuring the schedule, click **OK**.

9. Click **OK**.

<https://technet.microsoft.com/en-us/library/dd759233.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. Server1 has the File Server Resource Manager role service installed.

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

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

What should you do?

**Exhibit:**

**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.

Additional E-mail Headers...

OK   Cancel

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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

### **Setting optional notification thresholds**

When storage in a volume or folder reaches a threshold level that you define, File Server Resource Manager can send e-mail messages to administrators or specific users, log an event, execute a command or a script, or generate reports. You can configure more than one type of notification for each threshold, and you can define multiple thresholds for any quota (or quota template). By default, no notifications are generated.

To send e-mail notifications and configure the storage reports with parameters that are appropriate for your server environment, you must first set the general File Server Resource Manager options.

### **To configure notifications that File Server Resource Manager will generate at a quota threshold**

1. In the **Create Quota Template** dialog box, under **Notification thresholds**, click **Add**. The **Add Threshold** dialog box appears.
2. To set a quota limit percentage that will generate a notification:

In the **Generate notifications when usage reaches (%)** text box, enter a percentage of the quota limit for the notification threshold. (The default percentage for the first notification threshold is 85 percent.)

3. To configure e-mail notifications:

On the **E-mail Message** tab, set the following options:

To notify administrators when a threshold is reached, select the **Send e-mail to the following administrators** check box, and then enter the names of the administrative accounts that will receive the notifications. Use the format *account@domain*, and use semicolons to separate multiple accounts.

To send e-mail to the person who saved the file that reached the quota threshold, select the **Send e-mail to the user who exceeded the threshold** check box.

To configure the message, edit the default subject line and message body that are provided. The text that is in brackets inserts variable information about the quota event that caused the notification. For example, the **[Source Io Owner]** variable inserts the name of the user who saved the file that reached the quota threshold. To insert additional variables in the text, click **Insert Variable**.

To configure additional headers (including From, Cc, Bcc, and Reply-to), click **Additional E-mail Headers**.



4. To log an event:

On the **Event Log** tab, select the **Send warning to event log** check box, and edit the default log entry.

5. To run a command or script:

On the **Command** tab, select the **Run this command or script** check box. Then type the command, or click **Browse** to search for the location where the script is stored. You can also enter command arguments, select a working directory for the command or script, or modify the command security setting.

6. To generate one or more storage reports:

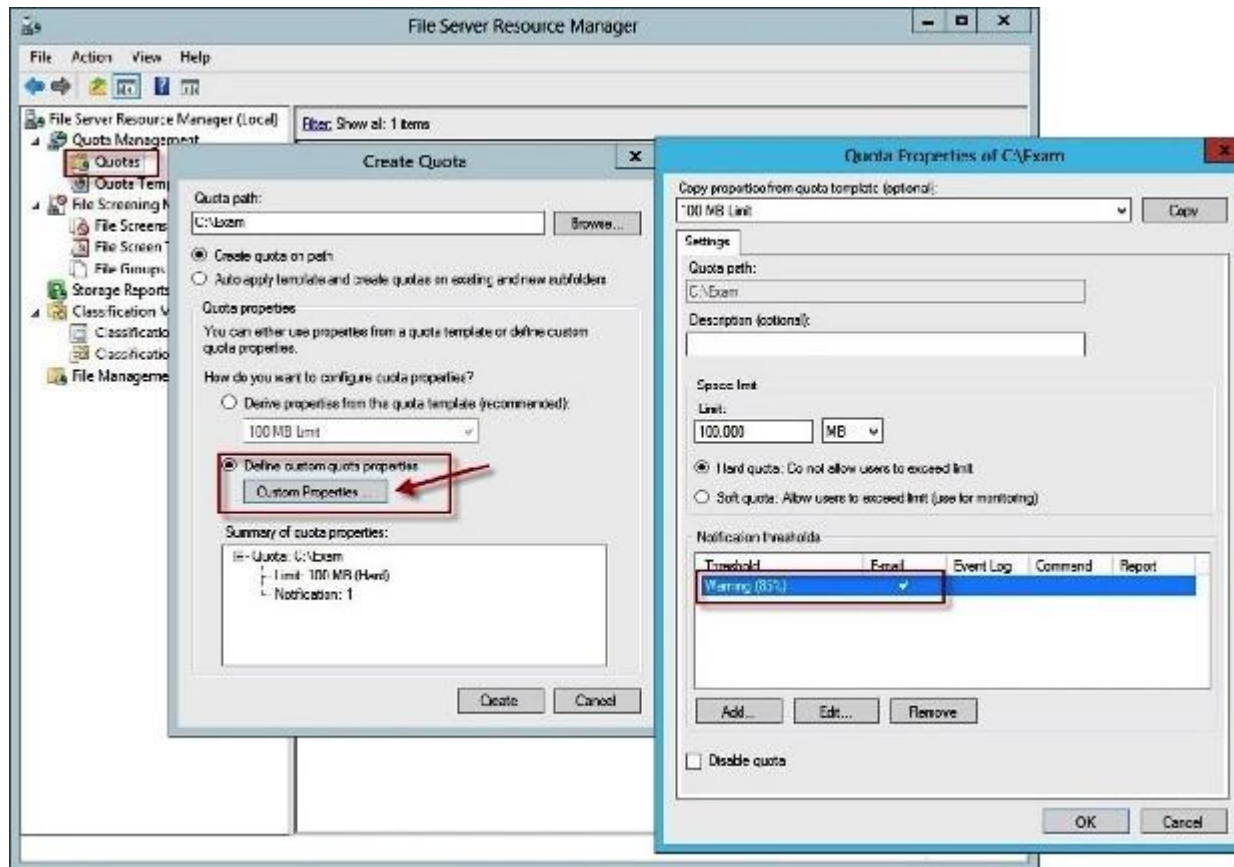
On the **Report** tab, select the **Generate reports** check box, and then select which reports to generate. (You can choose one or more administrative e-mail recipients for the report or e-mail the report to the user who reached the threshold.)

The report is saved in the default location for incident reports, which you can modify in the **File Server Resource Manager Options** dialog box.

7. Click **OK** to save your notification threshold.

8. Repeat these steps if you want to configure additional notification thresholds for the quota template.





<https://technet.microsoft.com/en-us/library/cc725711.aspx>

#### QUESTION 70

Your company has a main office and a branch office. The main office is located in Seattle. The branch office is located in Montreal. Each office is configured as an Active Directory site. The network contains an Active Directory domain named adatum.com. The Seattle office contains a file server named Server1. The Montreal office contains a file server named Server2. The servers run Windows Server 2012 R2 and have the File and Storage Services server role, the DFS Namespaces role service, and the DFS Replication role service installed.

Server1 and Server2 each have a share named Share1 that is replicated by using DFS Replication. You need to ensure that users connect to the replicated folder in their respective office when they connect to \\contoso.com\Share1.

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

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

**Correct Answer:** BCE

**Section:** Configure File and Print Services

**Explanation**

**Explanation/Reference:**

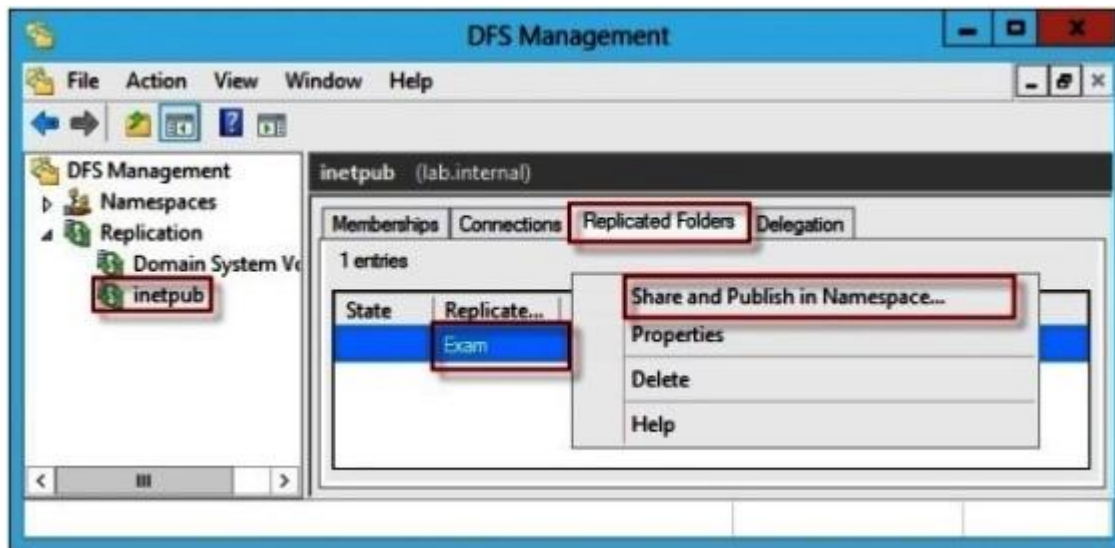
To **create a new namespace**, you can use Server Manager to create the namespace when you install the DFS Namespaces role service. You can also use the New-DfsnRoot cmdlet from a Windows PowerShell session. The DFSN Windows PowerShell module was introduced in Windows Server 2012.

<https://technet.microsoft.com/en-us/library/cc731531.aspx>

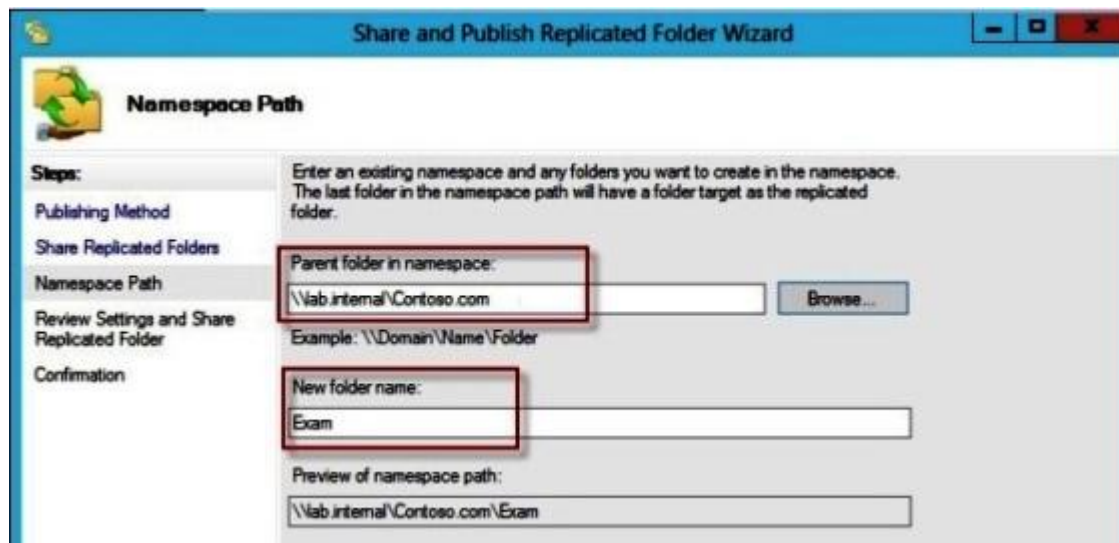
To enable file sharing on a replicated folder and optionally add the folder to a DFS namespace, use the following procedures:

**To share a replicated folder**

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

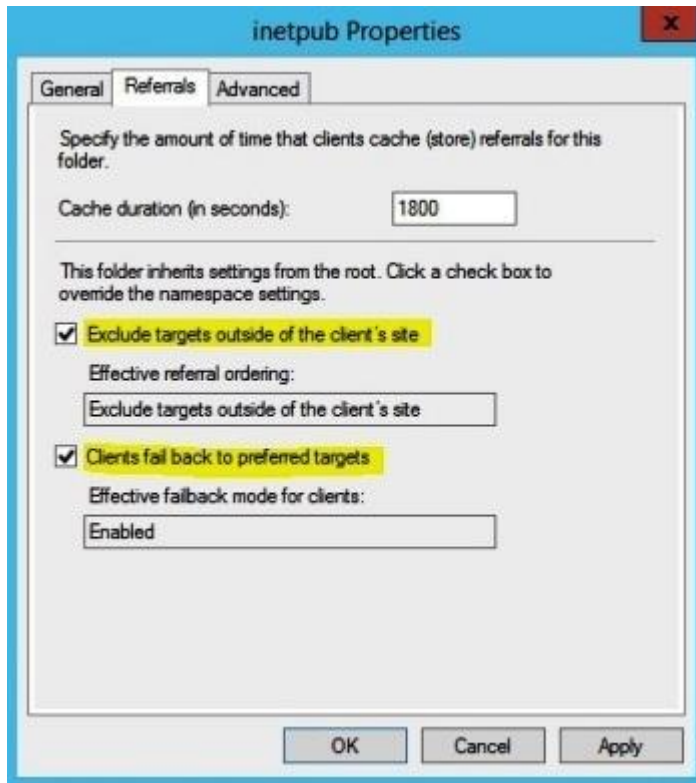


4. On the **Publishing Method** page, choose **Share the replicated folder** or **Share and Publish in Namespace** , and then follow the steps in the wizard.



<https://technet.microsoft.com/en-us/library/cc772379.aspx>

If you do not want clients to access folder targets outside of their site, you can override the ordering method for individual folders. To do this, right-click a folder with targets in the console tree, click **Properties**, click the **Referrals** tab, and then click **Exclude targets outside of the client's site**. Note that if no same-site targets are available, the client fails to access the folder because no folder targets are returned in the referral.



[https://technet.microsoft.com/en-us/library/cc732863\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732863(v=ws.10).aspx)

#### QUESTION 71

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**

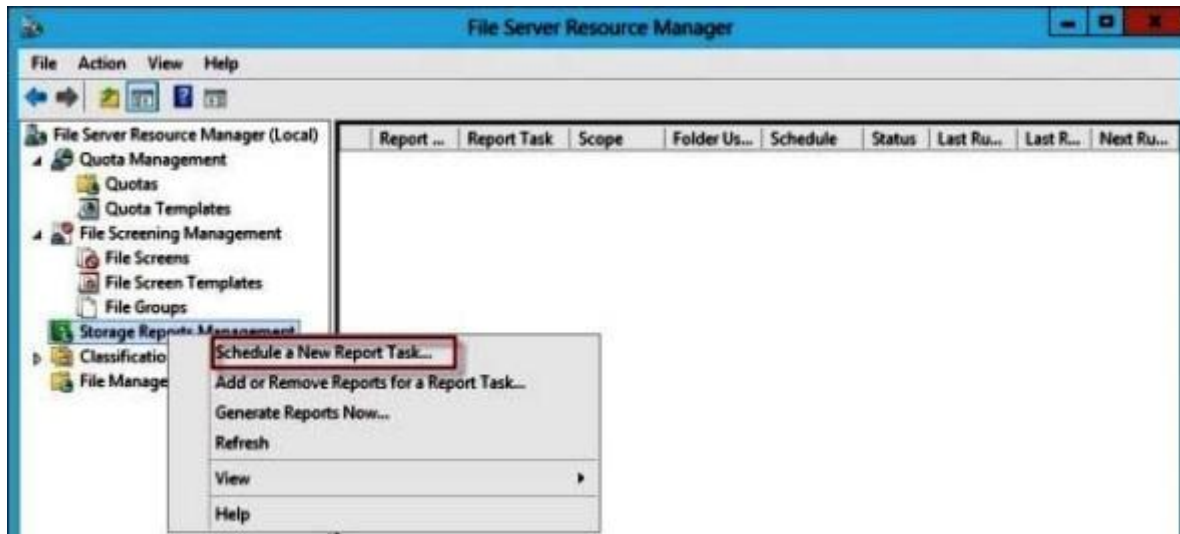
**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

On the **Storage Reports Management** node of the File Server Resource Manager MMC snap-in, you can perform the following tasks:

- Schedule periodic storage reports that allow you to identify trends in disk usage.
- Monitor attempts to save unauthorized files for all users or a selected group of users.
- Generate storage reports instantly.



<https://technet.microsoft.com/en-us/library/cc771212.aspx>

## QUESTION 72

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: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

Remote differential compression (RDC) is a “diff-over-the-wire” protocol that can be used to efficiently update files over a limited-bandwidth network. RDC detects insertions, removals, re-arrangements of data in files, enabling DFS Replication to replicate only the changes when files are updated.

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.

[https://technet.microsoft.com/en-us/library/cc758825\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc758825(v=ws.10).aspx)

### **QUESTION 73**

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed. Each time a user receives an access-denied message after attempting to access a folder on Server1, an email notification is sent to a distribution list named DL1.

You create a folder named Folder1 on Server1, and then you configure custom NTFS permissions for Folder 1. You need to ensure that when a user receives an access-denied message while attempting to access Folder1, an email notification is sent to a distribution list named DL2. The solution must not prevent DL1 from receiving notifications about other access-denied messages.

What should you do?

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

**Correct Answer: C**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

There are a few considerations and decisions that should be made before you deploy access-denied assistance.

Use the following table to plan your access-denied assistance deployment in your organization.

Task	Description
1.1 Determine the access-denied assistance model	Determine whether your organization should use an email model or a Web services model for access-denied assistance.
1.2. Determine who should handle access requests	You can assign each file share an owner distribution list that will receive access requests.
1.3. Customize the access-denied assistance message	The access-denied assistance message should be customized for your organization. The included message is only a sample.
1.4. Plan for exceptions	Exceptions happen when a user account needs access to a specific file share but they do not need access to everything that the security group has.
1.5. Determine how access-denied assistance is deployed	Access-denied assistance can be configured at the file server level or at the file share level.

### **1.2. Determine who should handle access requests**

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.

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

<https://technet.microsoft.com/en-us/library/jj574182.aspx>

**QUESTION 74**

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**

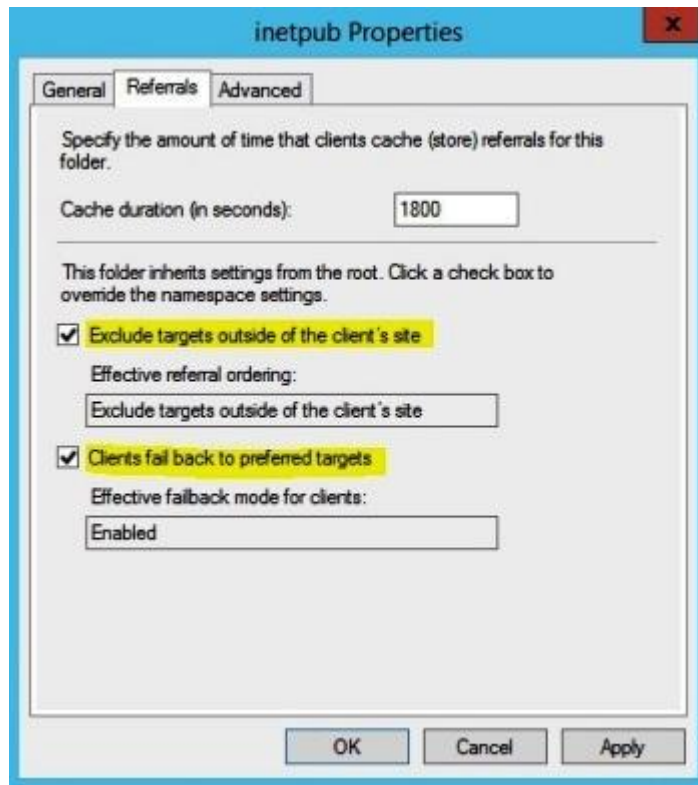
**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

If you do not want clients to access folder targets outside of their site, you can override the ordering method for individual folders. To do this, right-click a folder with targets in the console tree, click **Properties**, click the **Referrals** tab, and then click **Exclude targets outside of the client's site**. Note that if no same-site targets are available, the client fails to access the folder because no folder targets are returned in the referral.





[https://technet.microsoft.com/en-us/library/cc732863\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732863(v=ws.10).aspx)

#### QUESTION 75

Your network contains an Active Directory domain named adatum.com. The domain contains a domain controller named DC1.

On DC1, you create a new volume named E. You restart DC1 in Directory Service Restore Mode. You open ntdsutil.exe and you set NTDS as the active instance. You need to move the Active Directory logs to E:\NTDS.

Which Ntdsutil context should you use?

- A. IFM
- B. Configurable Settings
- C. Partition management
- D. Files

**Correct Answer: D**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). You can use the **ntdsutil** commands to perform database maintenance of AD DS, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled. This tool is intended for use by experienced administrators.

Command: **files**

Description: Manages AD DS or AD LDS database files.

<https://technet.microsoft.com/en-us/library/cc753343.aspx>

#### **QUESTION 76**

Your network contains an Active Directory domain named contoso.com. The domain does not contain a certification authority (CA). All servers run Windows Server 2012 R2. All client computers run Windows 8.

You need to add a data recovery agent for the Encrypting File System (EFS) to the domain.

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

- A. From Windows PowerShell, run Get-Certificate.
- B. From the Default Domain Controllers Policy, select Create Data Recovery Agent.
- C. From the Default Domain Policy, select Add Data Recovery Agent.
- D. From a command prompt, run cipher.exe.
- E. From the Default Domain Policy, select Create Data Recovery Agent.
- F. From the Default Domain Controllers Policy, select Add Data Recovery Agent.

**Correct Answer: AC**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

#### **CONFIGURING THE EFS RECOVERY AGENT**

If for some reason, a person leaves the company or a person loses the original key and the encrypted files cannot be read, you can set up a **data**

**recovery agent (DRA)** that can recover EFS-encrypted files for a domain. To define DRAs, you can use Active Directory group policies to configure one or more user accounts as DRAs for your entire organization. However, to accomplish this, you need to have an enterprise CA.

## ADD RECOVERY AGENTS FOR EFS

To add new users as recovery agents, assign the EFS recovery certificates issued by the enterprise CA to the user account, and then perform the following steps:

1. Log in as the DRA account.
2. Open the **Group Policy Management console**.
3. Expand **Forest, Domains**, and then the **name of your domain**.
4. Right-click the **Default Domain Policy** and click **Edit**.
5. Expand **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**.
6. Right-click **Encrypting File System**, and select **Create Data Recovery Agent**.
7. Click **Encrypting File System** and notice the certificates that are displayed.
8. Close the **Group Policy Editor**.
9. Close **Group Policy Management console**.

(*Administering Windows Server® 2012, Exam 70-411*, Microsoft® Official Academic Course, Patrick Regan, 2013, John Wiley & Sons, Inc., p. 196.)

The **Get-Certificate** cmdlet can be used to submit a certificate request and install the resulting certificate, install a certificate from a pending certificate request, and enroll for ldap. If the request is issued, then the returned certificate is installed in the store determined by the **CertStoreLocation** parameter and return the certificate in the EnrollmentResult structure with status Issued. If the request is made pending, then the request is installed in the machine REQUEST store and a request is returned in the EnrollmentResult structure with status Pending.

<https://technet.microsoft.com/en-us/library/hh848632>

## QUESTION 77

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

Domain Controller Name	Operating System	Operations Master Role
DC1	Windows Server 2008 R2	PDC Emulator Infrastructure Master
DC2	Windows Server 2008 R2	RID Master
DC3	Windows Server 2012 R2	Schema Master

You are creating a Distributed File System (DFS) namespace as shown in the exhibit. You need to identify which configuration prevents you from

creating a DFS namespace in Windows Server 2008 mode.

Which configuration should you identify?

**Exhibit:**

**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

- A. The location of the PDC emulator role
- B. The functional level of the domain

- C. The operating system on Server1 and Server3
- D. The location of the RID master role

**Correct Answer: B**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

Access-based enumeration hides files and folders that users do not have permission to access. By default, this feature is not enabled for DFS namespaces. You can enable access-based enumeration of DFS folders by using DFS Management. To control access-based enumeration of files and folders in folder targets, you must enable access-based enumeration on each shared folder by using Share and Storage Management.

To enable access-based enumeration on a namespace, all namespace servers must be running Windows Server 2008 or newer. Additionally, domain-based namespaces must use the Windows Server 2008 mode.

If you upgrade the domain functional level to Windows Server 2008 while there are existing domain-based namespaces, DFS Management will allow you to enable access-based enumeration on these namespaces. However, you will not be able to edit permissions to hide folders from any groups or users unless you migrate the namespaces to the Windows Server 2008 mode. For more information, see **Migrate a Domain-based Namespace to Windows Server 2008 Mode**.

<https://technet.microsoft.com/en-us/library/dd759150.aspx>

#### **QUESTION 78**

Your domain has a Windows 8.1 computer name Computer1 using BitLocker. The E:\ drive is encrypted and currently locked.

You need to unlock the E:\ drive with the recovery key stored on C:\.

What should you run?

- A. Unlock-BitLocker
- B. Suspend-BitLocker
- C. Enable-BitLockerAutoUnloc
- D. Disable-BitLocker

**Correct Answer: A**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

The **Unlock-BitLocker** cmdlet restores access to encrypted data on a volume that uses BitLocker Drive Encryption. You can use the Lock-BitLocker cmdlet to prevent access.

In order to restore access, provide one of the following key protectors for the volume:

- Active Directory Domain Services (AD DS) account
- Password
- Recovery key
- Recovery password

<https://technet.microsoft.com/en-us/library/jj649833.aspx>

#### QUESTION 79

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1. The File Server Resource Manager role service is installed on Server1. All servers run Windows Server 2012 R2. A Group Policy object (GPO) named GPO1 is linked to the organizational unit (OU) that contains Server1.

The settings in GPO1 are configured as shown in the exhibit. (Click the Exhibit button.)

Server1 contains a folder named Folder1. Folder1 is shared as Share1.

You attempt to configure access-denied assistance on Server1, but the Enable access-denied assistance option cannot be selected from File Server Resource Manager. You need to ensure that you can configure access- denied assistance on Server1 manually by using File Server Resource Manager.

What should you do?

**Exhibit:**



- A. Set the Customize message for Access Denied errors policy setting to Enabled for GPO1
- B. Set the Enable access-denied assistance on client for all file types policy setting to Enabled for GPO1
- C. Set the Customize message for Access Denied errors policy setting to Not Configured for GPO1
- D. Set the Enable access-denied assistance on client for all file types policy setting to Disabled for GPO1

**Correct Answer: C**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

You can configure access-denied assistance within a domain by using Group Policy, or you can configure the assistance individually on each file server by using the File Server Resource Manager console. You can also change the access-denied message for a specific shared folder on a file server.

<https://technet.microsoft.com/en-us/library/hh831402.aspx>

Within Group Policy, if the **Customize message for Access Denied errors** setting is set to the **Enabled** state, then the setting will be managed by Group Policy only. If the setting state is **Disabled**, it will be non-functional. However, if the setting state is set as **Not configured**, then it will be a configuration option available to be configured using the **File Server Resource Manager** console.

#### **QUESTION 80**

Your network contains an Active Directory domain named adatum.com. All domain controllers run Windows Server 2008 R2. The domain contains a file server named Server6 that runs Windows Server 2012 R2. Server6 contains a folder named Folder1. Folder1 is shared as Share1.

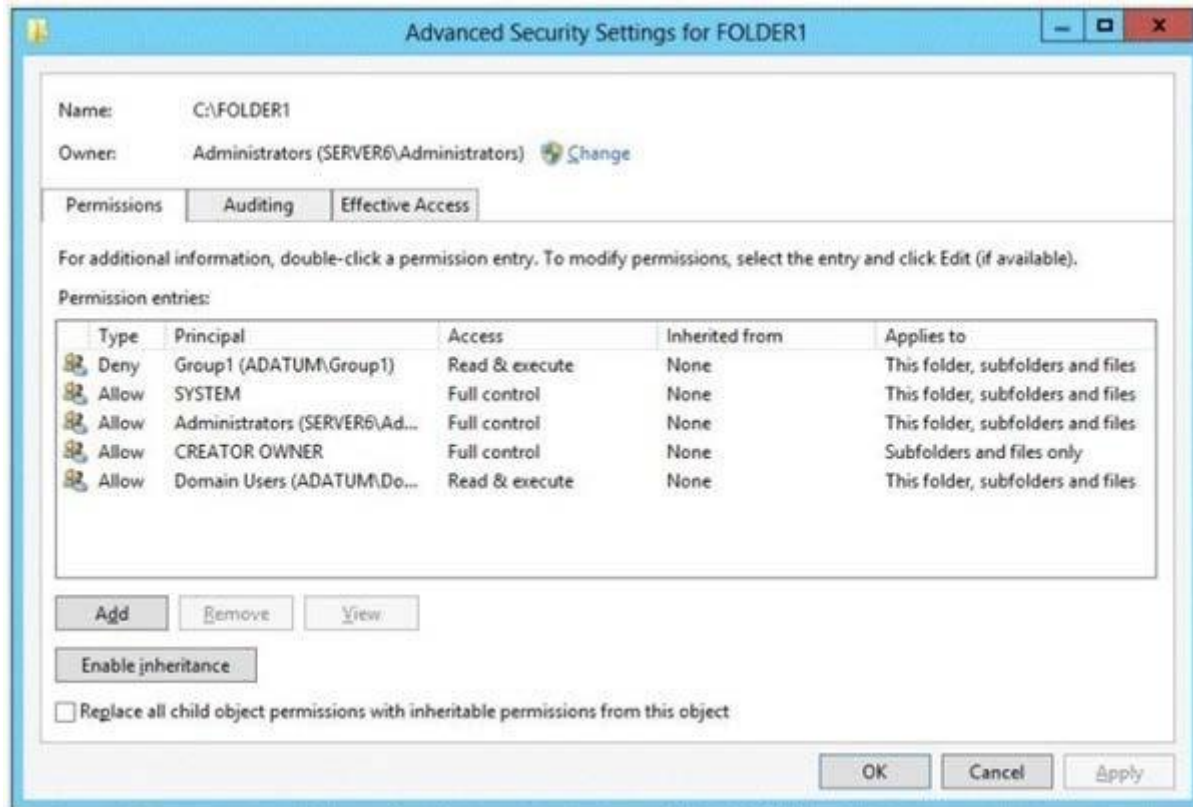
The NTFS permissions on Folder1 are shown in the exhibit. (Click the Exhibit button.)

The domain contains two global groups named Group1 and Group2.

You need to ensure that only users who are members of both Group1 and Group2 are denied access to Folder1.

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

**Exhibit:**



- A. Remove the Deny permission for Group1 from Folder1
- B. Deny Group2 permission to Folder1
- C. Install a domain controller that runs Windows Server 2012 R2
- D. Create a conditional expression
- E. Deny Group2 permission to Share1
- F. Deny Group1 permission to Share1

**Correct Answer:** AD

**Section:** Configure File and Print Services

**Explanation**

**Explanation/Reference:**



Windows Server 2012 takes advantage of conditional access permission entries by inserting user claims, device claims, and resource properties, into conditional expressions. Windows Server 2012 security evaluates these expressions and allows or denies access based on results of the evaluation. Securing access to resources through claims is known as claims-based access control. Claims-based access control works with traditional access control to provide an additional layer of authorization that is flexible to the varying needs of the enterprise environment.

<http://social.technet.microsoft.com/wiki/contents/articles/14269.introducing-dynamic-access-control.aspx>

#### QUESTION 81

You have 20 servers that run Windows Server 2012 R2.

You need to create a Windows PowerShell script that registers each server in Microsoft Azure Online Backup and sets an encryption passphrase.

Which two PowerShell cmdlets should you run in the script? (Each correct answer presents part of the solution. Choose two.)

- A. New-OBPolicy
- B. New-OBRetentionPolicy
- C. Add-OBFileSpec
- D. Start-OBRegistration
- E. Set OBMachineSetting

**Correct Answer:** DE

**Section:** Configure File and Print Services

**Explanation**

**Explanation/Reference:**

The **Start-OBRegistration** cmdlet registers the server with Microsoft Azure Backup using the vault credentials downloaded during enrollment.

<https://technet.microsoft.com/en-us/library/hh770398.aspx>

The **Set-OBMachineSetting** cmdlet sets a OBMachineSetting object for the server that includes proxy server settings for accessing the internet, network bandwidth throttling settings, and the encryption passphrase that is required to decrypt the files during recovery to another server.

<https://technet.microsoft.com/en-us/library/hh770409.aspx>

#### QUESTION 82

You have 30 servers that run Windows Server 2012 R2. All of the servers are backed up daily by using Microsoft Azure Online Backup.

You need to perform an immediate backup of all the servers to Microsoft Azure Online Backup.

Which Windows PowerShell cmdlets should you run on each server?

- A. Start-OBRegistration | Start-OBBBackup
- B. Get-OBPolicy | Start-OBBBackup
- C. Get-WBBBackupTarget | Start-WBBBackup
- D. Get-WBPolicy | Start-WBBBackup

**Correct Answer:** B

**Section:** Configure File and Print Services

**Explanation**

**Explanation/Reference:**

The **Get-OBPolicy** cmdlet gets the current backup policy that is set for the server, including the details about scheduling backups, files included in the backup, and retention policy.

Once the changes have been made to the policy object, the updated policy should be set as the current one using the Set-OBPolicy cmdlet.

To use Microsoft Azure Backup cmdlets, the user must be a member of the Administrators group or Backup Operators group.

<https://technet.microsoft.com/en-us/library/hh770406>

The **Start-OBRegistration** cmdlet registers the server with Microsoft Azure Backup using the vault credentials downloaded during enrollment.

<https://technet.microsoft.com/en-us/library/hh770398.aspx>

### QUESTION 83

You have a server named FS1 that runs Windows Server 2012 R2.

You install the File and Storage Services server role on FS1. From Windows Explorer, you view the properties of a shared folder named Share1 and you discover that the Classification tab is missing. You need to ensure that you can assign classifications to Share1 from Windows Explorer manually.

What should you do?

- A. From Folder Options, clear Use Sharing Wizard (Recommend).
- B. Install the File Server Resource Manager role service
- C. From Folder Options, select Show hidden files, folders, and drives
- D. Install the Enhanced Storage feature

**Correct Answer:** B

## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

File Server Resource Manager is a set of features that allow you to manage and classify data that is stored on file servers. File Server Resource Manager includes the following features:

- **File Classification Infrastructure.** File Classification Infrastructure provides insight into your data by automating classification processes so that you can manage your data more effectively. You can classify files and apply policies based on this classification. Example policies include dynamic access control for restricting access to files, file encryption, and file expiration. Files can be classified automatically by using file classification rules or manually by modifying the properties of a selected file or folder.

<https://technet.microsoft.com/en-us/library/hh831701.aspx>

## QUESTION 84

Your network contains an Active Directory domain named contoso.com. All client computers run Windows Vista Service Pack 2 (SP2).

All client computers are in an organizational unit (OU) named OU1. All user accounts are in an OU named OU2. All users log on to their client computer by using standard user accounts. A Group Policy object (GPO) named GPO1 is linked to OU1. A GPO named GPO2 is linked to OU2.

You need to apply advanced audit policy settings to all of the client computers.

What should you do?

- A. In GPO1, configure a startup script that runs auditpol.exe.
- B. In GPO2, configure a logon script that runs auditpol.exe.
- C. In GPO1, configure the Advanced Audit Policy Configuration settings.
- D. In GPO2, configure the Advanced Audit Policy Configuration settings.

**Correct Answer: C**

## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

The basic security audit policy settings in **Security Settings\Local Policies\Audit Policy** and the advanced security audit policy settings in **Security Settings\Advanced Audit Policy Configuration\System Audit Policies** appear to overlap, but they are recorded and applied differently. When you apply basic audit policy settings to the local computer by using the Local Security Policy snap-in, you are editing the effective audit policy, so changes made to basic audit policy settings will appear exactly as configured in Auditpol.exe.

There are a number of additional differences between the security audit policy settings in these two locations.

There are nine basic audit policy settings under **Security Settings\Local Policies\Audit Policy** and 53 settings under **Advanced Audit Policy Configuration**. The settings available in **Security Settings\Advanced Audit Policy Configuration** address similar issues as the nine basic settings in **Local Policies\Audit Policy**, but they allow administrators to be more selective in the number and types of events to audit. For example, the basic audit policy provides a single setting for account logon, and the advanced audit policy provides four. Enabling the single basic account logon setting would be the equivalent of setting all four advanced account logon settings. In comparison, setting a single advanced audit policy setting does not generate audit events for activities that you are not interested in tracking.

In addition, if you enable success auditing for the basic **Audit account logon events** setting, only success events will be logged for all account logon-related behaviors. In comparison, depending on the needs of your organization, you can configure success auditing for one advanced account logon setting, failure auditing for a second advanced account logon setting, success and failure auditing for a third advanced account logon setting, or no auditing.

The nine basic settings under **Security Settings\Local Policies\Audit Policy** were introduced in Windows 2000. Therefore, they are available in all versions of Windows released since then. The advanced audit policy settings were introduced in Windows Vista and Windows Server 2008. The advanced settings can only be used on computers running at least Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008.

<https://technet.microsoft.com/en-us/library/dn319046.aspx>

#### QUESTION 85

You work as a Network Administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain named ABC.com. All servers in the ABC.com domain have Microsoft Windows Server 2012 R2 installed and all client computers have Windows 8 Pro installed.

BitLocker Drive Encryption (Bitlocker) is enabled on all client computers. ABC.com wants you to implement BitLocker Network Unlock.

Which of the following servers would you required to implement BitLocker Network Unlock?

- A. A Domain Controller.
- B. A DHCP server.
- C. A DNS Server.
- D. A Windows Deployment Server.
- E. An Application Server.
- F. A Web Server.
- G. A File and Print Server.
- H. A Windows Server Update Services server.

**Correct Answer: D**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

Network Unlock must meet mandatory hardware and software requirements before the feature can automatically unlock domain joined systems. These requirements include:

- Supported Windows operating systems: Any computer running the versions of Windows designated in the Applies To list at the beginning of this topic.
- Any supported operating system with UEFI DHCP drivers can be Network Unlock clients.
- A server running the **Windows Deployment Services (WDS) role** on any supported server operating system.
- BitLocker Network Unlock optional feature installed on any supported server operating system.
- A DHCP server, separate from the WDS server.
- Properly configured public/private key pairing.
- Network Unlock Group Policy settings configured.

<https://technet.microsoft.com/en-us/library/jj574173.aspx>

**QUESTION 86**

You work as a network administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain name ABC.com. All servers in the ABC.com domain have Microsoft Windows Server 2012 R2 installed. The computer accounts for all file servers are located in an organizational unit (OU) named DataOU.

You are required to track user access to shared folders on the file servers.

Which of the following actions should you consider?

- A. You should configure auditing of Account Logon events for the DataOU.
- B. You should configure auditing of Object Access events for the DataOU.
- C. You should configure auditing of Global Object Access Auditing events for the DataOU.
- D. You should configure auditing of Directory Service Access events for the DataOU.
- E. You should configure auditing of Privilege Use events for the DataOU.

**Correct Answer: B**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:****Audit object access**

This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified.

[https://technet.microsoft.com/en-us/library/Cc776774\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Cc776774(v=WS.10).aspx)

#### QUESTION 87

You are the administrator of an Active Directory Domain Services (AD DS) domain named ABC.com. The domain has a Microsoft Windows Server 2012 R2 server named ABC-SR05 that hosts the File and Storage Services server role.

ABC-SR05 hosts a shared folder named userData. You want to receive an email alert when a multimedia file is saved to the userData folder.

Which tool should you use?

- A. You should use File Management Tasks in File Server Resource Manager.
- B. You should use File Screen Management in File Server Resource Manager.
- C. You should use Quota Management in File Server Resource Manager.
- D. You should use File Management Tasks in File Server Resource Manager.
- E. You should use Storage Reports in File Server Resource Manager.

**Correct Answer: B**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

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. When you generate storage reports, you have the option of sending the reports to specific recipients by e-mail. If you want to routinely notify certain administrators about quota and file screening events, or send storage reports, you can configure one or more default recipients.

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

#### **To configure e-mail options**

1. In the console tree, right-click **File Server Resource Manager**, and then click **Configure Options**. The **File Server Resource Manager Options** dialog box opens.
2. 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 and storage reports.
3. If you want to routinely notify certain administrators about quota or file screening events or e-mail storage reports, under **Default administrator recipients**, type each e-mail address.  
Use the format *account@domain*. Use semicolons to separate multiple accounts.

4. To specify a different "From" address for e-mail notifications and storage reports sent from File Server Resource Manager, under **Default "From" e-mail address**, type the e-mail address that you want to appear in your message.
5. To test your settings, click **Send Test E-mail**.
6. Click **OK**.

<https://technet.microsoft.com/en-us/library/Cc754526.aspx>

#### QUESTION 88

our network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has a drive named E that is encrypted by using BitLocker Drive Encryption (BitLocker). A recovery key is stored on drive C. Drive E becomes locked.

When you attempt to use the recovery key, you receive the error message shown in the exhibit. (Click the Exhibit button.)

You need to access the data stored on drive E. What should you run first?

**Exhibit:**



- A. `manage-bde -protectors -get e:`
- B. `manage-bde -unlock e: -recoverykey c:\`
- C. `manage-bde -unlock e: -recoverykey c:\`
- D. `unlock-bitlocker -mountpoint e: -recoverykeypath c:`

**Correct Answer: A**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

`manage-bde -protectors` manages the protection methods used for the BitLocker encryption key.

The `-get` parameter displays all the key protection methods enabled on the drive and provides their type and identifier (ID).

<https://technet.microsoft.com/en-us/library/ff829848.aspx>

#### QUESTION 89

A system administrator is trying to determine which file system to use for a server that will become a Windows Server 2012 R2 file server and domain controller.

The company has the following requirements:

- The file system must allow for file-level security from within Windows 2012 Server.
- The file system must make efficient use of space on large partitions.
- The domain controller SYSVOL must be stored on the partition.

Which of the following file systems meets these requirements?

- A. FAT
- B. FAT32
- C. HPFS
- D. NTFS

**Correct Answer: D**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

#### NTFS Overview

The list below describes some of the practical applications in which NTFS should be used as the file system.

- **Increasing security.** NTFS allows you to set permissions on a file or folder, and specify the groups and users whose access you want to restrict or allow, and then select the type of access.
- **Supporting large volumes.** NTFS allows you to create an NTFS volume up to 16 terabytes using the default cluster size (4 KB) for large volumes. You can create NTFS volumes up to 256 terabytes using the maximum cluster size of 64 KB.

<https://technet.microsoft.com/en-us/library/Dn466522.aspx>

#### Active Directory Domain Services Overview

Requirements for running Active Directory Domain Services



**NTFS** – The drives that store the database, log files, and SYSVOL folder for Active Directory Domain Services (AD DS) must be placed on a local fixed volume. SYSVOL must be placed on a volume that is formatted with the NTFS file system. For security purposes, the Active Directory database and log files should be placed on a volume that is formatted with NTFS.

<https://technet.microsoft.com/en-us/library/Hh831484.aspx>

#### QUESTION 90

You work as a Network Administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain named ABC.com. All servers in the ABC.com domain have Microsoft Windows Server 2012 R2 installed.

ABC.com has a main office and a branch office. The two offices are connected by a slow WAN link.

A server in the main office named ABC-SR21 runs the File and Storage Services and Distributed File System roles. A server in the branch office named ABC-SR22 also runs the File and Storage Services and Distributed File System roles. Shared folders on ABC-SR21 and ABC-SR22 are replicated to each other using DFS Replication (DFSR).

You discover that DFS replication between the two servers is using too much bandwidth over the WAN link.

How can you limit the amount of bandwidth used by DFS replication?

- A. You should run the Set-DfsrConnectionSchedule cmdlet.
- B. You should run the Set-DfsrGroupSchedule cmdlet.
- C. You should run the Set-DfsReplicatedFolder cmdlet.
- D. You should run the Set-DfsReplicationGroup cmdlet.

**Correct Answer: B**

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

The **Set-DfsrGroupSchedule** cmdlet modifies a schedule for a replication group. DFS Replication schedules control the availability and bandwidth usage of replication.

[https://technet.microsoft.com/en-us/library/dn296568\(v=wps.630\).aspx](https://technet.microsoft.com/en-us/library/dn296568(v=wps.630).aspx)

#### QUESTION 91

Your network contains an Active Directory domain named contoso.com. You have a failover cluster named Cluster1. All of the nodes in Cluster1 have BitLocker Drive Encryption (BitLocker) installed.

You plan to add a new volume to the shared storage of Cluster1. You need to add the new volume to the shared storage. The solution must meet the following requirements:

- Encrypt the volume.
- Avoid using maintenance mode on the cluster.

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

**Select and Place:**

Actions

- Run the **Enable-BitLockerAutoUnlock** cmdlet.
- Run the **Enable-BitLocker** cmdlet.
- Run the **Lock-BitLocker** cmdlet.
- Add the volume to the cluster.
- Run the **Add-BitLockerProtector** cmdlet.

Answer Area

**Correct Answer:**

Actions

- Run the **Lock-BitLocker** cmdlet.
- Run the **Enable-BitLockerAutoUnlock** cmdlet.
- 

Answer Area

- Run the **Enable-BitLocker** cmdlet.
- Run the **Add-BitLockerProtector** cmdlet.
- Add the volume to the cluster.

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

When using BitLocker with volumes designated for a cluster, the volume will need to turn on BitLocker before its addition to the storage pool within cluster or put the resource into maintenance mode before BitLocker operations will complete.

When the cluster service owns a disk resource already, it needs to be set into maintenance mode before BitLocker can be enabled.

### **Turning on BitLocker before adding disks to a cluster using Windows PowerShell**

BitLocker encryption is available for disks before or after addition to a cluster storage pool. The advantage of encrypting volumes prior to adding them to a cluster is that the disk resource does not require suspending the resource to complete the operation. To turn on BitLocker for a disk before adding it to a cluster, do the following:

1. Install the BitLocker Drive Encryption feature if it is not already installed.
2. Ensure the disk is formatted NTFS and has a drive letter assigned to it.
3. Enable BitLocker on the volume using your choice of protector. A password protector is used in the Windows PowerShell script example below.

**Enable-BitLocker** E: -PasswordProtector -Password \$pw

4. Identify the name of the cluster with Windows PowerShell.

`Get-Cluster`

5. Add an ADAccountOrGroupProtector to the volume using the cluster name using a command such as:

**Add-BitLockerProtector** E: -ADAccountOrGroupProtector -ADAccountOrGroup CLUSTER\$

6. Repeat steps 1-6 for each disk in the cluster.

7. **Add the volume(s) to the cluster.**

<https://technet.microsoft.com/en-us/library/dn383585.aspx>

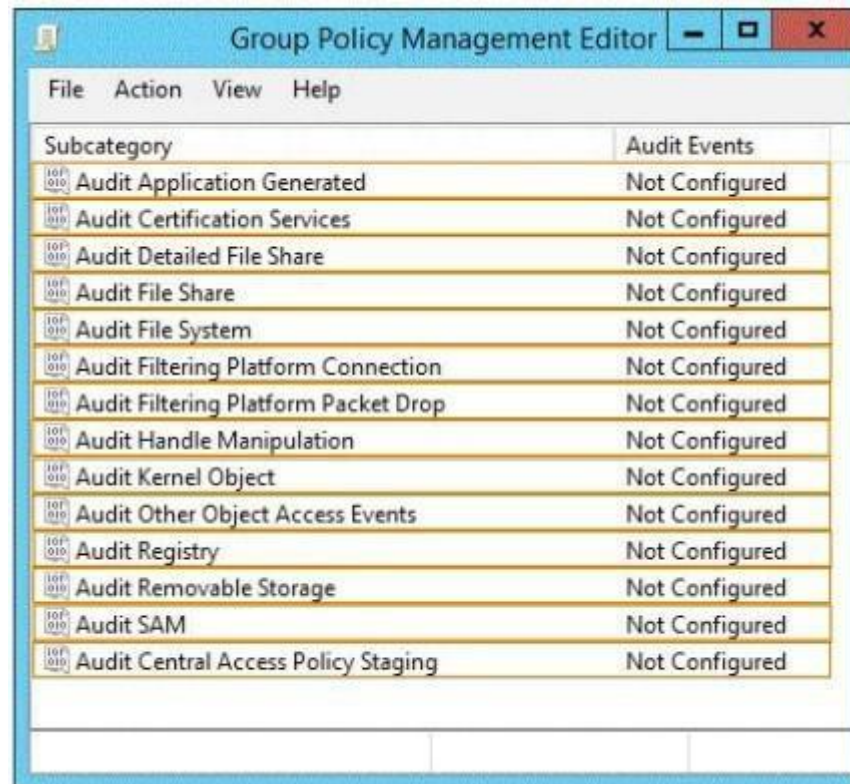
### **QUESTION 92**

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

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

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

**Hot Area:**



**Correct Answer:**



## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

#### To configure settings to monitor removable storage devices

1. Sign in to your domain controller by using domain administrator credentials.
2. In Server Manager, point to **Tools**, and then click **Group Policy Management**.
3. In the console tree, right-click the flexible access Group Policy Object on the domain controller, and then click **Edit**.
4. Double-click **Computer Configuration**, double-click **Security Settings**, double-click **Advanced Audit Policy Configuration**, double-click **Object Access**, and then double-click **Audit Removable Storage**.

5. Select the **Configure the following audit events** check box, select the **Success** check box (and the **Failure** check box, if desired), and then click **OK**.
6. If you selected the **Failure** check box, double-click **Audit Handle Manipulation**, select the **Configure the following audit events check box**, and then select **Failure**.
7. Click **OK**, and then close the Group Policy Management Editor.

<https://technet.microsoft.com/en-us/library/jj574128.aspx>

### QUESTION 93

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

You need to configure the DFS Replication environment to meet the following requirements:

- Increase the quota limit of the staging folder.
- Configure the staging folder cleanup process to provide the highest amount of free space possible.

Which cmdlets should you use to meet each requirement? To answer, select the appropriate options in the answer area.

#### Hot Area:

Answer Area	
Increase the quota limit of the staging folder.	<div>Set-DfsrGroupSchedule</div> <div>Set-DfsrMembership</div> <div>Set-DfsrReplicatedFolder</div> <div>Set-DfsrServiceConfiguration</div>
Configure the staging folder cleanup process to provide the highest amount of free space possible.	<div>Set-DfsrGroupSchedule</div> <div>Set-DfsrMembership</div> <div>Set-DfsrReplicatedFolder</div> <div>Set-DfsrServiceConfiguration</div>

**Correct Answer:**

Answer Area

Increase the quota limit of the staging folder.

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

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

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

## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

The **Set-DfsrServiceConfiguration** cmdlet modifies settings for the Distributed File System (DFS) Replication service on replication group members. Members of a replication group host replicated folders. Use this cmdlet to configure cleanup settings, debug logging settings, and automatic recovery for unexpected shut down.

DFS Replication stores files in a folder named ConflictsAndDeleted until it deletes them for space. DFS Replication can stage files in a staging folder. In both cases, you can set a maximum folder size, called a quota, by using the **Set-DfsrMembership** cmdlet. Use the current cmdlet to set the percent of the quota used to start and stop deletion of older files.

<https://technet.microsoft.com/en-us/library/dn296587.aspx>

### QUESTION 94

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

You need to configure Server1 to meet the following requirements:

- Ensure that old files in a folder named Folder1 are archived automatically to a folder named Archive1.
- Ensure that all storage reports are saved to a network share.

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



Hot Area:



Correct Answer:





## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

#### To create a custom task

1. Click the **File Management Tasks** node.
2. Right-click **File Management Tasks**, and then click **Create File Management Task** (or click **Create File Management Task** in the **Actions** pane). This opens the **Create File Management Task** dialog box.
3. On the **Action** tab, enter the following information:
  - **Type.** Select **Custom** from the drop-down menu.
  - **Executable.** Type or browse to a command to run when the file management task processes files. This executable must be set to be writable by Administrators and System only. If any other users have write access to the executable, it will not run correctly.
  - **Command settings.** To configure the arguments passed to the executable when a file management job processes files, edit the text box labeled **Arguments**. To insert additional variables in the text, place the cursor in the location in the text box where you want to insert the variable, select the

variable that you want to insert, and then click **Insert Variable**. The text that is in brackets inserts variable information that the executable can receive. For example, the [Source File Path] variable inserts the name of the file that should be processed by the executable. Optionally, click the **Working directory** button to specify the location of the custom executable.

- **Command Security.** Configure the security settings for this executable. By default, the command is run as Local Service, which is the most restrictive account available.

4. Click **OK**.

<https://technet.microsoft.com/en-us/library/dd759180.aspx>

You can specify the disk location where storage reports will be saved. A default path has been defined, but it can be changed. There are three types of reports:

Report type	Description
Incident reports	Generated automatically when a quota or file screening event occurs.
Scheduled reports	Generated when there is a report task defined in the <b>Storage Reports Management</b> node.
On-demand reports	Generated manually from the <b>Storage Reports Management</b> node when you click <b>Generate Reports Now</b> .

### To change the report locations

1. In the console tree, right-click **File Server Resource Manager**, and then click **Configure Options**. The **File Server Resource Manager Options** dialog box opens.
2. On the **Report Locations** tab, type the path or browse to the location where you want each of the report types to be saved.
3. Click **OK**.

<https://technet.microsoft.com/en-us/library/cc771521.aspx>

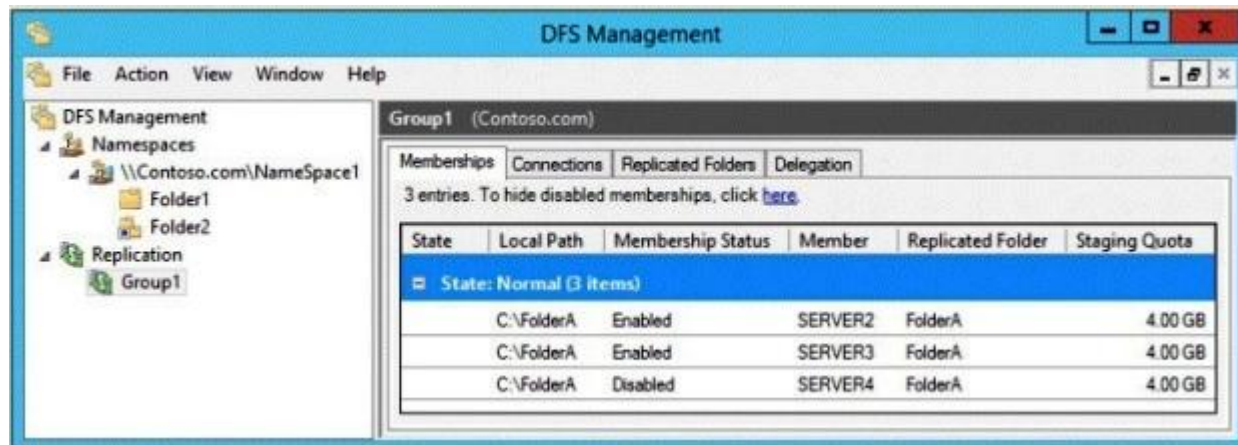
### QUESTION 95

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

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

Complete each statement according to the information presented in the exhibit. Each correct selection is worth one point.

**Exhibit:**



**Hot Area:**

Answer Area

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

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

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

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

**Correct Answer:**

Answer Area

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

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

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

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

## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

#### DFS Namespaces and DFS Replication Overview

DFS Namespaces and DFS Replication are role services in the File and Storage Services role.

- **DFS Namespaces** Enables you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. However, the underlying structure of the namespace can consist of numerous file shares that are located on different servers and in multiple sites.
- **DFS Replication** Enables you to efficiently replicate folders (including those referred to by a DFS namespace path) across multiple servers and sites.

<https://technet.microsoft.com/en-us/library/jj127250.aspx>

#### QUESTION 96

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

You create an organizational unit (OU) named OU1 and a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You move several file servers that store sensitive company documents to OU1. Each file server contains more than 40 shared folders. You need to audit all of the failed attempts to access the files on the file servers in OU1. The solution must minimize administrative effort.

Which two audit policies should you configure in GPO1? To answer, select the appropriate two objects in the answer area.

**Hot Area:**



**Correct Answer:**



## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

#### Audit object access

This policy setting enables auditing of the event generated by a user who accesses an object—for example, a file, folder, registry key, or printer—that has a SACL that specifies a requirement for auditing.

[https://technet.microsoft.com/en-us/library/cc766468\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766468(v=ws.10).aspx)

The Advanced Security Audit policy setting, **File System (Global Object Access Auditing)**, which enables you to configure a global system access control list (SACL) on the file system for an entire computer.

If you select the **Configure security** check box on the policy's property page, you can add a user or group to the global SACL. This enables you to define computer system access control lists (SACLs) per object type for the file system. The specified SACL is then automatically applied to every file system object type.

If both a file or folder SACL and a global SACL are configured on a computer, the effective SACL is derived by combining the file or folder SACL and the global SACL. This means that an audit event is generated if an activity matches either the file or folder SACL or the global SACL.

This policy setting must be used in combination with the **File System** security policy setting under Object Access. For more information, see Audit File

System.

<https://technet.microsoft.com/en-us/library/dn319112.aspx>

#### QUESTION 97

Your network contains 25 Web servers that run Windows Server 2012 R2.

You need to configure auditing policies that meet the following requirements:

- Generate an event each time a new process is created.
- Generate an event each time a user attempts to access a file share.

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

**Hot Area:**



**Correct Answer:**





## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

Auditing subcategories:

#### **Detailed Tracking**—Process Creation

Reports the creation of a process and the name of the program or user that created it.

#### **Object Access**—File Share

Reports when a file share is accessed.

[https://technet.microsoft.com/en-us/library/cc766468\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766468(v=ws.10).aspx)

### QUESTION 98

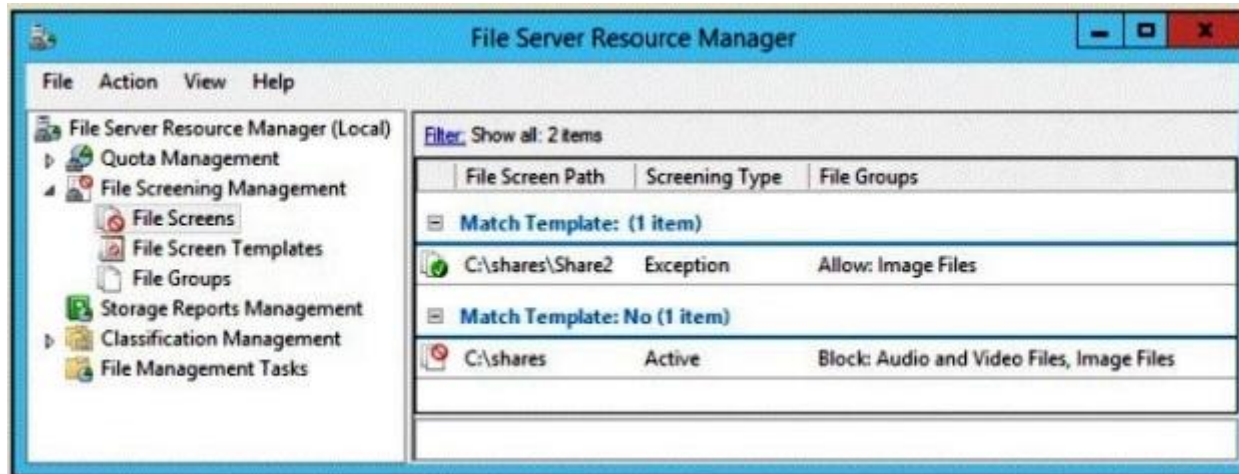
You have a file server named Server1 that runs Windows Server 2012 R2. A user named User1 is assigned the modify NTFS permission to a folder named C:\shares and all of the subfolders of C:\shares.

On Server1, you open File Server Resource Manager as shown in the exhibit. (Click the Exhibit button.)

Complete each statement according to the information presented in the exhibit. Each correct selection is worth one point.



**Exhibit:**



**Hot Area:**

Answer Area

User1 can copy a file named ... to C:\shares.

User1 cannot copy a file named ... to a folder named C:\shares\share2.

File1.gif
File2.bmp
File3.jpg.zip
File4.mp3

File1.gif
File2.bmp
File3.jpg.zip
File4.mp3

**Correct Answer:**

**Answer Area**

User1 can copy a file named ... to C:\shares.

User1 cannot copy a file named ... to a folder named C:\shares\share2.

File1.gif
File2.bmp
File3.jpg.zip
File4.mp3

File1.gif
File2.bmp
File3.jpg.zip
File4.mp3

## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

File Server Resource Manager Overview

<https://technet.microsoft.com/en-us/library/hh831701.aspx>

Logical analysis:

C:\shares has access blocked for all Audio, Video, and Image files. File3.jpg.zip is an Archive file which contains an image file, but the file type of the archive is not an image file. Therefore, the file can be copied to C:\shares.

C:\shares\Share2 has all the same restrictions as the parent folder, with the "exception" that Image files are allowed. As before, File3.jpg.zip can still be copied to this folder. Also, because of the exception, the two image files can be copied to this sub-folder. However, File4.mp3, an audio file, is still blocked and cannot be copied.

### QUESTION 99

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

You need to audit access to removable storage devices.

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

#### Hot Area:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Correct Answer:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

#### Section: Configure File and Print Services

##### Explanation

##### Explanation/Reference:

##### Audit object access

This policy setting enables auditing of the event generated by a user who accesses an object—for example, a file, folder, registry key, or printer—that has a SACL that specifies a requirement for auditing.

[https://technet.microsoft.com/en-us/library/cc766468\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766468(v=ws.10).aspx)

#### QUESTION 100

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 the members of a group named Group1. User1 has the Department value set to Accounting, user2 has the Department value set to Marketing. Both users have the Employee Type value set to Contract Employee.

You create the auditing entry as shown in the exhibit. (Click the Exhibit button.)

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

**Exhibit:**

**Auditing Entry for Global File SACL**

Principal: **Authenticated Users** Select a principal

Type: **All**

**Permissions:**

<input type="checkbox"/> Full control	<input checked="" type="checkbox"/> Delete subfolders and files
<input type="checkbox"/> Traverse folder / execute file	<input checked="" type="checkbox"/> Delete
<input checked="" type="checkbox"/> List folder / read data	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Read attributes	<input checked="" type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Take ownership
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Read
<input type="checkbox"/> Create folders / append data	<input type="checkbox"/> Write
<input type="checkbox"/> Write attributes	<input type="checkbox"/> Execute
<input type="checkbox"/> Write extended attributes	

**Clear all**

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

**Manage grouping**

User	Department	Not equals	Value	Accounting	Remove
And					
User	Employee Type	Equals	Value	Contract Employee	Remove

Add a condition

**OK** **Cancel**

**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 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 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: Configure File and Print Services**  
**Explanation**

**Explanation/Reference:**

Advanced Security Audit Policy Step-by-Step Guide

[https://technet.microsoft.com/en-us/library/dd408940\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd408940(v=ws.10).aspx)

Logical analysis:

The current Department condition is "Not equals" for the value of "Accounting." Since User1 is a member of the Accounting group, audit events will not be logged. To log events for User1, the Department condition must be modified.

The current Permissions identified include folder access, permission changes, and file deletion, but not opening files. To log events when User2 opens files, permissions settings must be modified to include "Read" or "Write" attributes.

### QUESTION 101

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

Server1 has the following BitLocker Drive Encryption (BitLocker) settings:

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

You need to ensure that drive D will unlock automatically when Server1 restarts.

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

**Hot Area:**

Answer Area

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Add-BitLockerKeyProtector	-MountPoint C:	-AdAccountOrGroupProtector Contoso\Server	-Service
Enable-BitLockerAutoUnlock	-MountPoint D:	-Pin \$SecureString	TpmAndPinAndStartupKeyProtecto
			-TpmAndPinProtector



Correct Answer:

Answer Area			
Add-BitLockerKeyProtector	-MountPoint C:	-AdAccountOrGroupProtector Contoso\Server	-Service
Enable-BitLockerAutoUnlock	-MountPoint D:	-Pin \$SecureString	TpmAndPinAndStartupKeyProtecto
			-TpmAndPinProtector

## Section: Configure File and Print Services

### Explanation

#### Explanation/Reference:

#### Using BitLocker with Clustered Volumes

BitLocker on volumes within a cluster are managed based on how the cluster service "views" the volume to be protected. The volume can be a physical disk resource such as a logical unit number (LUN) on a storage area network (SAN) or network attached storage (NAS).

Alternatively, the volume can be a cluster-shared volume, a shared namespace, within the cluster. Windows Server 2012 has expanded the CSV architecture, now known as CSV2.0, to enable support for BitLocker. When using BitLocker with volumes designated for a cluster, the volume will need to turn on BitLocker before its addition to the storage pool within cluster or put the resource into maintenance mode before BitLocker operations will complete.

Windows PowerShell or the manage-bde command line interface is the preferred method to manage BitLocker on CSV2.0 volumes. This is recommended over the BitLocker Control Panel item because CSV2.0 volumes are mount points. Mount points are an NTFS object that is used to provide an entry point to other volumes. Mount points do not require the use of a drive letter. Volumes that lack drive letters do not appear in the BitLocker Control Panel item. Additionally, the new Active Directory-based protector option required for cluster disk resource or CSV2.0 resources is not available in the Control Panel item.

<https://technet.microsoft.com/en-us/library/dn383585.aspx>

The **Add-BitLockerKeyProtector** cmdlet adds a protector for the volume key of the volume protected with BitLocker Drive Encryption.

#### **-MountPoint<String[]>**

Specifies an array of drive letters or BitLocker volume objects. This cmdlet adds a key protector to the volumes specified. To obtain a BitLocker volume object, use the Get-BitLockerVolume cmdlet.

#### **-ADAccountOrGroupProtector**

Indicates that BitLocker uses an AD DS account as a protector for the volume encryption key.

#### **-Service**



Indicates that the system account for this computer unlocks the encrypted volume.

<https://technet.microsoft.com/en-us/library/jj649835.aspx>

### QUESTION 102

Your network contains an Active Directory domain named corp.contoso.com. The domain contains two member servers named Server1 and Edge1. Both servers run Windows Server 2012 R2.

Your company wants to implement a central location where the system events from all of the servers in the domain will be collected. From Server1, a network technician creates a collector-initiated subscription for Edge1. You discover that Server1 does not contain any events from Edge1. You view the runtime status of the subscription as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that the system events from Edge1 are collected on Server1.

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

#### Exhibit:



#### Hot Area:

**Subscription Properties - Interesting Event Collection**

Subscription name:

Description:

Destination log:

Subscription type and source computers

☒ Collector initiated

This computer contacts the selected source computers and provides the subscription.

☐ Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

User account (the selected account must have read access to the source logs):

CORP\Administrator

Change user account or configure advanced settings:

**Correct Answer:**

Subscription Properties - Interesting Event Collection

Subscription name:

Description:

Destination log:

Subscription type and source computers

☒ Collector initiated

This computer contacts the selected source computers and provides the subscription.

☐ Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

User account (the selected account must have read access to the source logs):

Change user account or configure advanced settings:

## Section: Configure File and Print Services

### Explanation

### Explanation/Reference:

### Configure Advanced Subscription Settings

You can configure how collected events are delivered and specify the account used to manage the process of collecting events. Event Viewer provides three event delivery optimization options: **Normal** , **Minimize Bandwidth** and **Minimize Latency** . The following table lists each option along with a description of when it is an appropriate choice.

Event Delivery Optimization Options	Description
Normal	This option ensures reliable delivery of events and does not attempt to conserve bandwidth. It is the appropriate choice unless you need tighter control over bandwidth usage or need forwarded events delivered as quickly as possible. It uses pull delivery mode, batches 5 items at a time and sets a batch timeout of 15 minutes.
Minimize Bandwidth	This option ensures that the use of network bandwidth for event delivery is strictly controlled. It is an appropriate choice if you want to limit the frequency of network connections made to deliver events. It uses push delivery mode and sets a batch timeout of 6 hours. In addition, it uses a heartbeat interval of 6 hours.
Minimize Latency	This option ensures that events are delivered with minimal delay. It is an appropriate choice if you are collecting alerts or critical events. It uses push delivery mode and sets a batch timeout of 30 seconds.

The **Custom** event delivery option is never used when managing subscriptions created by using the Event Viewer snap-in. The Event Viewer can only create subscriptions with event delivery settings that correspond to the **Normal** , **Minimize Bandwidth** or **Minimize Latency** options. However, you can use Event Viewer to manage a subscription that was created or updated by using a different method, like the wecutil command-line tool. In that case, the **Custom** option is selected to indicate that the set of delivery settings of the subscription do not correspond to any of those supported by Event Viewer.

### To configure advanced subscription settings

1. Perform steps 1—6 of the Create a New Subscription procedure.
2. Click **Advanced** .
3. On the **Advanced Subscription Settings** dialog box, you can either specify an event delivery optimization or specify the account used to manage the process of collecting events.
  - To specify an event delivery optimization: Select the **Event Delivery Optimization** option you want and click **OK** .
  - To specify the account used to manage the process of collecting events, select the **Specific User** option, then click **User and Password** and enter the user name and password of the account and click **OK** . Click **OK** on the **Advanced Subscription Settings** dialog box.

<https://technet.microsoft.com/en-us/library/cc749167.aspx>

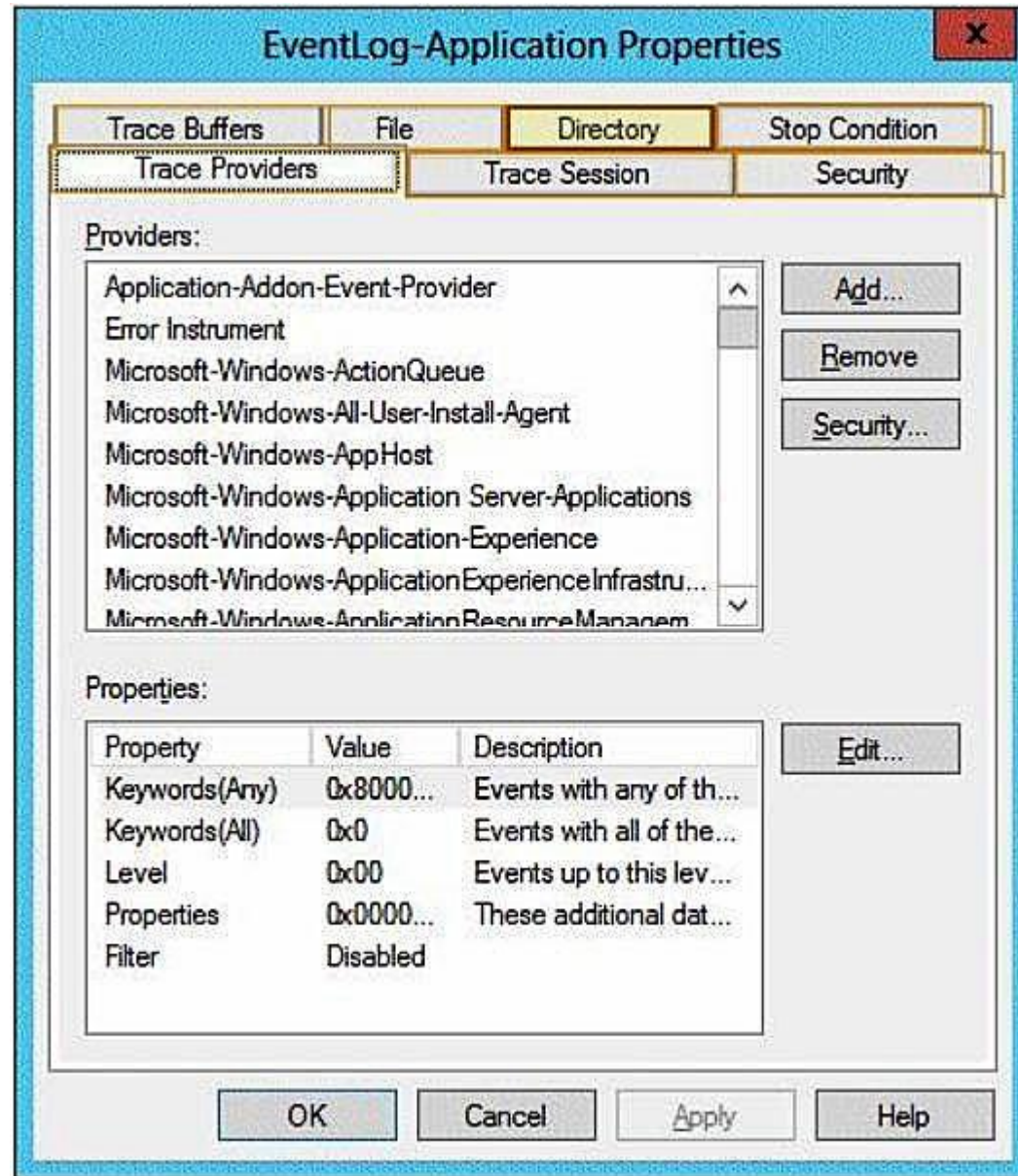
**QUESTION 103**

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

You enable the EventLog-Application event trace session. You need to set the maximum size of the log file used by the trace session to 10 MB.

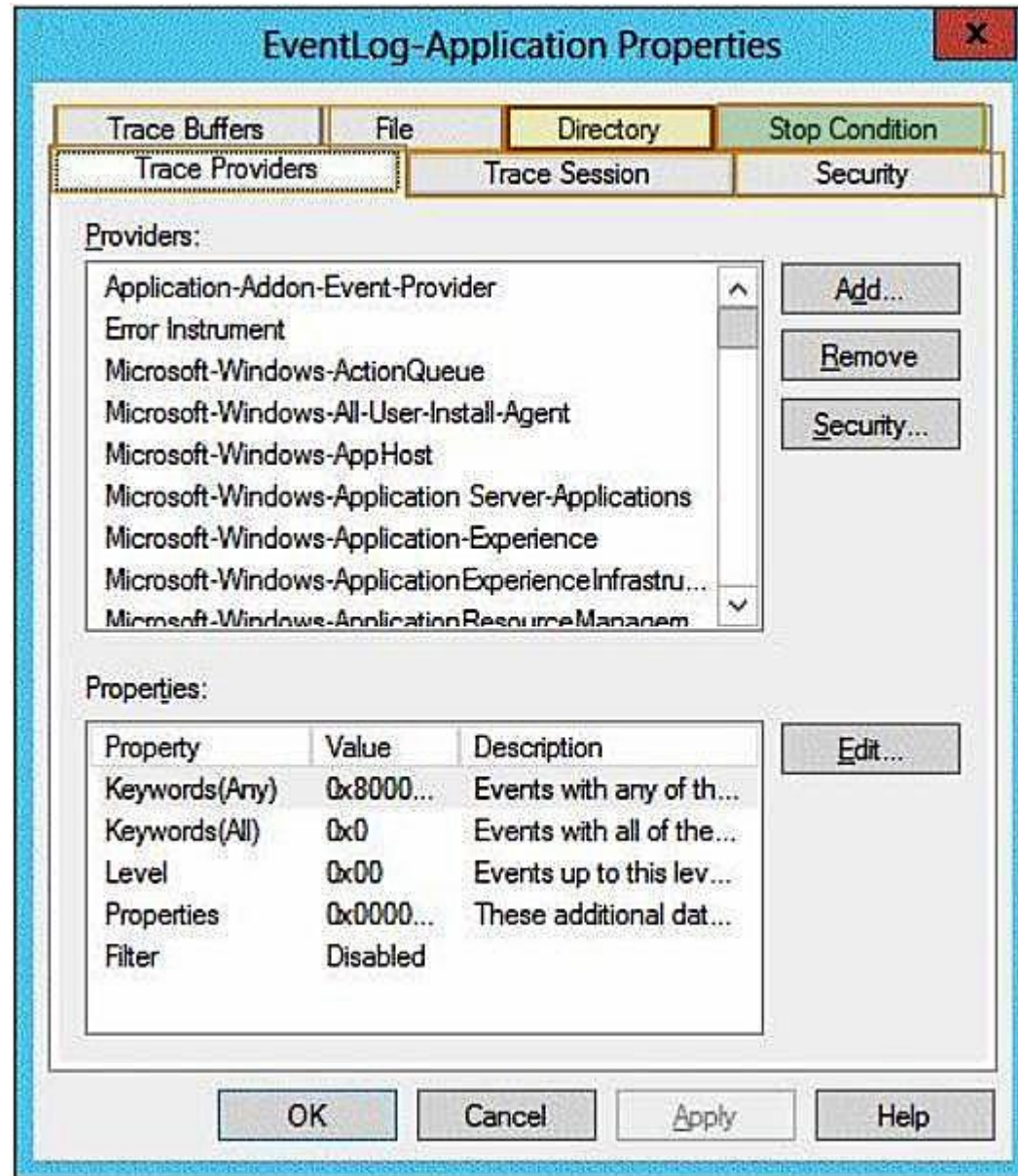
From which tab should you perform the configuration? To answer, select the appropriate tab in the answer area.

**Hot Area:**



Correct Answer:





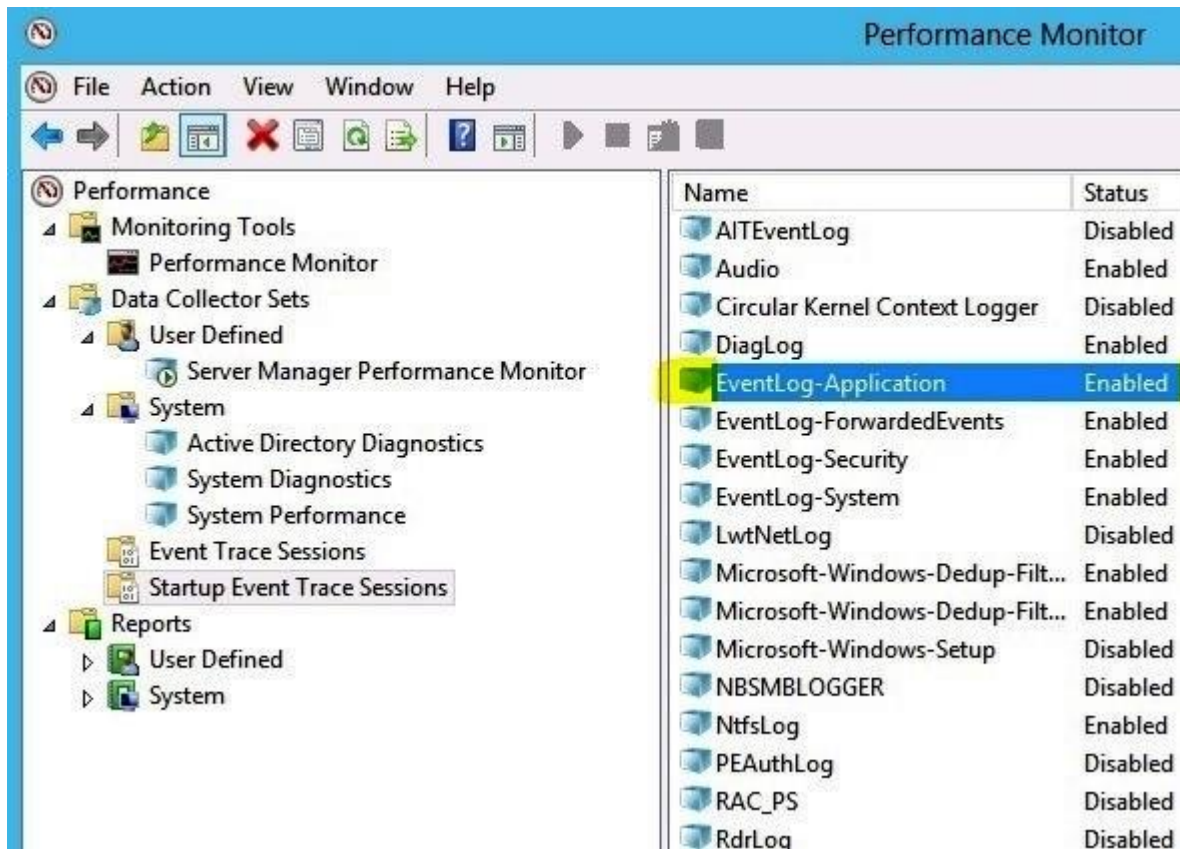
### Section: Configure File and Print Services

## Explanation

### Explanation/Reference:

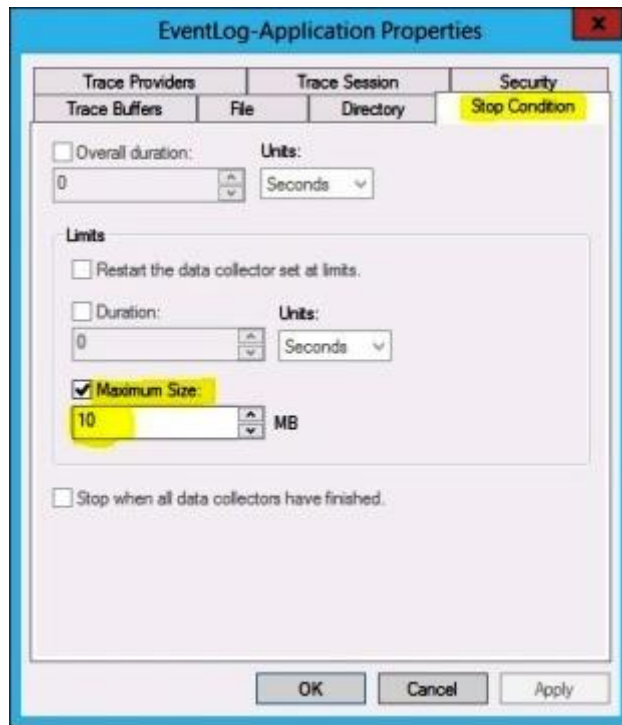
#### To schedule the Stop condition for a Data Collector Set

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



2. In the console pane, right-click the name of the Data Collector Set that you want to schedule and click **Properties**.
3. Click the **Stop Condition** tab.





4. To stop collecting data after a period of time, select the **Overall duration** check box and choose the quantity and units. Note that your overall duration must be longer than the interval at which data is sampled in order to see any data in the report. Do not select an overall duration if you want to collect data indefinitely.
5. Use limits to segment data collection into separate logs by selecting the **When a limit is reached, restart the data collector set** check box. If both limit types are selected, data collection will stop or restart when the first limit is reached.
  - Select **Duration** to configure a time period for data collection to write to a single log file.
  - Select **Maximum Size** to restart the Data Collector Set or to stop collecting data when the log file reaches the limit.
6. If you have configured an overall duration, you can click the **Stop when all data collectors have finished** check box to allow all data collectors to finish recording the most recent values before the Data Collector Set is stopped.
7. When finished, click **OK**.

[https://technet.microsoft.com/en-us/library/dd744567\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd744567(v=ws.10).aspx)

**QUESTION 104**

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

You need to create a certificate template for the BitLocker Drive Encryption (BitLocker) Network Unlock feature.

Which Cryptography setting of the certificate template should you modify? To answer, select the appropriate setting in the answer area.

**Hot Area:**

**Properties of New Template**

Superseded Templates		Extensions	Security
Subject Name		Server	Issuance Requirements
Compatibility	General	Request Handling	Cryptography

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 1024

Choose which cryptographic providers can be used for requests

☐ Requests can use any provider available on the subject's computer

☒ Requests must use one of the following providers:

Providers:

- ☒ Microsoft Enhanced Cryptographic Provider v1.0
- ☐ Microsoft Base Cryptographic Provider v1.0
- ☐ Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
- ☐ Microsoft DH SChannel Cryptographic Provider
- ☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider

Request hash: Determined by CSP

☐ Use alternate signature format

OK Cancel Apply Help

**Correct Answer:**

**Properties of New Template**

Superseded Templates		Extensions	Security
Subject Name		Server	Issuance Requirements
Compatibility	General	Request Handling	Cryptography

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 1024

Choose which cryptographic providers can be used for requests

☐ Requests can use any provider available on the subject's computer

☒ Requests must use one of the following providers:

Providers:

- ☒ Microsoft Enhanced Cryptographic Provider v1.0
- ☐ Microsoft Base Cryptographic Provider v1.0
- ☐ Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
- ☐ Microsoft DH SChannel Cryptographic Provider
- ☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider

Request hash: Determined by CSP

☐ Use alternate signature format

OK Cancel Apply Help

**Section: Configure File and Print Services**

**Explanation**

**Explanation/Reference:**

The network key is stored on the system drive along with an AES 256 session key, and encrypted with the **2048-bit** RSA public key of the unlock server's certificate. The network key is decrypted with the help of a provider on a supported version of Windows Server running WDS, and returned encrypted with its corresponding session key.

The server side configuration to enable Network Unlock also requires provisioning a **2048-bit** RSA public/private key pair in the form of an X.509 certificate, and for the public key certificate to be distributed to the clients. This certificate must be managed and deployed through the Group Policy editor directly on a domain controller with at least a Domain Functional Level of Windows Server 2012. This certificate is the public key that encrypts the intermediate network key (which is one of the two secrets required to unlock the drive; the other secret is stored in the TPM).

### Create the certificate template for Network Unlock

The following steps detail how to create a certificate template for use with BitLocker Network Unlock. A properly configured Active Directory Services Certification Authority can use this certificate to create and issue Network Unlock certificates.

1. Open the Certificates Template snap-in (certtmpl.msc).
2. Locate the User template. Right-click the template name and select **Duplicate Template**
3. On the **Compatibility** tab, change the **Certification Authority** and **Certificate recipient** fields to Windows Server 2012 and Windows 8 respectively. Ensure the **Show resulting changes** dialog box is selected.
4. Select the **General** tab of the template. The **Template display name** and **Template name** should clearly identify that the template will be used for Network Unlock. Clear the checkbox for the **Publish certificate in Active Directory** option.
5. Select the **Request Handling** tab. Select **Encryption** from the **Purpose** drop down menu. Ensure the **Allow private key to be exported** option is selected.
6. Select the **Cryptography** tab. Set the **Minimum key size** to **2048**. (Any Microsoft cryptographic provider that supports RSA can be used for this template, but for simplicity and forward compatibility we recommend using the **Microsoft Software Key Storage Provider**.)
7. Select the **Requests must use one of the following providers** option and clear all options except for the cryptography provider you selected, such as the **Microsoft Software Key Storage Provider**.
8. Select the **Subject Name** tab. Select **Supply in the request**. Select **OK** if the certificate templates pop-up dialog appears.
9. Select the **Issuance Requirements** tab. Select both **CA certificate manager approval** and **Valid existing certificate** options.
10. Select the **Extensions** tab. Select **Application Policies** and choose **Edit....**
11. In the **Edit Application Policies Extension** options dialog box, select **Client Authentication**, **Encrypting File System**, and **Secure Email** and choose **Remove**.
12. On the **Edit Application Policies Extension** dialog box, select **Add**.

13. On the **Add Application Policy** dialog box, select **New**. In the **New Application Policy** dialog box enter the following information in the space provided and then click **OK** to create the BitLocker Network Unlock application policy:

- **Name:**BitLocker Network Unlock
- **Object Identifier:**1.3.6.1.4.1.311.67.1.1

14. Select the newly created **BitLocker Network Unlock** application policy and select **OK**

15. With the **Extensions** tab still open, select the **Edit Key Usage Extension** dialog, select the **Allow key exchange only with key encryption (key encipherment)** option. Select the **Make this extension critical** option.

16. Select the **Security** tab. Confirm that the **Domain Admins** group has been granted **Enroll** permission

17. Select **OK** to complete configuration of the template.

<https://technet.microsoft.com/en-us/library/jj574173.aspx>

#### **QUESTION 105**

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The domain contains an organizational unit (OU) named FileServers\_OU. FileServers\_OU contains the computer accounts for all of the file servers in the domain.

You need to audit the users who successfully access shares on the file servers.

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

**Hot Area:**

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Correct Answer:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

#### Section: Configure File and Print Services

##### Explanation

##### Explanation/Reference:

##### Audit object access

This policy setting enables auditing of the event generated by a user who accesses an object—for example, a file, folder, registry key, or printer—that has a SACL that specifies a requirement for auditing.

[https://technet.microsoft.com/en-us/library/cc766468\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766468(v=ws.10).aspx)

#### QUESTION 106

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.

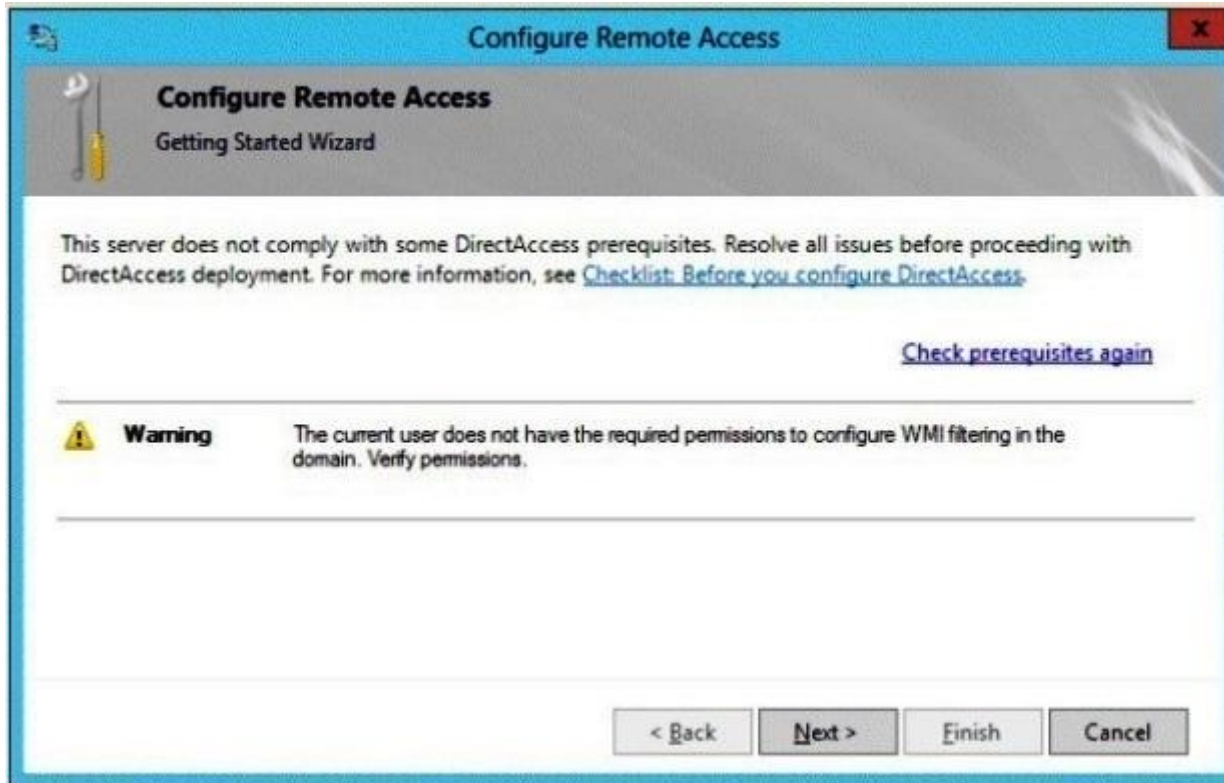
You log on to Server1 by using a user account named User2. From the Remote Access Management Console, you run the Getting Started Wizard and you receive a warning message as shown in the exhibit. (Click the Exhibit button.)

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?

**Exhibit:**



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

**Correct Answer:** B

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

The person deploying remote access on the server requires local administrator permissions on the server, and domain user permissions.

<https://technet.microsoft.com/en-us/library/hh831436.aspx>

#### **QUESTION 107**

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: Configure network services and access**

**Explanation**

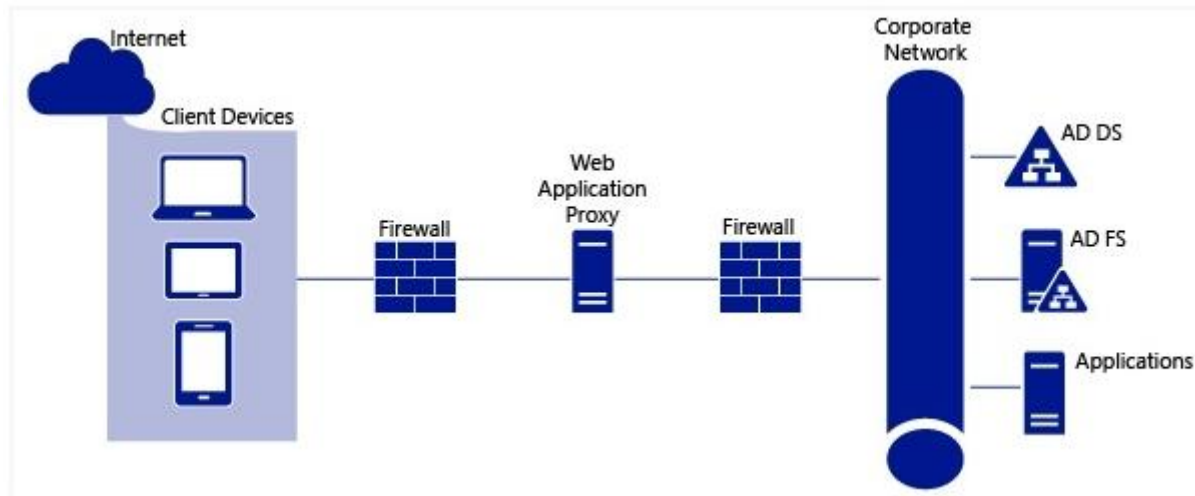
**Explanation/Reference:**

#### **Planning to Publish Applications Using Web Application Proxy**

This section describes planning steps that can be taken when you use Web Application Proxy – a Remote Access role service - to provide reverse proxy functionality for corporate web applications and services. When you use Web Application Proxy with Active Directory Federation Services (AD FS), you can manage the risk of exposing your applications to the Internet by configuring features provided by AD FS, including: Workplace Join, multifactor authentication (MFA), and multifactor access control.

Web Application Proxy also functions as an AD FS proxy.

The following diagram shows the topology used in this scenario for Web Application Proxy to publish Microsoft applications and other line-of-business (LOB) applications.



<https://technet.microsoft.com/en-us/library/dn383650.aspx>

#### QUESTION 108

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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

Network address translation (NAT) allows you to share a connection to the public Internet through a single interface with a single public IP address. The computers on the private network use private, non-routable addresses. NAT maps the private addresses to the public address.

### To enable network address translation addressing

1. In the RRAS MMC snap-in, expand *Your Server Name*. If you are using Server Manager, expand **Routing and Remote Access**.
2. Expand **IPv4**, right-click **NAT**, and then click **Properties**.
3. If you do not have a DHCP server on the private network, then you can use the RRAS server to respond to DHCP address requests. To do this, on the **Address Assignment** tab, select the **Automatically assign IP addresses by using the DHCP allocator** check box.
4. To allocate addresses to clients on the private network by acting as a DHCP server, in **IP address and Mask**, configure a subnet address from which the addresses are assigned. For example, if you enter 192.168.0.0 and a subnet mask of 255.255.255.0, then the RRAS server responds to DHCP requests with address assignments from 192.168.0.1 through 192.168.0.254.
5. (Optional) To exclude addresses in the configured network range from being assigned to DHCP clients on the private network, click **Exclude**, click **Add**, and then configure the addresses.
6. To add the public interface to the NAT configuration, right-click **NAT**, and then click **New Interface**. Select the interface connected to the public network, and then click **OK**.
7. On the **NAT** tab, click **Public interface connected to the Internet** and **Enable NAT on this interface**, and then click **OK**.
8. If you want to add additional public addresses assigned to this interface or configure service and port mappings to computers on the private network, see "IPv4 - NAT - Interface - Properties Page" (<https://technet.microsoft.com/en-us/library/dd469796.aspx>).
9. To add the private interface to the NAT configuration, right-click **NAT**, and then click **New Interface**. Select the interface connected to the private network, and then click **OK**.
10. On the **NAT** tab, click **Private interface connected to private network**, and then click **OK**.

<https://technet.microsoft.com/en-us/library/dd469812.aspx>

### QUESTION 109

You have a DNS server named Server1 that has a Server Core Installation on Windows Server 2012 R2.

You need to view the time-to-live (TTL) value of a name server (NS) record that is cached by the DNS Server service on Server1.

What should you run?

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

D. dnscacheugc.exe

**Correct Answer:** A

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

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

<https://technet.microsoft.com/en-us/library/jj649915.aspx>

#### **QUESTION 110**

You have a DNS server named DNS1 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:** Configure network services and access

**Explanation**

**Explanation/Reference:**

A *stub zone* is a copy of a zone that contains only the original zone's start of authority (SOA) resource record, the name server (NS) resource records listing the authoritative servers for the zone, and the glue address (A) resource records that are needed to identify these authoritative servers.

A DNS server that is hosting a stub zone is configured with the IP address of the authoritative server from which it loads. DNS servers can use stub zones for both iterative and recursive queries. When a DNS server hosting a stub zone receives a recursive query for a computer name in the zone to which the stub zone refers, the DNS server uses the IP address to query the authoritative server, or, if the query is iterative, returns a referral to the DNS servers listed in the stub zone.

**Stub zones are updated at regular intervals, determined by the refresh interval of the SOA resource record for the stub zone.** When a DNS

server loads a stub zone, it queries the zone's primary servers for SOA resource records, NS resource records at the zone's root, and glue address (A) resource records. The DNS server attempts to update its resource records at the end of the SOA resource record's refresh interval. To update its records, the DNS server queries the primary servers for the resource records listed earlier.

You can use stub zones to ensure that the DNS server that is authoritative for a parent zone automatically receives updates about the DNS servers that are authoritative for a child zone. To do this, add the stub zone to the server that is hosting the parent zone. Stub zones can be either file-based or Active Directory-integrated. If you use Active Directory-integrated stub zones, you can configure them on one computer and let Active Directory replication propagate them to other DNS servers running on domain controllers.

The screenshot shows the 'adatum.com Properties' dialog box with the 'Zone Transfers' tab selected. The 'Start of Authority (SOA)' section contains the following fields:

- Serial number: 1 (with an 'Increment' button)
- Primary server: server1.contoso.com (with a 'Browse...' button)
- Responsible person: hostmaster.contoso.com (with a 'Browse...' button)
- Refresh interval: 15 minutes (highlighted with a red rectangle)
- Retry interval: 10 minutes
- Expires after: 1 days
- Minimum (default) TTL: 1 hours

At the bottom, the 'TTL for this record' is set to 0:1:0:0 (DDDD:HH:MM:SS). Buttons for 'OK', 'Cancel', 'Apply', and 'Help' are at the bottom right.

[https://technet.microsoft.com/en-us/library/cc786068\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc786068(v=ws.10).aspx)

#### QUESTION 111

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:** Configure network services and access

**Explanation**

**Explanation/Reference:**

For a client computer to be provisioned to use DirectAccess, **it must belong to the selected security group**. After DirectAccess is configured, client computers in the security group are provisioned to receive the DirectAccess Group Policy Object (GPO).

In a Remote Access deployment, configuring application servers is an optional task. Remote Access enables you to require authentication for selected application servers, which is determined by their inclusion in an application servers security group. By default, traffic to application servers that require authentication is also encrypted; however, you can choose to not encrypt traffic to application servers and use authentication only.

**To configure application servers**

1. In the middle pane of the Remote Access Management console, in the **Step 4 Application Servers** area, click **Configure**.
2. In the DirectAccess Application Server Setup Wizard, to require authentication to selected application servers, click **Extend authentication to selected application servers**. Click **Add** to select the application server security group.
3. To limit access to only the servers in the application server security group, select the **Allow access only to servers included in the security groups** check box.
4. To use authentication without encryption, select the **Do not encrypt traffic. Use authentication only** check box.

5. Click **Finish**.

When the Remote Access configuration is complete, the **Remote Access Review** is displayed. You can review all of the settings that you previously selected, including:

- **GPO Settings:** The DirectAccess server GPO name and client GPO name are listed. Additionally, you can click the **Change** link next to the **GPO Settings** heading to modify the GPO settings.
- **Remote Clients:** The DirectAccess client configuration is displayed, including the *security group*, force tunneling status, connectivity verifiers, and DirectAccess connection name.
- **Remote Access Server:** The DirectAccess configuration is displayed including the public name/address, network adapter configuration, certificate information, and OTP information if configured.
- **Infrastructure Servers:** This list includes the network location server URL, DNS suffixes that are used by DirectAccess clients, and management server information.
- **Application Servers:** The DirectAccess remote management status is displayed, in addition to the *status of the end-to-end authentication to specific application servers*.

<https://technet.microsoft.com/en-us/library/jj134239.aspx>

### QUESTION 112

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 fabrikam.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: Configure network services and access**

**Explanation**



### **Explanation/Reference:**

#### **Primary zone**

When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named *zone\_name.dns* and it is located in the %windir%\System32\Dns folder on the server.

#### **Secondary zone**

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. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.

#### **Stub zone**

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.

<https://technet.microsoft.com/en-us/library/cc771898.aspx>

### **QUESTION 113**

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**

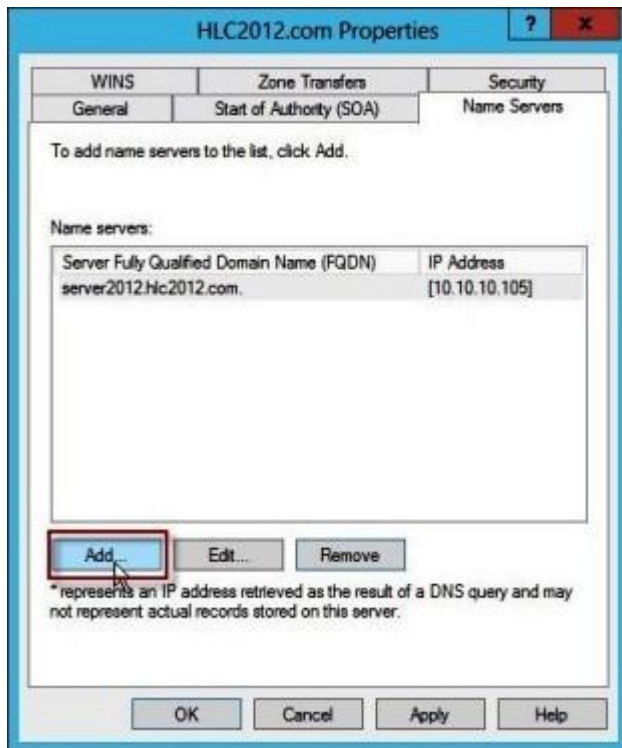
**Section: Configure network services and access**

**Explanation**

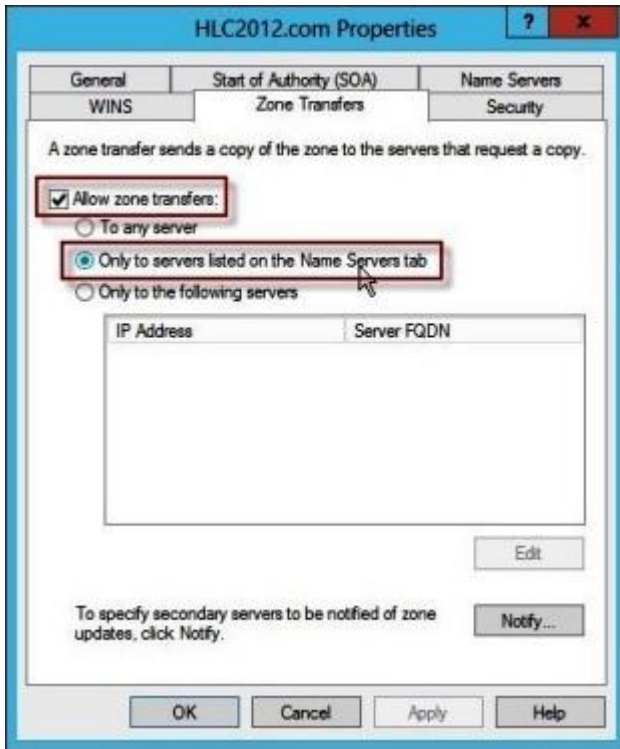
### **Explanation/Reference:**

Typically, adding a secondary DNS server to a zone involves three steps:

1. On the primary DNS server, *add the prospective secondary DNS server to the list of name servers* that are authoritative for the zone.



2. On the primary DNS server, verify that the transfer settings for the zone permit the zone to be transferred to the prospective secondary DNS server.



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

[https://technet.microsoft.com/en-us/library/cc816885\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc816885(v=ws.10).aspx)

#### QUESTION 114

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

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

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

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

#### D. Network Connections

**Correct Answer: C**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

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.

[https://technet.microsoft.com/en-us/library/ee382323\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee382323(v=ws.10).aspx)

#### QUESTION 115

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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

#### Primary zone

When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named *zone\_name.dns* and it is located in the %windir%\System32\Dns folder on the server.

**Secondary zone**

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. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.

**Stub zone**

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.

**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.

<https://technet.microsoft.com/en-us/library/cc771898.aspx>

**QUESTION 116**

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 DC6.

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: Configure network services and access**

## **Explanation**

### **Explanation/Reference:**

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.

<https://technet.microsoft.com/en-us/library/cc754292.aspx>

### **QUESTION 117**

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: dal.contoso.com  
Internal IPv6 address: 2002:c1a8:6a:3333::1  
External IPv4 address: 65.55.37.62

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

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

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

### **Exhibit:**

**Remote Access Setup**

---

**Infrastructure Server Setup**  
Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server

**DNS**

DNS Suffix Search List Management

Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.

	Name Suffix	DNS Server Address
▶	contoso.com	2002:c1a8:6a:3333::1
	server5.contoso.com	
*		

Select a local name resolution option:

☐ Use local name resolution if the name does not exist in DNS (most restrictive)

☒ Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended)

☐ Use local name resolution for any kind of DNS resolution error (least restrictive)

< Back
Next >
Finish
Cancel

- 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 da1.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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

Your DNS suffix search list should normally match the namespace rules in your NRPT. This is especially important in split-brained DNS scenarios, in which both an organization's internal private network and its publicly accessible resources use the same DNS domain name (such as contoso.com). To help DirectAccess clients resolve internal names correctly from the Internet, you can enter the full name of internal resources in the Name Suffix list and then specify for these resources a DNS server address corresponding to the IPv6 address of the internal DNS server. Likewise, you can enter the full

name of *external* resources in the Name Suffix list and then leave the DNS server address blank. A blank entry in the DNS server address directs the client to use the DNS server currently assigned to its network connection for the suffix or FQDN specified.

<https://www.microsoftpressstore.com/articles/article.aspx?p=2216993>

#### **QUESTION 118**

You have a DNS server named Server1. Server1 has a primary zone named contoso.com. Zone Aging/Scavenging is configured for the contoso.com zone.

One month ago, an administrator removed a server named Server2 from the network. You discover that a static resource record for Server2 is present in contoso.com. Resource records for decommissioned client computers are removed automatically from contoso.com. You need to ensure that the static resource records for all of the servers are removed automatically from contoso.com.

What should you modify?

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

**Correct Answer: B**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

#### **Prerequisites for aging/scavenging**

Before the aging and scavenging features of DNS can be used, several conditions must be met:

1. *Scavenging and aging must be enabled both at the DNS server and on the zone.*

By default, aging and scavenging of resource records is disabled.

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

Typically, only those resource records added dynamically using the DNS dynamic update protocol are subject to aging and scavenging.

You can, however, enable scavenging for other resource records added through non-dynamic means. For records added to zones in this way, either by loading a text-based zone file from another DNS server or by manually adding them to a zone, a time stamp of zero is set. This makes these records ineligible for use in aging/scavenging operations.

In order to change this default, you can administer these records individually, to reset and permit them to use a current (non-zero) time stamp value.



This enables these records to become aged and scavenged.

<https://technet.microsoft.com/en-us/library/cc759204>

#### **QUESTION 119**

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 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: Configure network services and access**

**Explanation**

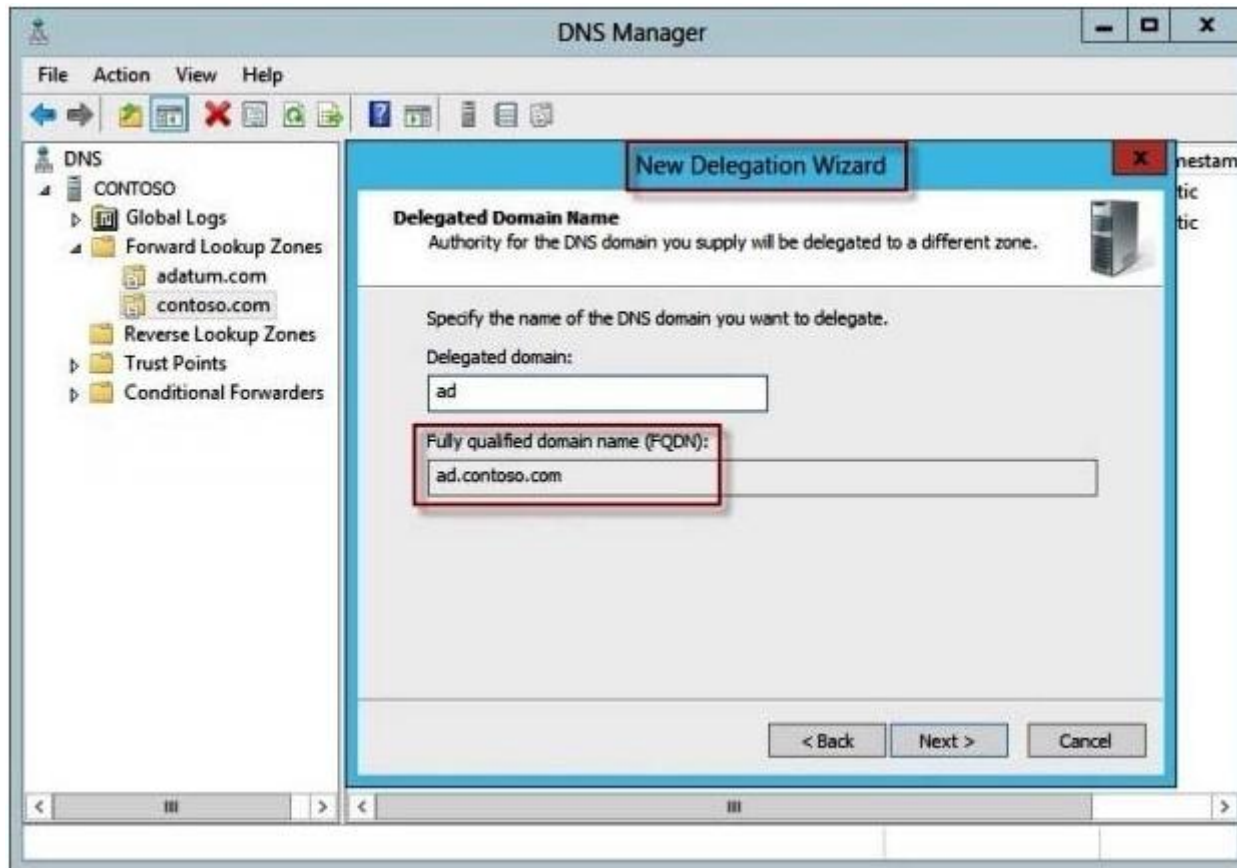
**Explanation/Reference:**

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.

When you delegate a zone, remember that for each new zone that you create, you will need delegation records in other zones that point to the authoritative DNS servers for the new zone. This is necessary both to transfer authority and to provide correct referral to other DNS servers and clients of the new servers that are being made authoritative for the new zone.

**To create a zone delegation using the Windows interface**

1. Open DNS Manager.
2. In the console tree, right-click the applicable subdomain, and then click **New Delegation**.



3. Follow the instructions in the New Delegation Wizard to finish creating the new delegated domain.

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

<https://technet.microsoft.com/en-us/library/cc753500.aspx>

#### QUESTION 120

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: Configure network services and access**

**Explanation**

### Explanation/Reference:

Using the Windows interface, open DNS. In the console tree, right-click the applicable zone and click **Transfer from master**.



<https://technet.microsoft.com/en-us/library/cc779391>

### QUESTION 121

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:** Configure network services and access

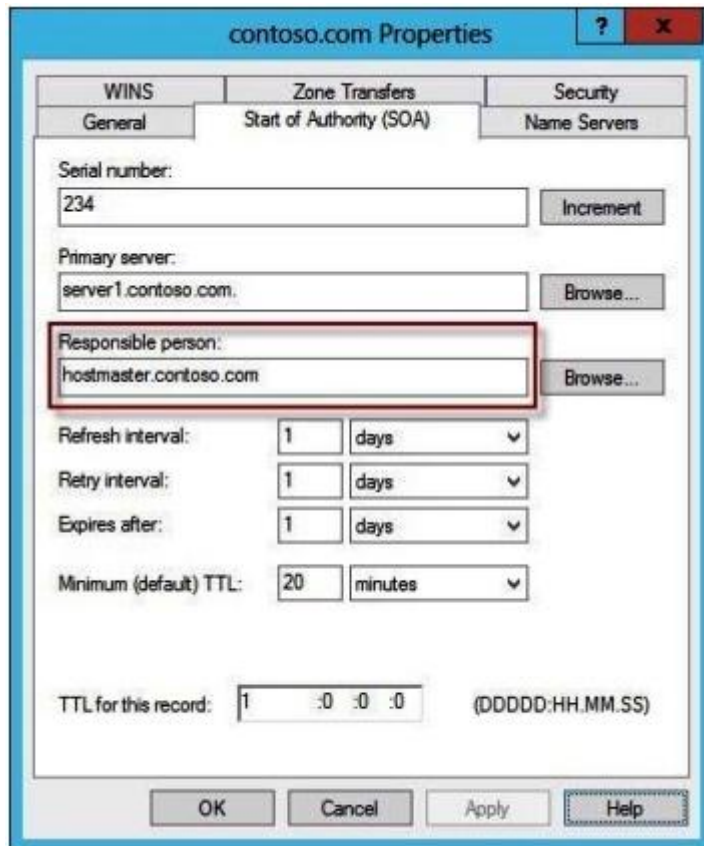
**Explanation**

**Explanation/Reference:**

**DNS best practices**

- **Enter the correct e-mail address of the responsible person for each zone you add to or manage on a DNS server.**

This field is used by applications to notify DNS administrators for a variety of reasons. For example, query errors, incorrect data returned in a query, and security problems are a few ways in which this field can be used. While most Internet e-mail addresses contain the at sign (@) when used in e-mail applications, this symbol must be replaced with a period (.) when entering an e-mail address for this field. For example, instead of "administrator@microsoft.com", you would use "administrator.microsoft.com".



<https://technet.microsoft.com/en-us/library/cc778439>

### QUESTION 122

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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

A *stub zone* is a copy of a zone that contains only the original zone's start of authority (SOA) resource record, the name server (NS) resource records listing the authoritative servers for the zone, and the glue address (A) resource records that are needed to identify these authoritative servers.

A DNS server that is hosting a stub zone is configured with the IP address of the authoritative server from which it loads. DNS servers can use stub zones for both iterative and recursive queries. When a DNS server hosting a stub zone receives a recursive query for a computer name in the zone to which the stub zone refers, the DNS server uses the IP address to query the authoritative server, or, if the query is iterative, returns a referral to the DNS servers listed in the stub zone.

Stub zones are updated at regular intervals, determined by the refresh interval of the SOA resource record for the stub zone. When a DNS server loads a stub zone, it queries the zone's primary servers for SOA resource records, NS resource records at the zone's root, and glue address (A) resource records. The DNS server attempts to update its resource records at the end of the SOA resource record's refresh interval. To update its records, the DNS server queries the primary servers for the resource records listed earlier.

You can use stub zones to ensure that the DNS server that is authoritative for a parent zone automatically receives updates about the DNS servers that are authoritative for a child zone. To do this, add the stub zone to the server that is hosting the parent zone. Stub zones can be either file-based or Active Directory–integrated. If you use Active Directory–integrated stub zones, you can configure them on one computer and let Active Directory replication propagate them to other DNS servers running on domain controllers.

<https://technet.microsoft.com/en-us/library/cc786068>

### **QUESTION 123**

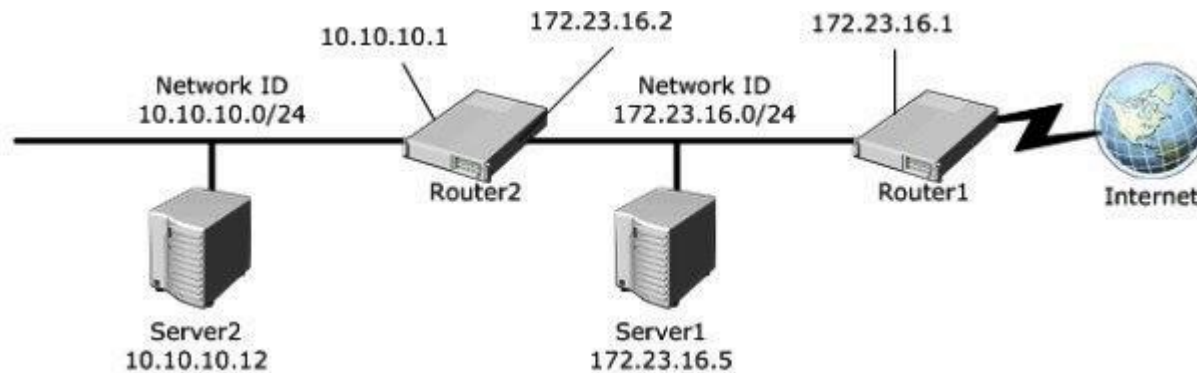
Your network is configured as shown in the exhibit. (Click the Exhibit button.)

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?

**Exhibit:**



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

**Correct Answer:** A

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

**To add a static IP route**

1. Open Command Prompt.
2. At the command prompt, type:

```
route add [destination] mask [subnetmask] [gateway] metric [costmetric]
```

where:



Static IP route entry	Definition
<i>destination</i>	Specifies either an IP address or host name for the network or host.
<i>subnetmask</i>	Specifies a subnet mask to be associated with this route entry. If <i>subnetmask</i> is not specified, 255.255.255.255 is used.
<i>gateway</i>	Specifies either an IP address or host name for the gateway or router to use when forwarding.
<i>costmetric</i>	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 <i>costmetric</i> is not specified, 1 is used.

For example, to add a static route to the 10.10.10.0 network that uses a subnet mask of 255.255.255.0 (or /24 CIDR notation), a gateway of 172.23.16.2, and a cost metric of 100, you type the following at a command prompt:

```
route add 10.10.10.0 mask 255.255.255.0 172.23.16.2 metric 100
```

Routes added by using the **-p** option are stored in the registry under the following key:

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes
```

<https://technet.microsoft.com/en-us/library/cc757323>

#### QUESTION 124

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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

### **Configure AD Integrated Zones**

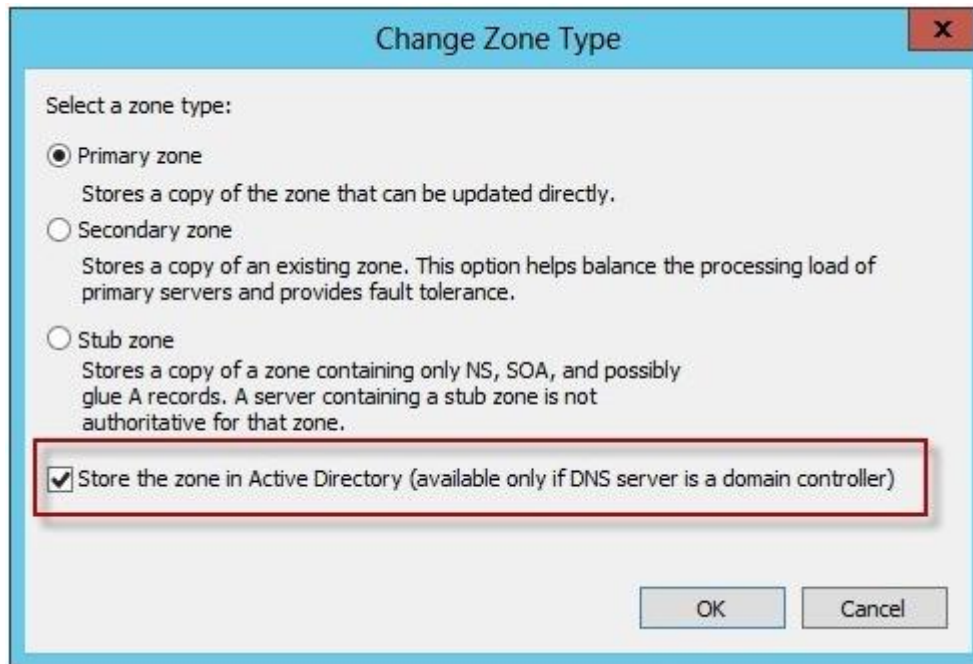
You can use this procedure to change a primary zone so that it is stored in Active Directory Domain Services (AD DS). When you store a primary zone in AD DS, the zone type is changed from primary to Active Directory (AD)-integrated. [Note: Security Properties cannot be applied to Standard Primary Zones.]

To change a zone type to AD integrated using the Windows interface

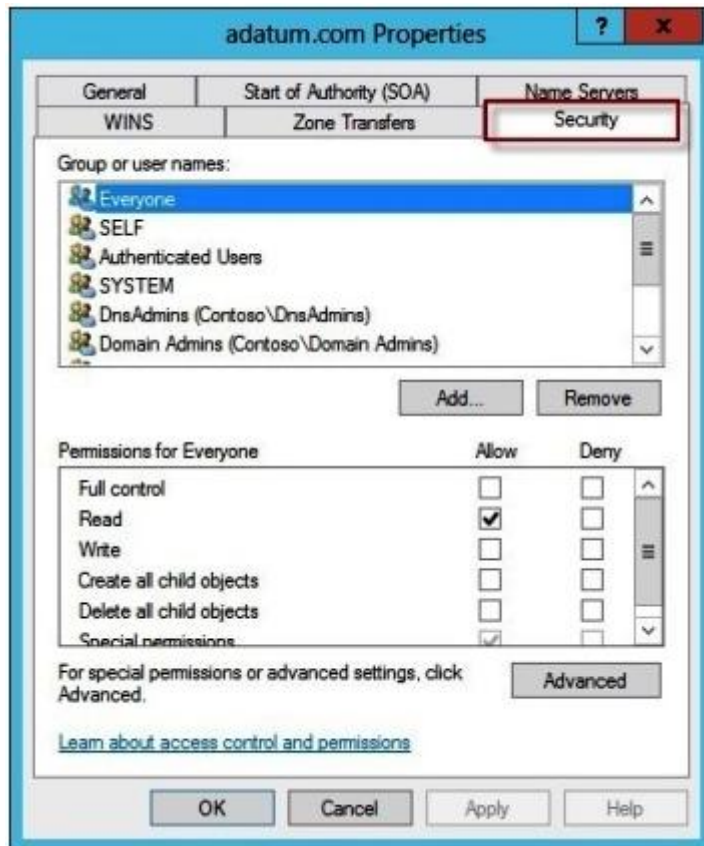
1. Click **Start**, click **Run**, type **dnsmgmt.msc**, and then press ENTER. The DNS Manager console will open.
2. In the console tree, right-click the zone you wish to configure, and then select **Properties**.



3. On the **General** tab, next to **Type**, click **Change**.
4. In **Change Zone Type**, select the **Store the zone in Active Directory** check box, and then click **OK**.



5. Click **Yes** when you are prompted to confirm this change, and then click **OK** to close zone properties.



Note that the **Security** tab is now available in the **Properties** dialog.

<https://technet.microsoft.com/en-us/library/ee649181>

### QUESTION 125

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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

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.

<https://technet.microsoft.com/en-us/library/jj134148.aspx>

#### **QUESTION 126**

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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

To load balance sessions in an RD Session Host server farm, you can use the RD Connection Broker Load Balancing feature together with Domain Name System (DNS) round robin. To configure DNS, you must create a DNS host resource record for each RD Session Host server in the farm that maps the RD Session Host server's IP address to the RD Session Host server farm name in DNS.

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

#### **QUESTION 127**

Your network has a router named Router1 that provides access to the Internet. You have a server named Server1 that runs Windows Server 2012 R2. Server1 is to use Router1 as the default gateway. A new router named Router2 is added to the network. Router2 provides access to the Internet. The IP address of the internal interface on Router2 is 10.1.14.254.

You need to configure Server1 to use Router2 to connect to the Internet if Router1 fails.

What should you do on Server1?

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

**Correct Answer: D**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

**To add a static IP route**

1. Open Command Prompt.
2. At the command prompt, type:

```
route add [destination] mask [subnetmask] [gateway] metric [costmetric]
```

where:

Static IP route entry	Definition
<i>destination</i>	Specifies either an IP address or host name for the network or host.
<i>subnetmask</i>	Specifies a subnet mask to be associated with this route entry. If <i>subnetmask</i> is not specified, 255.255.255.255 is used.
<i>gateway</i>	Specifies either an IP address or host name for the gateway or router to use when forwarding.
<i>costmetric</i>	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 <i>costmetric</i> is not specified, 1 is used.

For example, to add a static route to the 10.10.10.0 network that uses a subnet mask of 255.255.255.0 (or /24 CIDR notation), a gateway of 172.23.16.2, and a cost metric of 100, you type the following at a command prompt:

```
route add [destination] mask 255.255.255.0 10.1.14.254 metric 500
```

Routes added by using the **-p** option are stored in the registry under the following key:

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes
```

<https://technet.microsoft.com/en-us/library/cc757323>

Logical analysis:

The new route is an alternative if Router1 fails, so the metric cannot be 1. This eliminates two answer options. Since no specific destination host name or IP address is provided in the question, the destination address of 10.2.14.0/24 cannot be verified as appropriate. So, only one valid answer option remains.

### QUESTION 128

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

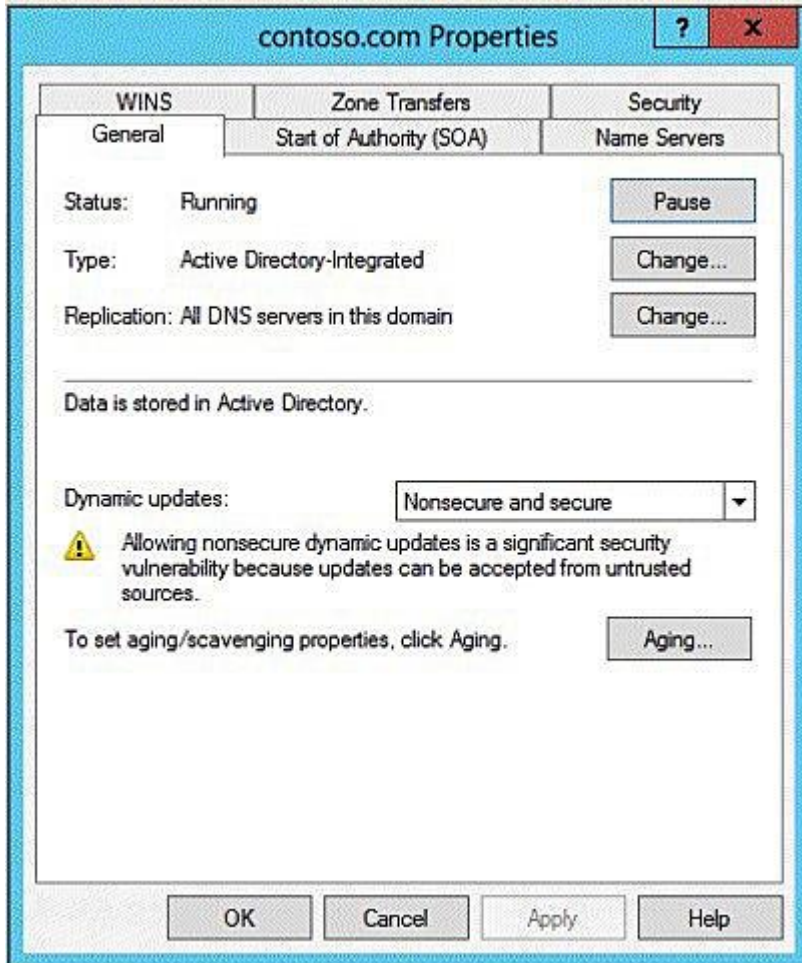
The domain contains a server named Server1 that is part of a workgroup named Workgroup. Server1 is configured to use DC1 as a DNS server.



You need to ensure that Server1 dynamically registers a host (A) record in the contoso.com zone.

What should you configure?

**Exhibit:**



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

**Correct Answer: D**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

#### **Configuring DNS client settings**

DNS configuration involves the following tasks when configuring TCP/IP properties for each computer:

- Setting a DNS computer or host name for each computer. For example, in the fully qualified domain name (FQDN) *wkstn1.example.microsoft.com.*, the DNS computer name is the leftmost label *wkstn1*.
- Setting a **primary DNS suffix for the computer**, which is placed after the computer or host name to form the FQDN. Using the previous example, the primary DNS suffix would be *example.microsoft.com*.
- Setting a list of DNS servers for clients to use when resolving DNS names, such as a preferred DNS server, and any alternate DNS servers to use if the preferred server is not available.
- Setting the DNS suffix search list or search method to be used by the client when it performs DNS query searches for short, unqualified domain names.

<https://technet.microsoft.com/en-us/library/cc778792>

#### **QUESTION 129**

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: A**

**Section: Configure network services and access**

## **Explanation**

### **Explanation/Reference:**

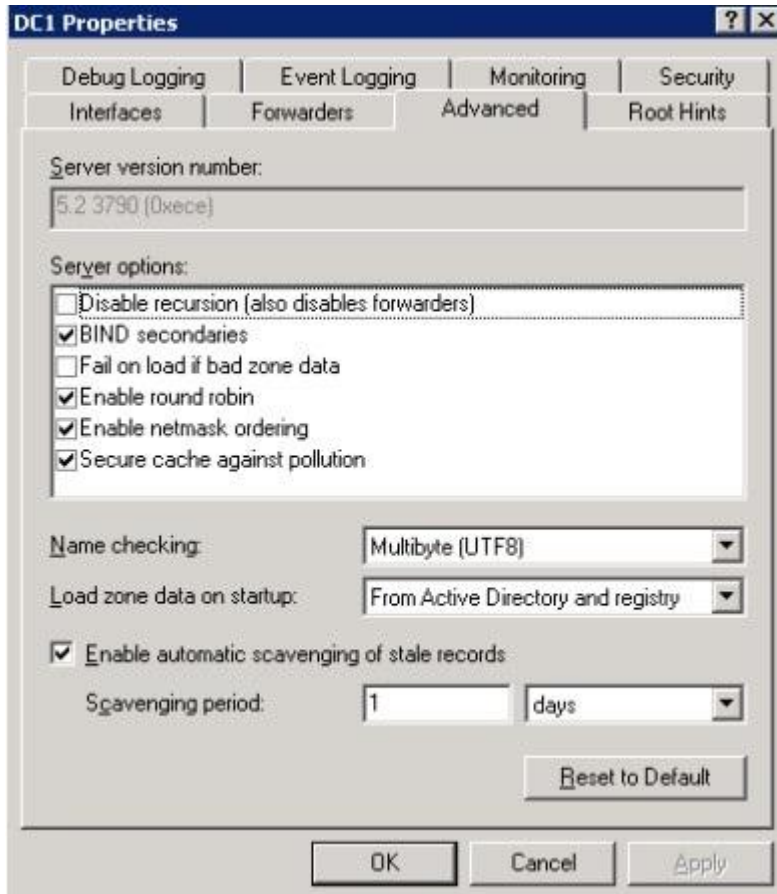
#### **BIND secondaries**

Determines whether to use fast transfer format for transfer of a zone to DNS servers running legacy Berkeley Internet Name Domain (BIND) implementations.

<https://technet.microsoft.com/en-us/library/cc757837>

Enables the Domain Name System (DNS) server to communicate with non-Microsoft DNS servers that use an earlier, slower version of the DNS BIND service.

<https://technet.microsoft.com/en-us/library/cc940771.aspx>



### QUESTION 130

Your network contains two DNS servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 hosts a primary zone for contoso.com. Server2 hosts a secondary zone for contoso.com.

You need to ensure that Server2 replicates changes to the contoso.com zone every five minutes.

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

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

D. Refresh interval

**Correct Answer:** D

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

The process of replicating a zone file to multiple DNS servers is called zone transfer. Zone transfer is achieved by copying the zone file from one DNS server to a second DNS server. Zone transfers can be made from both primary and secondary DNS servers.

When the DNS Server service on the secondary DNS server starts, or the refresh interval of the zone has expired (by default it is set to 15 minutes in the SOA RR of the zone), the secondary DNS server will query the master DNS server for the changes.

The screenshot shows the 'adatum.com Properties' dialog box with the 'Zone Transfers' tab selected. Within this tab, the 'Start of Authority (SOA)' sub-tab is active. The 'Refresh interval' is set to 5 minutes and is highlighted with a red rectangle. Other fields include: Serial number (1), Primary server (server1.contoso.com), Responsible person (hostmaster.contoso.com), Retry interval (10 minutes), Expires after (1 days), Minimum (default) TTL (1 hours), and TTL for this record (0:1:0:0). The dialog box has standard Windows controls at the bottom: OK, Cancel, Apply, and Help.

<https://technet.microsoft.com/en-us/library/dd197427>

### QUESTION 131

You have installed Routing and Remote Access on Server1.

What should you configure next to use it as a NAT server?

- A. Add New Interface
- B. Create Static Route
- C. Configure the IPv4 DHCP Relay Agent
- D. Configure the IPv6 DHCP Relay Agent

**Correct Answer: A**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

**To enable network address translation addressing**

1. In the RRAS MMC snap-in, expand *Your Server Name*. If you are using Server Manager, expand **Routing and Remote Access**.
2. Expand **IPv4**, right-click **NAT**, and then click **Properties**.
3. If you do not have a DHCP server on the private network, then you can use the RRAS server to respond to DHCP address requests. To do this, on the **Address Assignment** tab, select the **Automatically assign IP addresses by using the DHCP allocator** check box.
4. To allocate addresses to clients on the private network by acting as a DHCP server, in **IP address and Mask**, configure a subnet address from which the addresses are assigned. For example, if you enter 192.168.0.0 and a subnet mask of 255.255.255.0, then the RRAS server responds to DHCP requests with address assignments from 192.168.0.1 through 192.168.0.254.
5. (Optional) To exclude addresses in the configured network range from being assigned to DHCP clients on the private network, click **Exclude**, click **Add**, and then configure the addresses.
6. To add the public interface to the NAT configuration, right-click **NAT**, and then click **New Interface**. Select the interface connected to the public network, and then click **OK**.
7. On the **NAT** tab, click **Public interface connected to the Internet** and **Enable NAT on this interface**, and then click **OK**.
8. If you want to add additional public addresses assigned to this interface or configure service and port mappings to computers on the private network,

see "IPv4 - NAT - Interface - Properties Page" (<https://technet.microsoft.com/en-us/library/dd469796.aspx>).

9. To add the private interface to the NAT configuration, right-click **NAT**, and then click **New Interface**. Select the interface connected to the private network, and then click **OK**.

10. On the **NAT** tab, click **Private interface connected to private network**, and then click **OK**.

<https://technet.microsoft.com/en-us/library/dd469812.aspx>

### QUESTION 132

You upgraded all of your locations to Windows Server 2012 R2 and implemented the routing capability built into the servers. You chose to implement RIP.

After implementing the routers, you discover that routes that you don't want your network to consider are updating your RIP routing tables.

What can you do to control which networks the RIP routing protocol will communicate with on your network?

- A. Configure TCP/IP filtering.
- B. Configure RIP route filtering.
- C. Configure IP packet filtering.
- D. Configure RIP peer filtering.
- E. There is no way to control this behavior.

**Correct Answer: B**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

#### Route filters

You can configure route filters on each RIP interface so that the only routes considered for addition to the routing table are those that reflect reachable network IDs within the internetwork. For example, if an organization is using subnets of the private network ID 10.0.0.0, route filtering can be used so that the RIP routers discard all routes except those within the 10.0.0.0 network ID.

<https://technet.microsoft.com/en-us/library/cc739065>

### QUESTION 133

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: Configure network services and access**

**Explanation**

**Explanation/Reference:**

For DirectAccess connections, when the network connection speed cannot be determined, Group Policy processing defaults to slow-link mode. During sign-in, if a slow link is detected, Group Policy automatically switches to asynchronous processing. A new policy setting enables administrators to configure all 3G connections so that they are treated as a slow link. To disable 3G slow-link connections, select the **Always treat WWAN connections as a slow link** check box after you have enabled the **Configure Group Policy slow link detection** policy setting.

The **Configure Group Policy slow link detection** policy setting is located under Computer Configuration\Policies\Administrative Templates\System\Group Policy in the Group Policy Management Editor.

<https://technet.microsoft.com/en-us/library/dn265973.aspx>

#### **QUESTION 134**

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: Configure network services and access****Explanation****Explanation/Reference:**

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.

<https://technet.microsoft.com/en-us/library/cc754292.aspx>

**QUESTION 135**

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: Configure network services and access****Explanation****Explanation/Reference:**

Other DNS servers that are configured to load and host the zone use the expire interval to determine when zone data expires if it is not successfully transferred. By default, the expire interval for each zone is set to one day.

**To adjust the expire interval for a zone using the Windows interface:**

1. Open DNS Manager. To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. In the console tree, right-click the applicable zone, and then click **Properties**.

3. On the **General** tab, verify that the zone type is either **Primary** or **Active Directory-integrated**.
4. Click the **Start of Authority (SOA)** tab.
5. In **Expires after**, click a time period in minutes, hours, or days, and then type a number in the text box.
6. Click **OK** to save the adjusted interval.

**To adjust the expire interval for a zone using a command line:**

1. Open a command prompt. To open an elevated Command Prompt window, click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. At the command prompt, type the following command, and then press ENTER:

```
dnscmd <ServerName> /RecordAdd <ZoneName> <NodeName> [/Aging] [/OpenAcl] [<Ttl>] SOA <PrimSvr> <Admin>  
<Serial#> <Refresh> <Retry> <Expire> <MinTTL>
```

<https://technet.microsoft.com/en-us/library/cc816704>

**QUESTION 136**

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

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

Server name	Configuration
Server1	<ul style="list-style-type: none"><li>• Domain controller</li><li>• Windows Server Update Services (WSUS)</li></ul>
Server2	<ul style="list-style-type: none"><li>• Read-only domain controller (RODC)</li><li>• DNS server</li><li>• DHCP server</li></ul>
Server3	<ul style="list-style-type: none"><li>• Domain controller</li><li>• DHCP server</li></ul>
Server4	<ul style="list-style-type: none"><li>• Member server</li><li>• Distributed File System (DFS)</li></ul>

You need to deploy IP Address Management (IPAM) to manage DNS and DHCP.

On which server should you install IPAM?

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

**Correct Answer:** D

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

IPAM Server must be installed on a domain member computer running Windows Server® 2012 or a later operating system. The IPAM server is intended as a single purpose server and should not be installed with other network infrastructure roles such as DNS or DHCP. You cannot install IPAM on a domain controller. If IPAM Server is running on a computer that is also running the DHCP Server role, discovery of DHCP servers on the network will be disabled.

<https://technet.microsoft.com/en-us/library/jj878315.aspx>

#### **QUESTION 137**

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

You promote Server1 to a domain controller. You need to view the service location (SRV) records that Server1 registers in DNS.

What should you do on Server1?

- A. Open the Netlogon.dns file.
- B. Open the Srv.sys file.
- C. Run ipconfig /displaydns
- D. Run Get-DnsServerDiagnostics.

**Correct Answer:** A

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

When you use third-party DNS servers to support Active Directory, you can verify the registration of domain controller locator resource records. If the server does not support dynamic update, you need to add these records manually.

The Netlogon service creates a log file that contains all the locator resource records and places the log file in the following location:

`%SystemRoot%\System32\Config\Netlogon.dns`

You can check this file to find out which locator resource records are created for the domain controller.

<https://technet.microsoft.com/en-us/library/cc959303.aspx>

#### QUESTION 138

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

You create a group Managed Service Account named gservice1. You need to configure a service named Service1 to run as the gservice1 account.

How should you configure Service1?

- A. From Windows PowerShell, run Set-Service and specify the -PassThrough parameter.
- B. From a command prompt, run sc.exe and specify the config parameter.
- C. From Windows PowerShell, run Set-Service and specify the -StartupType parameter.
- D. From a command prompt, run sc.exe and specify the privs parameter.

**Correct Answer: B**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

**Sc config** modifies the value of a service's entries in the registry and in the Service Control Manager database.

```
sc [<ServerName>] config [<ServiceName>] [type= {own | share | kernel | filesys | rec | adapt | interact  
type= {own | share}}] [start= {boot | system | auto | demand | disabled | delayed-auto}] [error= {normal |  
severe | critical | ignore}] [binpath= <BinaryPathName>] [group= <LoadOrderGroup>] [tag= {yes | no}] [depend=  
<dependencies>] [obj= {<AccountName> | <ObjectName>}] [displayname= <DisplayName>] [password= <Password>]
```

<https://technet.microsoft.com/en-us/library/cc990290>

#### QUESTION 139

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

You need to create a custom Active Directory Application partition.

Which tool should you use?

- A. Netdom
- B. Ntdsutil
- C. Dsmo
- D. Dsmain

**Correct Answer:** B

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). You can use the **ntdsutil** commands to perform database maintenance of AD DS, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.

The **partition management** command, short form “**pa m**”, manages directory partitions.

<https://technet.microsoft.com/en-us/library/cc753343.aspx>

#### **QUESTION 140**

You administer a Microsoft Windows Server 2012 R2 domain named ABC.com. The ABC.com domain has two server computers named ABC-SR11 and ABC-SR12, both of which host the DFS replication roles and are members of the same DFS Replication group.

ABC.com is to relocate ABC-SR12 to a new office that will be connected to the main office by a VPN connection across the internet. You need to configure the amount of network bandwidth that can be consumed by the replication between the two servers.

Which of the following actions should you take?

- A. You should configure the Quota Size of Staging Folder and Conflict and Deleted Folder.
- B. You should configure the replication group schedule.
- C. You should configure the replication filters.
- D. You should configure the replication topology.

**Correct Answer:** B

**Section:** Configure network services and access

**Explanation**

**Explanation/Reference:**

### To edit the replication schedule and bandwidth

- To edit the schedule and bandwidth for a replication group, use the following steps:
  1. In the console tree under the **Replication** node, right-click the replication group with the schedule that you want to edit, and then click **Edit Replication Group Schedule**.
  2. Use the **Edit Schedule** dialog box to control when replication occurs, as well as the maximum amount of bandwidth replication can consume.
- To edit the schedule and bandwidth for a specific connection, use the following steps:
  1. In the console tree under the **Replication** node, select the appropriate replication group.
  2. Click the **Connections** tab, right-click the connection that you want to edit, and then click **Properties**.
  3. Click the **Schedule** tab, select **Custom connection schedule** and then click **Edit Schedule**.
  4. Use the **Edit Schedule** dialog box to control when replication occurs, as well as the maximum amount of bandwidth replication can consume.

<https://msdn.microsoft.com/en-us/library/Cc732278.aspx>

### QUESTION 141

You work as a Network Administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain named ABC.com. All servers in the ABC.com domain have Microsoft Windows Server 2012 R2 installed. All domain controllers in the domain are configured as DNS servers and host an Active Directory integrated zone for ABC.com.

You need to configure a Web server solution to host the company Intranet website. You configure three Windows Server 2012 R2 servers. The three Web servers dynamically register their IP addresses and hostnames in the ABC.com DNS zone.

You plan to use DNS Round Robin to distribute connections to <http://intranet.ABC.com> between the three Web servers. You need to create the DNS server records.

What DNS records should you create?

- A. You should create one Host (A) record for [intranet.ABC.com](http://intranet.ABC.com).
- B. You should create one Alias (CNAME) record for [intranet.ABC.com](http://intranet.ABC.com).
- C. You should create three Host (A) records for [intranet.ABC.com](http://intranet.ABC.com).
- D. You should create three Alias (CNAME) records for [intranet.ABC.com](http://intranet.ABC.com).
- E. You should create one Host (A) record for [intranet.ABC.com](http://intranet.ABC.com) and three Alias (CNAME) records, one for each Web server.
- F. You should create one Alias (CNAME) record for [intranet.ABC.com](http://intranet.ABC.com) and three Host (A) records, one for each Web server.

**Correct Answer: C**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

### **Configuring round robin**

Round robin is a local balancing mechanism used by DNS servers to share and distribute network resource loads. You can use it to rotate all resource record (RR) types contained in a query answer if multiple RRs are found.

By default, DNS uses round robin to rotate the order of RR data returned in query answers where multiple RRs of the same type exist for a queried DNS domain name. This feature provides a simple method for load balancing client use of Web servers and other frequently queried multihomed computers.

If round robin is disabled for a DNS server, the order of the response for these queries is based on a static ordering of RRs in the answer list as they are stored in the zone (either its zone file or Active Directory).

### **Example: Round-robin rotation**

A forward lookup-type query (for all A RRs that match a DNS domain name) is made for a multihomed computer (multihomed.example.microsoft.com) that has three IP addresses. Separate A RRs are used to map the host's name to each of these IP addresses in the zone. In the stored example.microsoft.com zone, the RRs appear in this fixed order:

```
multihomed IN A 10.0.0.1  
multihomed IN A 10.0.0.2  
multihomed IN A 10.0.0.3
```

The first DNS client that queries the server to resolve this host's name receives the list in default order. When a second client sends a subsequent query to resolve this name, the list is rotated as follows:

```
multihomed IN A 10.0.0.2  
multihomed IN A 10.0.0.3  
multihomed IN A 10.0.0.1
```

[https://technet.microsoft.com/en-us/library/Cc787484\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Cc787484(v=WS.10).aspx)

### **QUESTION 142**

You are the network administrator for a midsize computer company. You have a single Active Directory forest, and your DNS servers are configured as Active Directory Integrated zones.

When you look at the DNS records in Active Directory, you notice that there are many records for computers that do not exist on your domain. You want to make sure only domain computers register with your DNS servers.

What should you do to resolve this issue?

- A. Set dynamic updates to None.
- B. Set dynamic updates to Nonsecure and Secure.
- C. Set dynamic updates to Domain Users Only.
- D. Set dynamic updates to Secure Only.

**Correct Answer: D**

**Section: Configure network services and access**

**Explanation**

**Explanation/Reference:**

DNS client computers can use dynamic update to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address. Secure dynamic update is supported only for Active Directory-integrated zones. If the zone type is configured differently, you must change the zone type and directory-integrate the zone before securing it for DNS dynamic updates.

[https://technet.microsoft.com/en-us/library/Ee649287\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Ee649287(v=WS.10).aspx)

#### **QUESTION 143**

You have a server named LON-SVR1 that runs Windows Server 2012 R2. LON-SVR1 has the Remote Access server role installed. LON-SVR1 is located in the perimeter network.

The IPv4 routing table on LON-SVR1 is configured as shown in the following exhibit. (Click the Exhibit button.)

Your company purchases an additional router named Router1. Router1 has an interface that connects to the perimeter network and an interface that connects to the Internet. The IP address of the interface that connects to the perimeter network is 172.16.0.2. You need to ensure that LON-SVR1 will route traffic to the Internet by using Router1 if the current default gateway is unavailable.

How should you configure the static route on LON-SVR1? To answer, select the appropriate static route in the answer area.

**Exhibit:**



LON-SVR1 - IP Routing Table				
Destination	Network mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.16.0.1	Local Area C...	276
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	51
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	306
172.16.0.0	255.255.0.0	0.0.0.0	Local Area C...	276
172.16.0.21	255.255.255.255	0.0.0.0	Local Area C...	276
172.16.255.255	255.255.255.255	0.0.0.0	Local Area C...	276
224.0.0.0	240.0.0.0	0.0.0.0	Local Area C...	276
255.255.255.255	255.255.255.255	0.0.0.0	Local Area C...	276

Hot Area:

IPv4 Static Route

Interface:

Local Area Connection

Destination:

0 . 0 . 0 . 0

Network mask:

0 . 0 . 0 . 0

Gateway:

172 . 16 . 0 . 2

Metric:

300

☒ Use this route to initiate demand-dial connections

[For more information](#)

OK

Cancel

IPv4 Static Route

Interface:

Local Area Connection

Destination:

0 . 0 . 0 . 0

Network mask:

0 . 0 . 0 . 0

Gateway:

172 . 16 . 0 . 2

Metric:

255

☒ Use this route to initiate demand-dial connections

[For more information](#)

OK

Cancel

IPv4 Static Route

Interface:

Local Area Connection

Destination:

172 . 16 . 0 . 0

Network mask:

255 . 240 . 0 . 0

Gateway:

172 . 16 . 0 . 2

Metric:

300

☒ Use this route to initiate demand-dial connections

[For more information](#)

OK

Cancel

IPv4 Static Route

Interface:

Local Area Connection

Destination:

0 . 0 . 0 . 0

Network mask:

255 . 255 . 255 . 255

Gateway:

172 . 16 . 0 . 2

Metric:

300

☒ Use this route to initiate demand-dial connections

[For more information](#)

OK

Cancel

Correct Answer:



## Section: Configure network services and access

### Explanation

### Explanation/Reference:

#### Default Route

The entry corresponding to the default gateway configuration is a **network destination of 0.0.0.0** with a **network mask (netmask) of 0.0.0.0**. Any destination IP address joined with 0.0.0.0 by a logical AND results in 0.0.0.0. Therefore, for any IP address, the default route produces a match. If the

default route is chosen because no better routes were found, the IP packet is forwarded to the IP address in the Gateway column using the interface corresponding to the IP address in the Interface column.

### **Metric**

A number used to indicate the cost of the route so the best route among possible multiple routes to the same destination can be selected.

### **Route Determination Process**

To determine which routing table entry is used for the forwarding decision, IP uses the following process:

For each entry in a routing table, perform a bit-wise logical AND between the destination IP address and the network mask. Compare the result with the network ID of the entry for a match.

The list of matching routes is compiled. The route that has the longest match (the route that matched the most amount of bits with the destination IP address) is chosen. The longest matching route is the most specific route to the destination IP address. If multiple entries with the longest match are found (multiple routes to the same network ID, for example), the router uses the **lowest metric** to select the best route. If multiple entries exist that are the longest match and the lowest metric, the router is free to choose which routing table entry to use.

<https://technet.microsoft.com/en-us/library/cc958823.aspx>

### **QUESTION 144**

Your network contains an Active Directory domain named fabrikam.com. You implement DirectAccess and an IKEv2 VPN.

You need to view the properties of the VPN connection.

Which connection properties should you view? To answer, select the appropriate connection properties in the answer area.

### **Hot Area:**



**Correct Answer:**



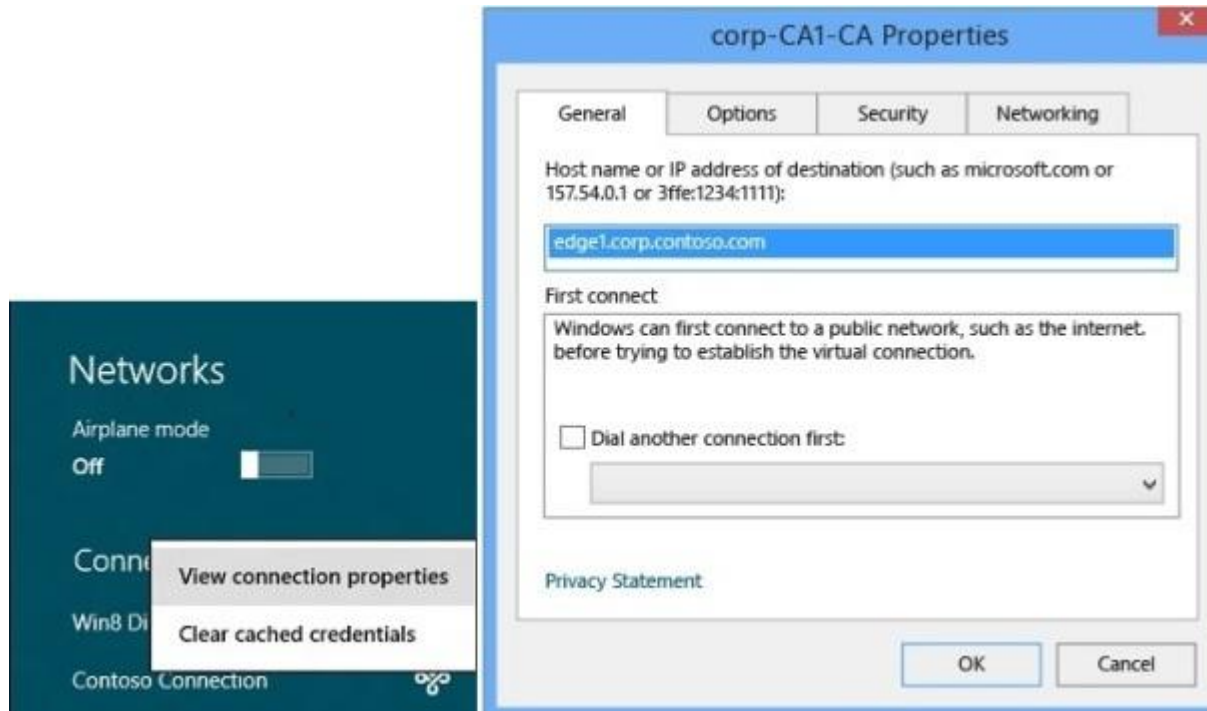
**Section: Configure network services and access**  
**Explanation**

**Explanation/Reference:**

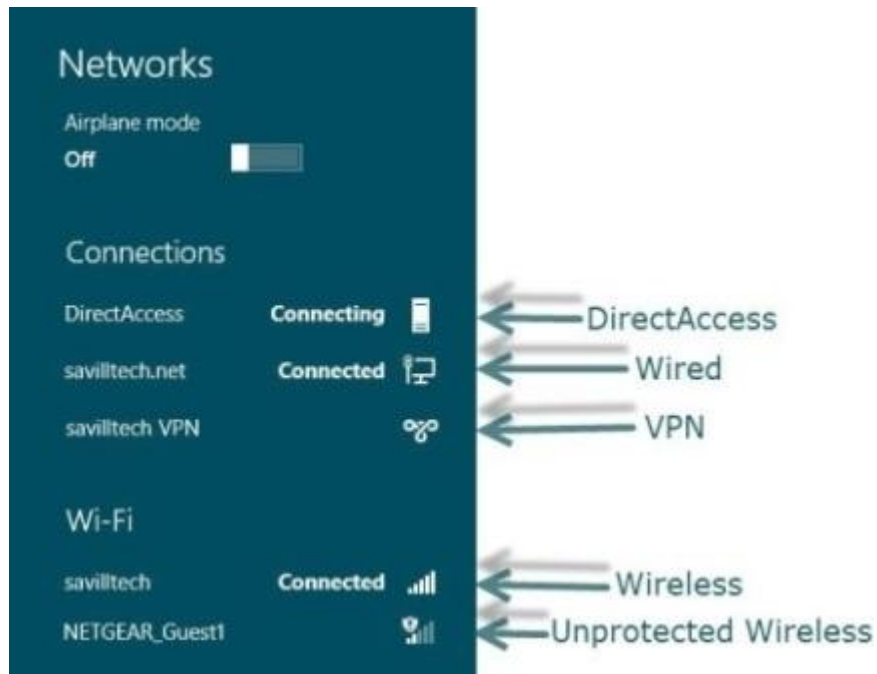
**Edit connection properties**

To edit a connection that you have already configured, right-click the connection, and then select **Connection Properties**.

To access **Connection Properties**, in the **Networks**, click **View Connection Properties**.



<https://technet.microsoft.com/en-us/library/jj613767.aspx>



#### QUESTION 145

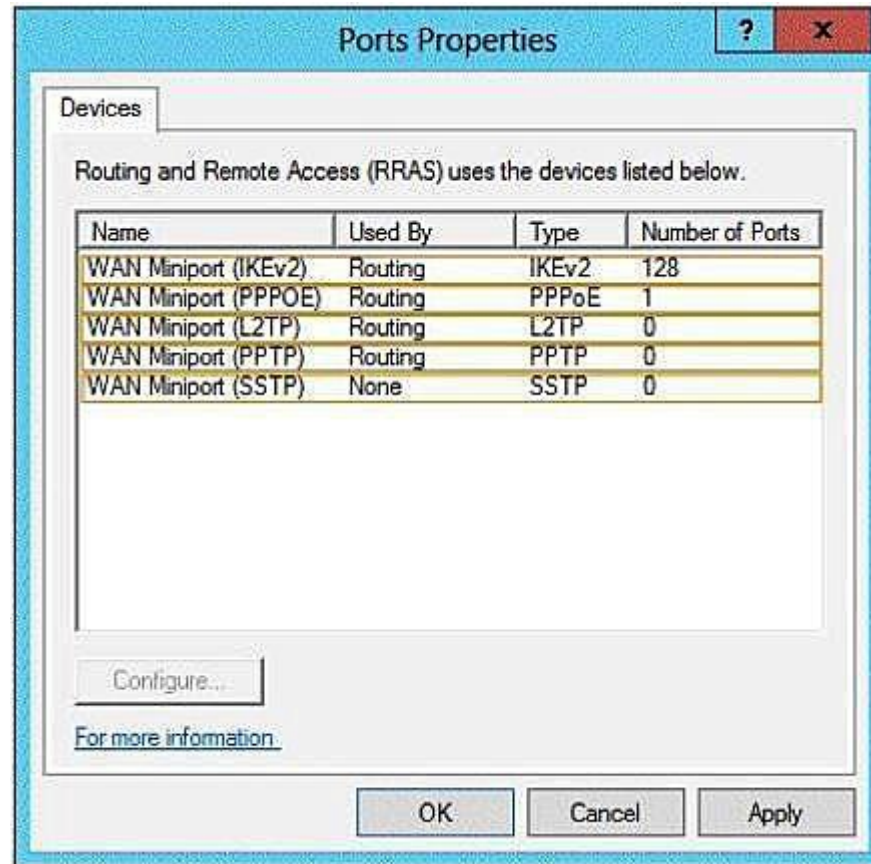
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Access server role installed.

You need to configure the ports on Server1 to ensure that client computers can establish VPN connections to Server1 by using TCP port 443.

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

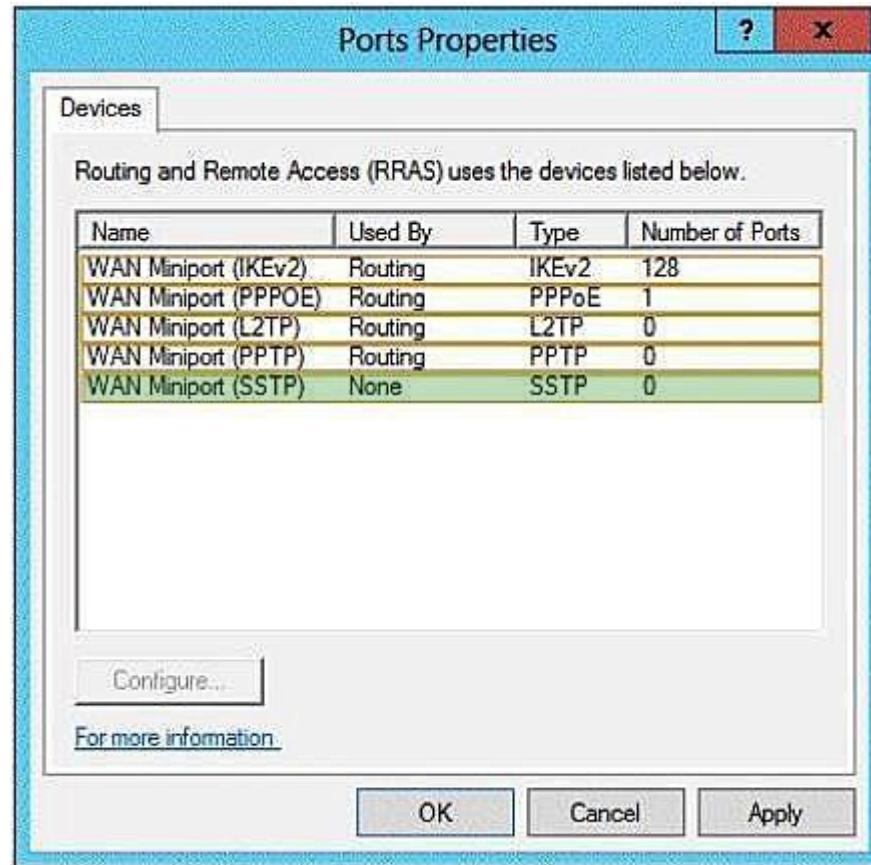
**Hot Area:**





Correct Answer:





### Section: Configure network services and access

#### Explanation

#### Explanation/Reference:

**Secure Socket Tunneling Protocol (SSTP)** is a new tunneling protocol that uses the HTTPS protocol over **TCP port 443** to pass traffic through firewalls and Web proxies that might block PPTP and L2TP/IPsec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the Secure Sockets Layer (SSL) channel of the HTTPS protocol. The use of PPP allows support for strong authentication methods, such as EAP-TLS. SSL provides transport-level security with enhanced key negotiation, encryption, and integrity checking.

When a client tries to establish a SSTP-based VPN connection, SSTP first establishes a bidirectional HTTPS layer with the SSTP server. Over this HTTPS layer, the protocol packets flow as the data payload.

<https://technet.microsoft.com/en-us/library/cc771298>

**QUESTION 146**

Your network contains an Active Directory domain named contoso.com. All DNS servers host a DNS zone named adatum.com. The adatum.com zone is not Active Directory-integrated.

An administrator modifies the start of authority (SOA) record for the adatum.com zone. After the modification, you discover that when you add or modify DNS records in the adatum.com zone, the changes are not transferred to the DNS servers that host secondary copies of the adatum.com zone. You need to ensure that the records are transferred to all the copies of the adatum.com zone.

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

**Hot Area:**

adatum.com Properties

Name Servers WINS Zone Transfers

General Start of Authority (SOA)

Serial number:  
251 Increment

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

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

Refresh interval: 15 minutes

Retry interval: 10 minutes

Expires after: 1 days

Minimum (default) TTL: 1 hours

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

OK Cancel Apply Help

Correct Answer:

adatum.com Properties

Name Servers	WINS	Zone Transfers
General	Start of Authority (SOA)	
Serial number: <input type="text" value="251"/> <input type="button" value="Increment"/>		
Primary server: <input type="text" value="server1.contoso.com."/> <input type="button" value="Browse..."/>		
Responsible person: <input type="text" value="hostmaster.contoso.com."/> <input type="button" value="Browse..."/>		
Refresh interval:	<input type="text" value="15"/>	minutes ▾
Retry interval:	<input type="text" value="10"/>	minutes ▾
Expires after:	<input type="text" value="1"/>	days ▾
Minimum (default) TTL:	<input type="text" value="1"/>	hours ▾
TTL for this record: <input type="text" value="0"/> : <input type="text" value="1"/> : <input type="text" value="0"/> : <input type="text" value="0"/> (DDDDD:HH.MM.SS)		
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Help"/>		

Section: Configure network services and access

Explanation

Explanation/Reference:

SOA resource record fields

Serial number

The revision number of the zone file. This number increases each time a resource record in the zone changes. It is important that this value increases each time the zone is changed, so that either partial zone changes or the fully revised zone can be replicated to other secondary servers during subsequent transfers.

<https://technet.microsoft.com/en-us/library/dd197495>

#### QUESTION 147

Your network contains an Active Directory domain named contoso.com. You implement DirectAccess.

You need to view the properties of the DirectAccess connection. Which connection properties should you view?

To answer, select the appropriate connection properties in the answer area.

**Hot Area:**



**Correct Answer:**



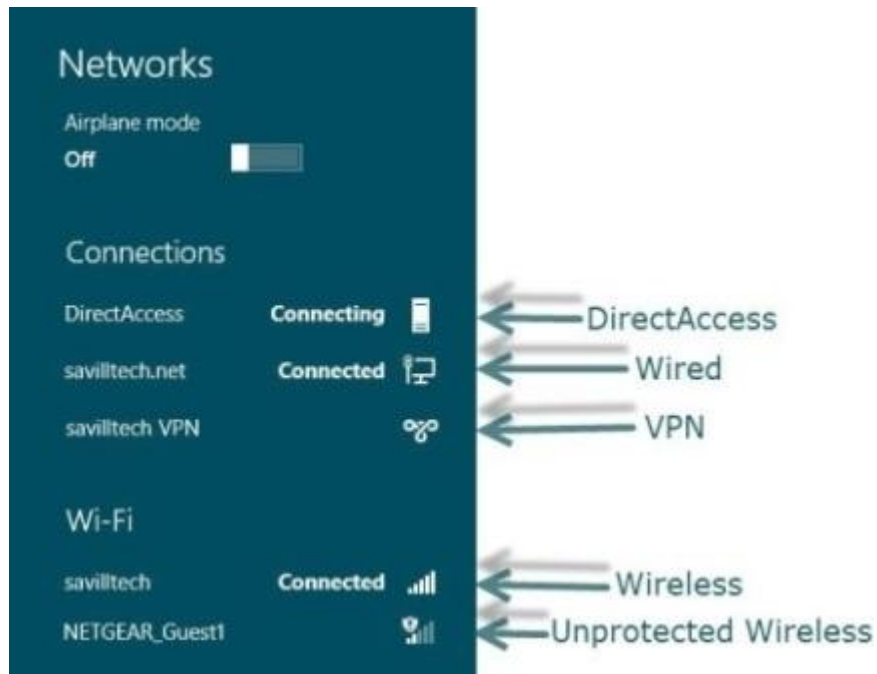
**Section: Configure network services and access**  
**Explanation**

**Explanation/Reference:**

Right-click the **DirectAccess** network entry from the list of available networks and select the **View connection properties** option.



<http://blogs.technet.com/b/jasonjones/archive/2013/11/13/the-evolution-of-collecting-directaccess-client-diagnostic-log-information.aspx>



#### QUESTION 148

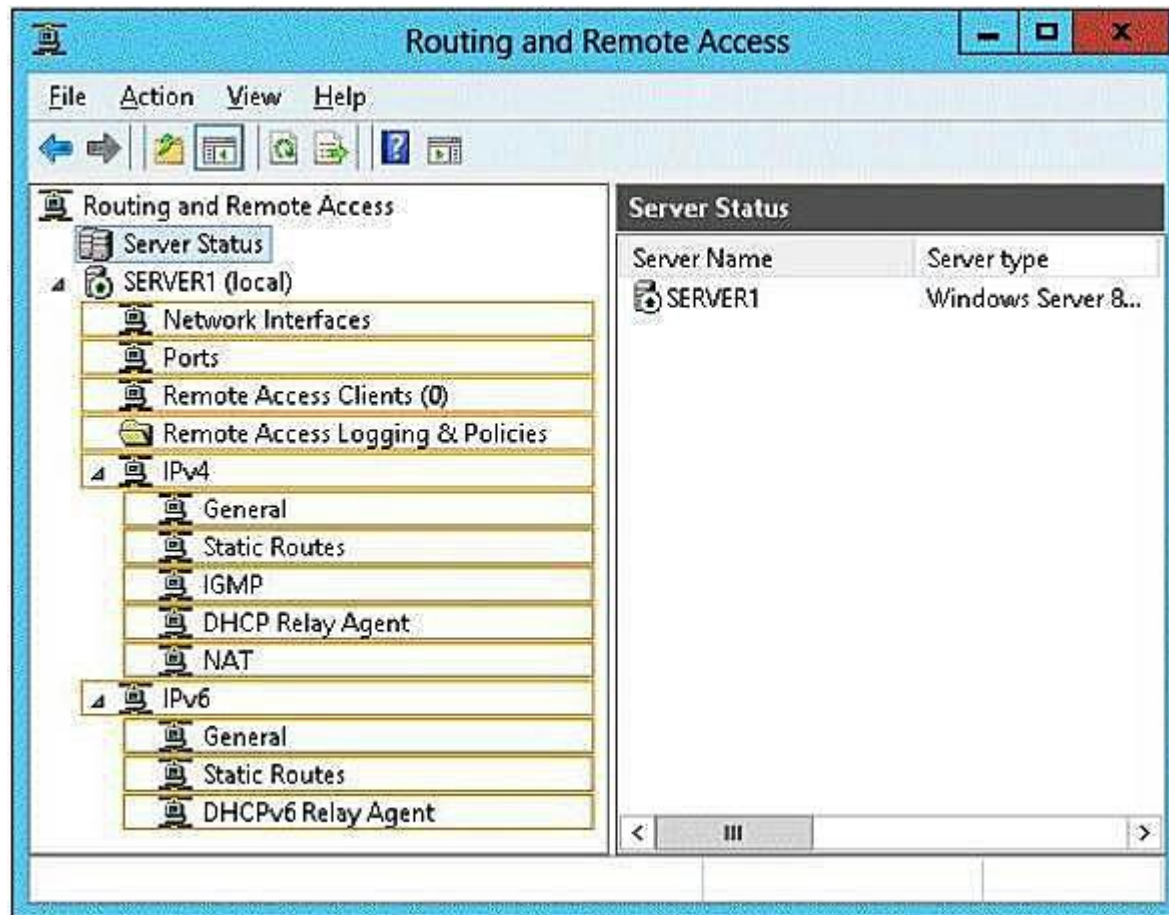
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has two network adapters and is located in a perimeter network.

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

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

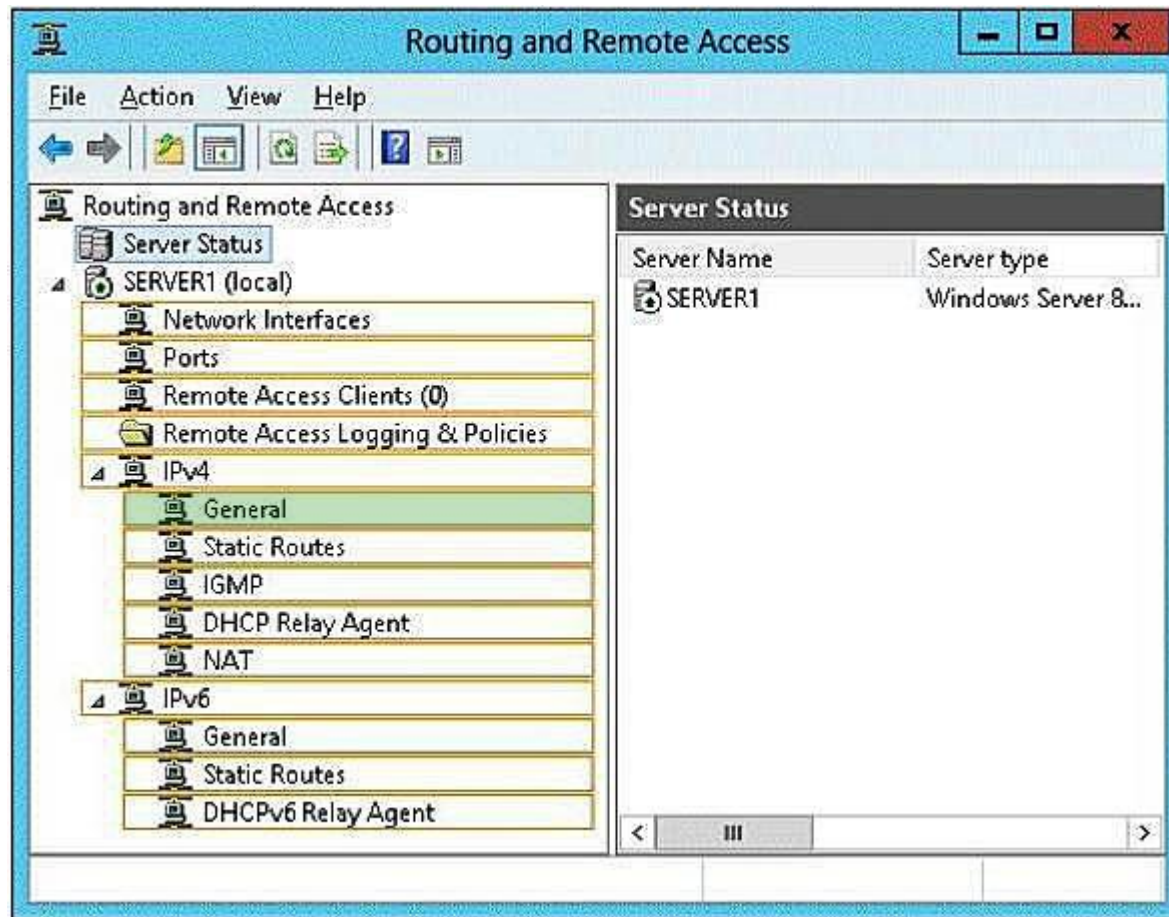
**Hot Area:**





Correct Answer:





**Section: Configure network services and access**

**Explanation**

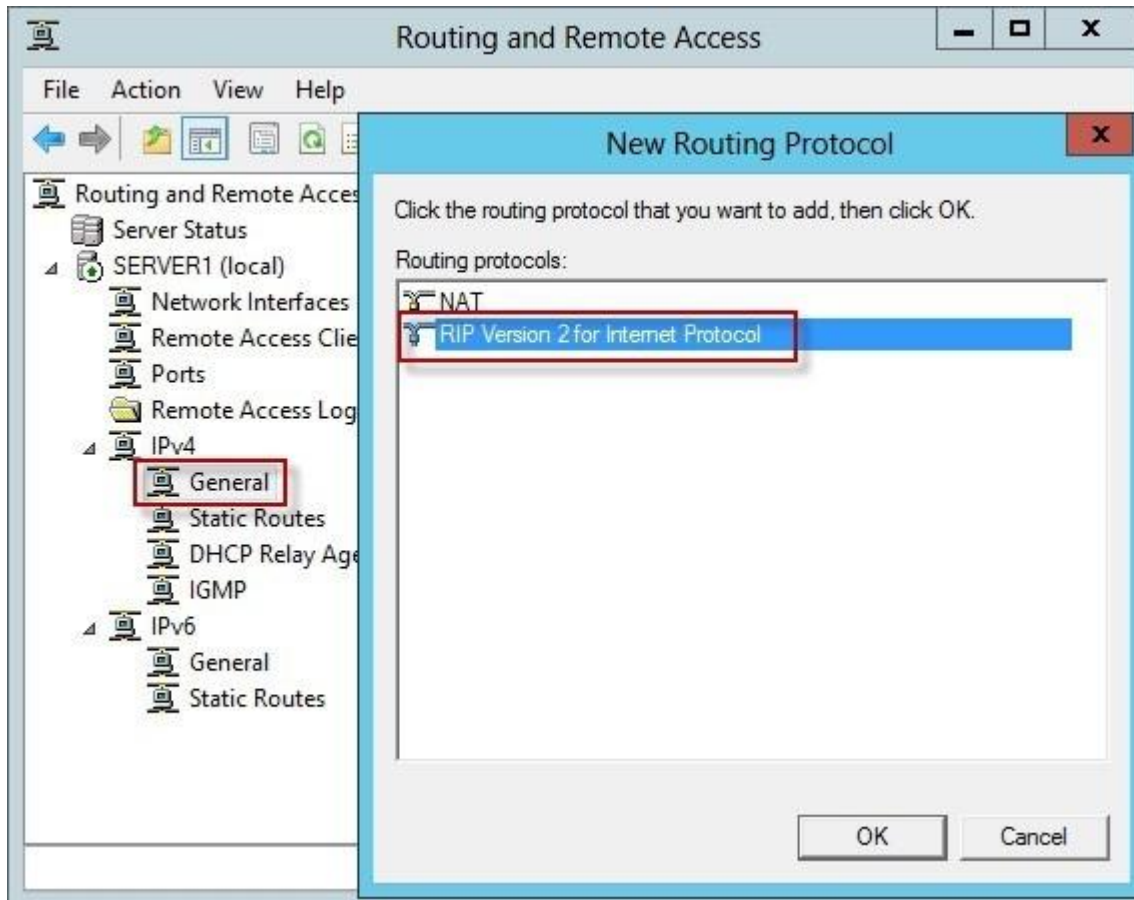
**Explanation/Reference:**

**Enable and Configure RIP**

Configure Routing Information Protocol (RIP) to enable the RRAS server to exchange routing information with other routers. By default, RIP is not enabled on an RRAS server.

**To enable and configure RIP**

1. In the RRAS MMC snap-in, expand **IPv4**, right-click **General**, and then click **New Routing Protocol**.



2. Select **RIP Version 2 for Internet Protocol**, and then click **OK**. **RIP** now appears in the navigation pane under **IPv4**.
3. Right-click **RIP**, and then click **New Interface**.
4. Select the interface connected to a subnet on which the remote router is connected, and then click **OK**.
5. RIP is configured with default settings. If these are satisfactory, click **OK** to save your changes.
6. If you want to customize logging or configure the list of routers with which this server can exchange information, right-click **RIP**, and then click

**Properties.**

<https://technet.microsoft.com/en-us/library/dd469737.aspx>

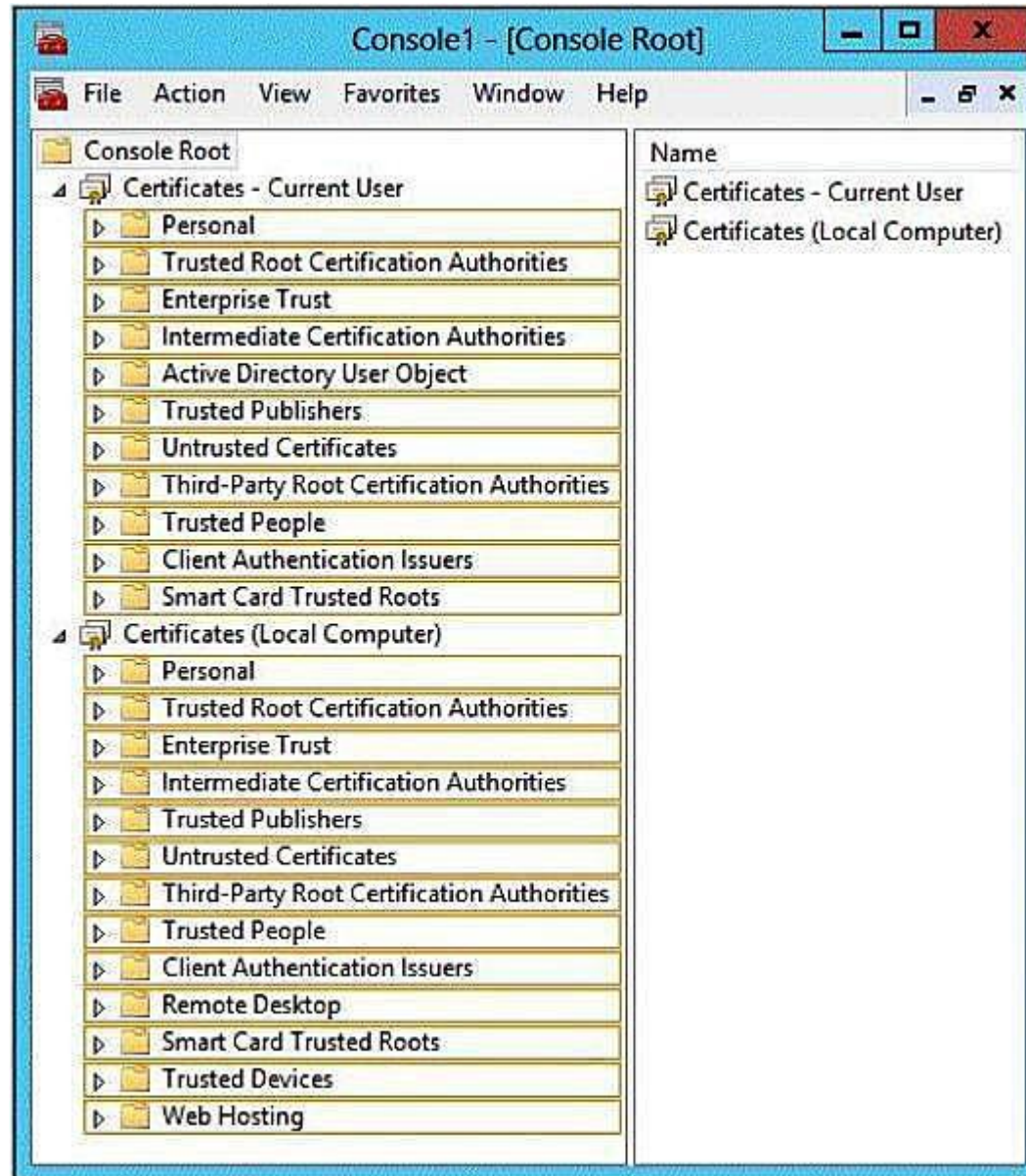
**QUESTION 149**

You have a server named Server1 that has the Web Server (IIS) server role installed.

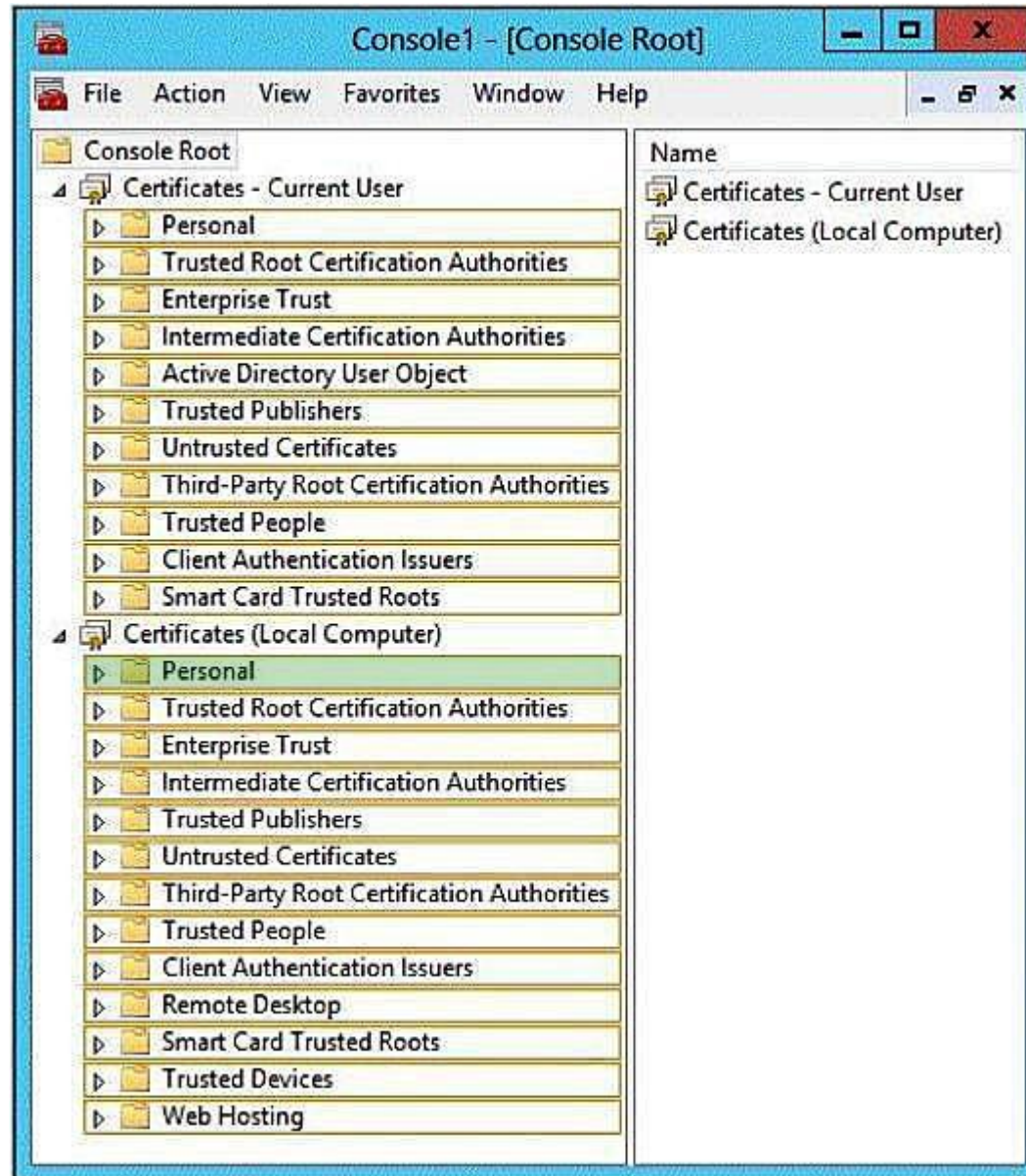
You obtain a Web Server certificate. You need to configure a website on Server1 to use Secure Sockets Layer (SSL).

To which store should you import the certificate? To answer, select the appropriate store in the answer area.

**Hot Area:**



Correct Answer:



**Section: Configure network services and access**

**Explanation**



## Explanation/Reference:

### Certificate store

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

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

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

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

<https://technet.microsoft.com/en-us/library/ee407543>

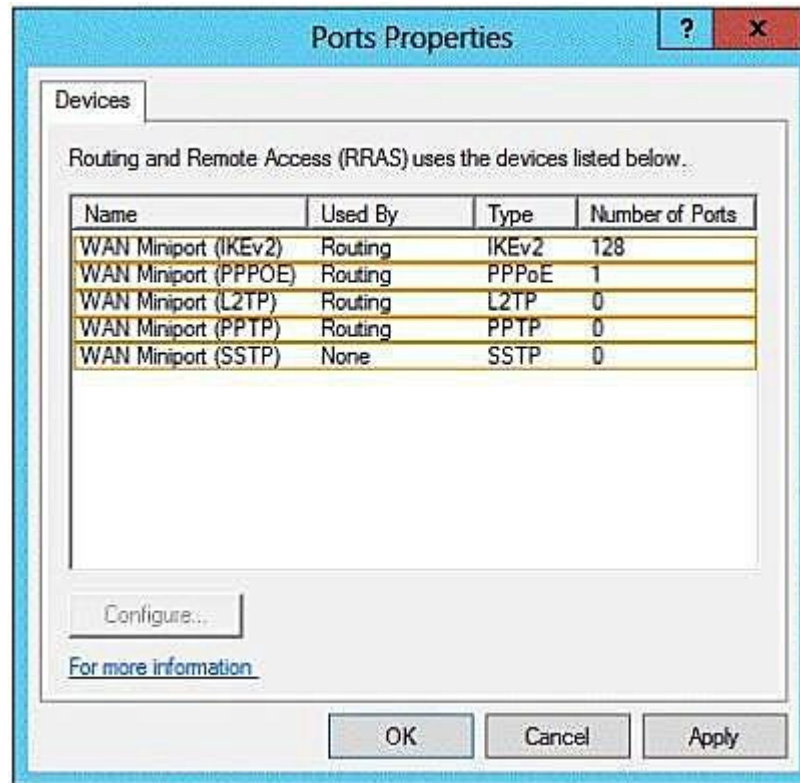
### QUESTION 150

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

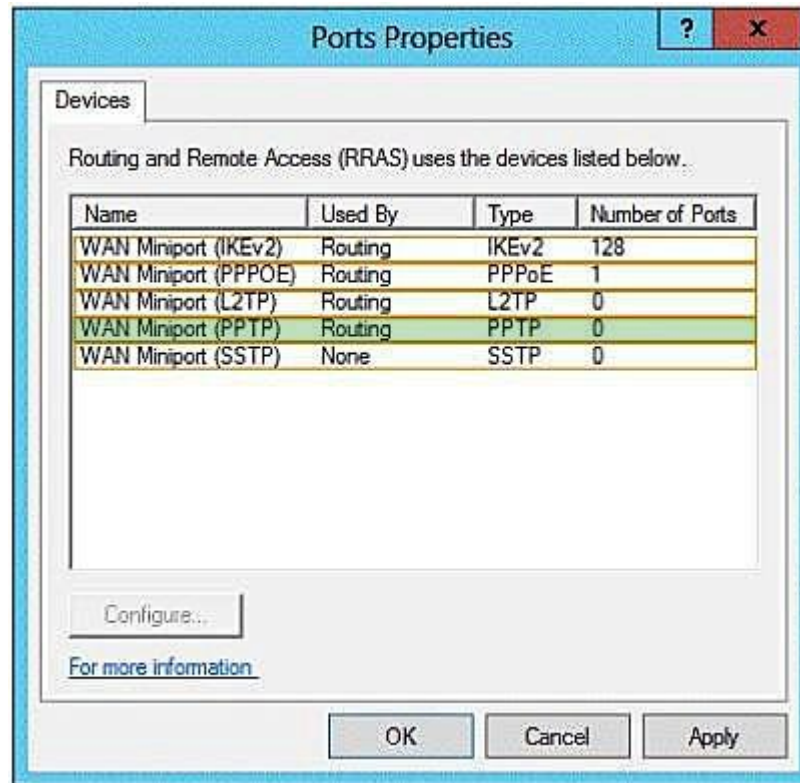
You need to configure the ports on Server1 to ensure that client computers can establish VPN connections to Server1. The solution must NOT require the use of certificates or pre-shared keys.

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

### Hot Area:



**Correct Answer:**



## Section: Configure network services and access

### Explanation

### Explanation/Reference:

When choosing between PPTP, L2TP/IPsec, SSTP, and IKEv2 remote access VPN solutions, consider the following:

PPTP can be used with a variety of Microsoft clients, including Microsoft Windows® 2000 and later versions of Windows. **Unlike L2TP/IPsec and IKEv2, PPTP does not require the use of a public key infrastructure (PKI).** By using encryption, PPTP-based VPN connections provide data confidentiality (captured packets cannot be interpreted without the encryption key). PPTP-based VPN connections, however, do not provide data integrity (proof that the data was not modified in transit) or data origin authentication (proof that the data was sent by the authorized user).

L2TP can be used with client computers running Windows 2000 and later versions of Windows. L2TP supports either computer certificates or a preshared key as the authentication method for IPsec. Computer certificate authentication, the recommended authentication method, requires a PKI to issue computer certificates to the VPN server computer and all VPN client computers. By using IPsec, L2TP/IPsec VPN connections provide data confidentiality, data integrity, and data authentication.



Unlike PPTP and SSTP, L2TP/IPsec enables machine authentication at the IPsec layer and user level authentication at the PPP layer.

SSTP can only be used with client computers running Windows Vista Service Pack 1 (SP1), Windows Server 2008, and later versions of Windows. By using SSL, SSTP VPN connections provide data confidentiality, data integrity, and data authentication.

IKEv2 is supported only on computers running Windows 7 and Windows Server 2008 R2. By using IPsec, IKEv2 VPN connections provide data confidentiality, data integrity, and data authentication. IKEv2 supports the latest IPsec encryption algorithms. Because of its support for mobility (MOBIKE), it is much more resilient to changing network connectivity, making it a good choice for mobile users who move between access points and even switch between wired and wireless connections.

<https://technet.microsoft.com/en-us/library/dd469817>

### **QUESTION 151**

Your network contains a DNS server named Server1 that runs Windows Server 2012 R2. Server1 has a zone named contoso.com. The network contains a server named Server2 that runs Windows Server 2008 R2. Server1 and Server2 are members of an Active Directory domain named contoso.com.

You change the IP address of Server2. Several hours later, some users report that they cannot connect to Server2. On the affected users' client computers, you flush the DNS client resolver cache, and the users successfully connect to Server2. You need to reduce the amount of time that the client computers cache DNS records from contoso.com.

Which value should you modify in the Start of Authority (SOA) record? To answer, select the appropriate setting in the answer area.

**Hot Area:**

contoso.com Properties

Name Servers WINS Zone Transfers

General Start of Authority (SOA)

Serial number:

234 Increment

Primary server:

server1.contoso.com. Browse...

Responsible person:

hostmaster.contoso.com. Browse...

Refresh interval: 1 days

Retry interval: 1 days

Expires after: 1 days

Minimum (default) TTL: 1 days

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

OK Cancel Apply Help

Correct Answer:

The screenshot shows the 'contoso.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The 'General' sub-tab is also active. The fields are as follows:

Field	Value	Action
Serial number:	234	Increment
Primary server:	server1.contoso.com.	Browse...
Responsible person:	hostmaster.contoso.com.	Browse...
Refresh interval:	1 days	
Retry interval:	1 days	
Expires after:	1 days	
Minimum (default) TTL:	1 days	
TTL for this record:	1 :00 :00	(DDDD:HH.MM.SS)

Buttons at the bottom: OK, Cancel, Apply, Help.

## Section: Configure network services and access

### Explanation

#### Explanation/Reference:

#### Time-to-Live for resource records

The Time-to-Live (TTL) value in a resource record indicates a length of time used by other DNS servers to determine how long to cache information for a record before expiring and discarding it. For example, most resource records created by the DNS Server service inherit the minimum (default) TTL of one hour from the start of authority (SOA) resource record, which prevents extended caching by other DNS servers.

A DNS client resolver caches the responses it receives when it resolves DNS queries. These cached responses can then be used to answer later queries for the same information. The cached data, however, has a limited lifetime specified in the TTL parameter returned with the response data. TTL ensures that the DNS server does not keep information for so long that it becomes out of date. TTL for the cache can be set on the DNS database (for each individual resource record, by specifying the TTL field of the record and per zone through the minimum TTL field of the SOA record) as well as on the DNS client resolver side by specifying the maximum TTL the resolver allows to cache the resource records.

There are two competing factors to consider when setting the TTL. The first is the accuracy of the cached information, and the second is the utilization of the DNS servers and the amount of network traffic. If the TTL is short, then the likelihood of having old information is reduced considerably, but it increases utilization of DNS servers and network traffic, because the DNS client must query DNS servers for the expired data the next time it is requested. If the TTL is long, the cached responses could become outdated, meaning the resolver could give false answers to queries. At the same time, a long TTL decreases utilization of DNS servers and reduces network traffic because the DNS client answers queries using its cached data.

If a query is answered with an entry from cache, the TTL of the entry is also passed with the response. This way the resolvers that receive the response know how long the entry is valid. The resolvers honor the TTL from the responding server; they do not reset it based on their own TTL. Consequently, entries truly expire rather than live in perpetuity as they move from DNS server to DNS server with an updated TTL.

<https://technet.microsoft.com/en-us/library/dd197427>

#### **QUESTION 152**

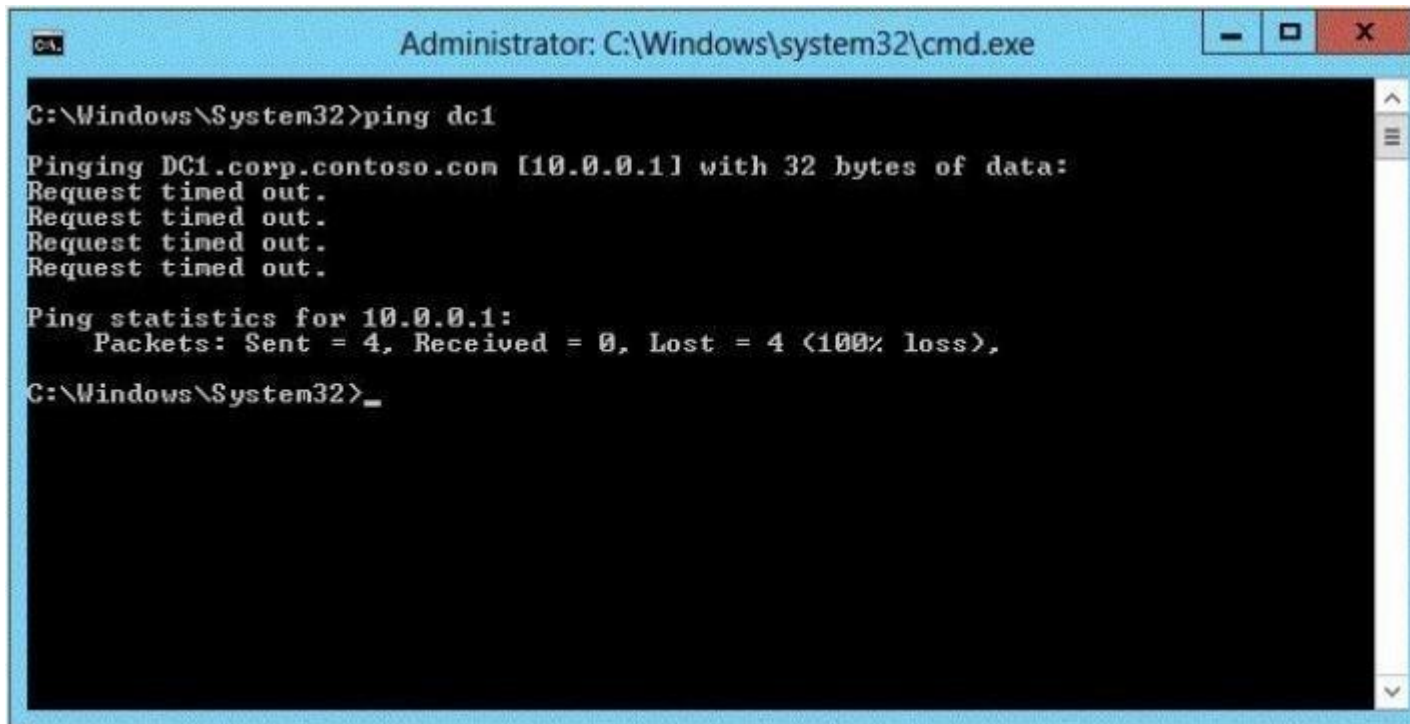
Your network contains an Active Directory domain named corp.contoso.com. The domain contains a domain controller named DC1.

When you run ping dcl.corp.contoso.com, you receive the result as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that DC1 can respond to the Ping command.

Which rule should you modify? To answer, select the appropriate rule in the answer area.

**Exhibit:**



```
Administrator: C:\Windows\system32\cmd.exe

C:\Windows\System32>ping dc1

Pinging DC1.corp.contoso.com [10.0.0.1] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

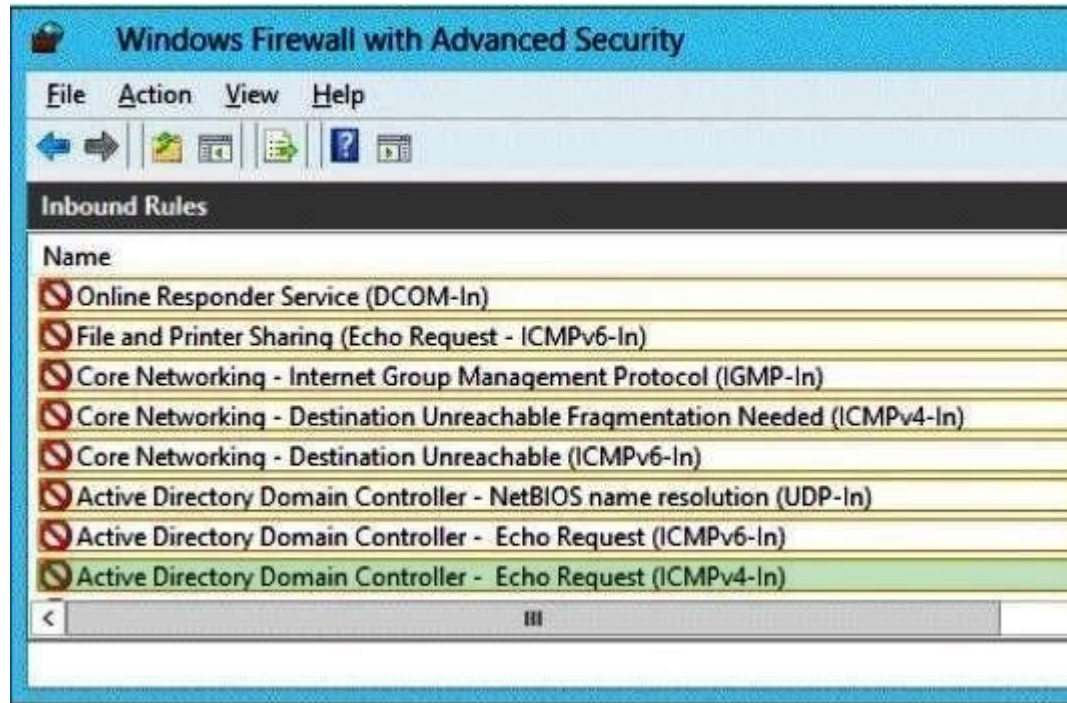
C:\Windows\System32>_
```

Hot Area:



Correct Answer:





### Section: Configure network services and access

#### Explanation

#### Explanation/Reference:

A common step in troubleshooting connectivity situations is to use the Ping tool to ping the IP address of the computer to which you are trying to connect. When you ping, you send an ICMP Echo message (also known as an ICMP Echo Request message) and get an ICMP Echo Reply message in response. By default, Windows Firewall does not allow incoming ICMP Echo messages, and therefore the computer cannot send an ICMP Echo Reply in response.

Enabling incoming ICMP Echo messages will allow others to ping your computer. However, it also leaves your computer vulnerable to the types of attacks that use ICMP Echo messages. Therefore, we recommended that you enable the Allow incoming echo request setting temporarily, and then disable it when it is no longer needed.

<https://technet.microsoft.com/en-us/library/cc749323>

#### QUESTION 153

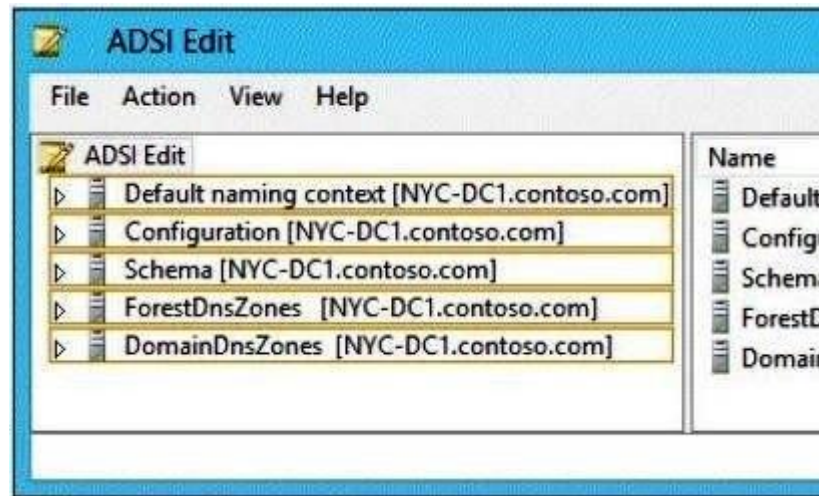
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. The contoso.com zone is Active Directory-

integrated and configured to replicate to all of the domain controllers in the contoso.com domain. Server1 has a DNS record in the contoso.com zone.

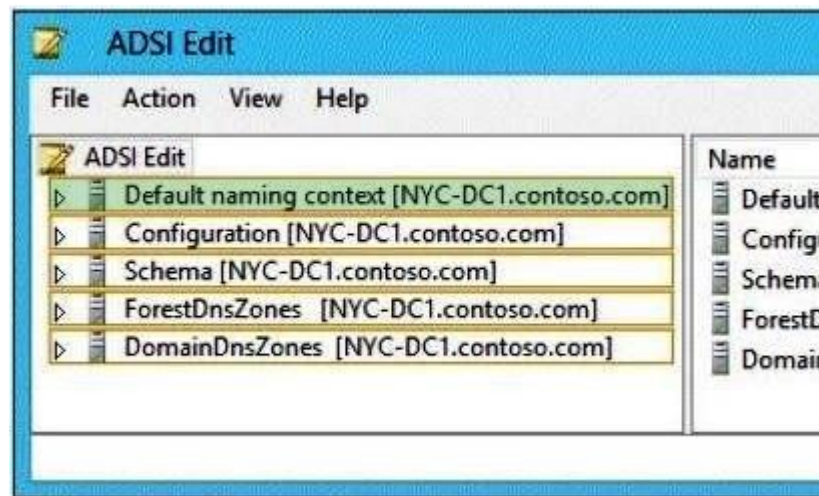
You need to verify when the DNS record for Server1 was last updated.

In which Active Directory partition should you view the DNS record of Server1? To answer, select the appropriate Active Directory partition in the answer area.

**Hot Area:**



**Correct Answer:**





## Section: Configure network services and access

### Explanation

#### Explanation/Reference:

The default naming context (directory partition) for a particular server is the distinguished name of the domain directory partition for which this domain controller is authoritative.

<https://technet.microsoft.com/en-us/library/cc772829>

You can use the ADSIEdit MMC console to carry out LDAP operations against any of the directory partitions. If you can enable ADSIEdit to communicate to the directory, LDAP is working. Also, any of the Active Directory snap-ins can help you determine if DNS, the IP layer, and the directory service are working and available.

<https://technet.microsoft.com/en-us/library/cc961921.aspx>

### QUESTION 154

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

You add a VPN server named Server2 to the network. On Server1, you create several network policies. You need to configure Server1 to accept authentication requests from Server2.

Which tool should you use on Server1?

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

**Correct Answer: C**

**Section: Configure a Network Policy Server (NPS) infrastructure**

### Explanation

#### Explanation/Reference:

The **New-NpsRadiusClient** cmdlet creates a Remote Authentication Dial-In User Service (RADIUS) client. A RADIUS client uses a RADIUS server to manage authentication, authorization, and accounting requests that the client sends. A RADIUS client can be an access server, such as a dial-up server or wireless access point, or a RADIUS proxy.

## Syntax

```
New-NpsRadiusClient [-Name] <String> [-Address] <String> [-AuthAttributeRequired <Boolean> ] [-Disabled] [-NapCompatible <Boolean> ] [-SharedSecret <String> ] [-VendorName <String> ] [ <CommonParameters>]
```



```
PS C:\Users\Administrator> New-NpsRadiusClient -Name "FromServer2" -Address "10.1.0.0/16" -AuthAttributeRequired 0 -NapCompatible 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
```

<https://technet.microsoft.com/en-us/library/jj872740>

## QUESTION 155

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

On Server1, you create a network policy named Policy1. You need to configure Policy1 to ensure that users are added to a VLAN.

Which attributes should you add to Policy1?

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

**Correct Answer: C**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

**To configure a network policy for VLANs**

1. On the NPS server, click **Start**, click **Administrative Tools**, and then click **Network Policy Server**. The NPS console opens.
2. Double-click **Policies**, click **Network Policies**, and then in the details pane double-click the policy that you want to configure.
3. In the policy **Properties** dialog box, click the **Settings** tab.

4. In policy **Properties**, in **Settings**, in **RADIUS Attributes**, ensure that **Standard** is selected.
5. In the details pane, in **Attributes**, the **Service-Type** attribute is configured with a default value of **Framed**. By default, for policies with access methods of VPN and dial-up, the **Framed-Protocol** attribute is configured with a value of **PPP**. To specify additional connection attributes required for VLANs, click **Add**. The **Add Standard RADIUS Attribute** dialog box opens.
6. In **Add Standard RADIUS Attribute**, in **Attributes**, scroll down to and add the following attributes:
  - a. **Tunnel-Medium-Type**. Select a value appropriate to the previous selections you have made for the policy. For example, if the network policy you are configuring is a wireless policy, select **Value: 802 (Includes all 802 media plus Ethernet canonical format)**.
  - b. **Tunnel-Pvt-Group-ID**. Enter the integer that represents the VLAN number to which group members will be assigned.
  - c. **Tunnel-Type**. Select **Virtual LANs (VLAN)**.
7. In **Add Standard RADIUS Attribute**, click **Close**.
8. If your network access server (NAS) requires use of the **Tunnel-Tag** attribute, use the following steps to add the **Tunnel-Tag** attribute to the network policy. If your NAS documentation does not mention this attribute, do not add it to the policy. Add the attributes as follows:
  - a. In policy **Properties**, in **Settings**, in **RADIUS Attributes**, click **Vendor Specific**.
  - b. In the details pane, click **Add**. The **Add Vendor Specific Attribute** dialog box opens.
  - c. In **Attributes**, scroll down to and select **Tunnel-Tag**, and then click **Add**. The **Attribute Information** dialog box opens.
  - d. In **Attribute value**, type the value that you obtained from your hardware documentation.

<https://technet.microsoft.com/en-us/library/cc772124>

#### QUESTION 156

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

On Server1, you create a network policy named Policy1. You need to configure Policy1 to apply only to VPN connections that use the L2TP protocol.

What should you configure in Policy1?

- A. The Tunnel Type
- B. The Service Type
- C. The NAS Port Type
- D. The Framed Protocol

**Correct Answer:** A

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

**Tunnel Type**

Restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP. The Tunnel Type attribute is typically used when you deploy virtual local area networks (VLANs).

<https://technet.microsoft.com/en-us/library/cc731220>

**QUESTION 157**

Your company has offices in five locations around the country. Most of the users' activity is local to their own network. Occasionally, some of the users in one location need to send confidential information to one of the other four locations or to retrieve information from one of them. The communication between the remote locations is sporadic and relatively infrequent, so you have configured RRAS to use demand-dial lines to set up the connections.

Management's only requirement is that any communication between the office locations be appropriately secured.

Which of the following steps should you take to ensure compliance with this requirement? (Each correct answer presents part of the solution. Choose two.)

- A. Configure CHAP on all the RRAS servers.
- B. Configure PAP on all the RRAS servers.
- C. Configure MPPE on all the RRAS servers.
- D. Configure L2TP on all the RRAS servers.
- E. Configure MS-CHAPv2 on all the RRAS servers.

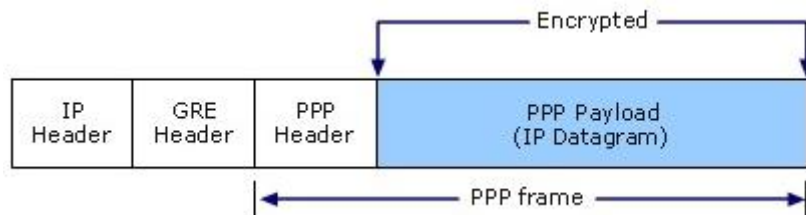
**Correct Answer:** CE

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

**Structure of a PPTP packet containing an IP datagram**



The PPP frame is encrypted with **Microsoft Point-to-Point Encryption (MPPE)** by using encryption keys generated from the **Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)** or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication process. Virtual private networking clients must use the MS-CHAP v2 or EAP-TLS authentication protocols in order for the payloads of PPP frames to be encrypted. PPTP is taking advantage of the underlying PPP encryption and encapsulating a previously encrypted PPP frame.

<https://technet.microsoft.com/en-us/library/dd469817>

#### QUESTION 158

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: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

*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.

<https://technet.microsoft.com/en-us/library/cc754107.aspx>

### QUESTION 159

You are a network administrator of an Active Directory domain named contoso.com. You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the DHCP Server server role and the Network Policy Server role service installed.

You enable Network Access Protection (NAP) on all of the DHCP scopes on Server1. You need to create a DHCP policy that will apply to all of the NAP non-compliant DHCP clients.

Which criteria should you specify when you create the DHCP policy?

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

**Correct Answer: B**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

**To configure a NAP-enabled DHCP server**

1. On the DHCP server, click **Start**, click **Run**, in **Open**, type **dhcpcmgmt.smc**, and then press ENTER.
2. In the DHCP console, open **<servername>\IPv4**.
3. Right-click the name of the DHCP scope that you will use for NAP client computers, and then click **Properties**.
4. On the **Network Access Protection** tab, under **Network Access Protection Settings**, choose **Enable for this scope**, verify that **Use default Network Access Protection profile** is selected, and then click **OK**.
5. In the DHCP console tree, under the DHCP scope that you have selected, right-click **Scope Options**, and then click **Configure Options**.
6. On the **Advanced** tab, verify that **Default User Class** is selected next to **User class**.
7. Select the **003 Router** check box, and in **IP Address**, under **Data entry**, type the IP address for the default gateway used by compliant NAP client computers, and then click **Add**.
8. Select the **006 DNS Servers** check box, and in **IP Address**, under **Data entry**, type the IP address for each router to be used by compliant NAP client computers, and then click **Add**.
9. Select the **015 DNS Domain Name** check box, and in **String value**, under **Data entry**, type your organization's domain name (for example,

**woodgrovebank.local**), and then click **Apply**. This domain is a full-access network assigned to compliant NAP clients.

10. On the **Advanced** tab, next to **User class**, choose **Default Network Access Protection Class**.

11. Select the **003 Router** check box, and in **IP Address**, under **Data entry**, type the IP address for the default gateway used by noncompliant NAP client computers, and then click **Add**. This can be the same default gateway that is used by compliant NAP clients.

**Note:** The default gateway will not be used by noncompliant NAP client computers unless it is required to create static host routes to the DHCP server or to remediation servers.

12. Select the **006 DNS Servers** check box, and in **IP Address**, under **Data entry**, type the IP address for each DNS server to be used by noncompliant NAP client computers, and then click **Add**. These can be the same DNS servers used by compliant NAP clients.

13. Select the **015 DNS Domain Name** check box, and in **String value**, under **Data entry**, type a name to identify the restricted domain (for example, **restricted.woodgrovebank.local**), and then click **OK**. This domain is a restricted-access network assigned to noncompliant NAP clients.

14. Click **OK** to close the **Scope Options** dialog box.

15. Close the DHCP console.

[https://msdn.microsoft.com/en-us/library/dd296905\(v=ws.10\).aspx](https://msdn.microsoft.com/en-us/library/dd296905(v=ws.10).aspx)

#### QUESTION 160

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

An administrator creates a RADIUS client template named Template1. You create a RADIUS client named Client1 by using Template1. You need to modify the shared secret for Client1.

What should you do first?

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

**Correct Answer: D**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

You can use Network Policy Server (NPS) templates to create configuration elements, such as Remote Authentication Dial-In User Service (RADIUS) clients or shared secrets, that you can reuse on the local NPS server and export for use on other NPS servers. Templates Management provides a node in the NPS console where you can create, modify, delete, duplicate, and view the use of NPS templates. NPS templates are designed to reduce the amount of time and cost that it takes to configure NPS on one or more servers.

The screenshot shows the 'New RADIUS Client' dialog box. The 'Settings' tab is active. The 'Enable this RADIUS client' checkbox is checked. The 'Select an existing template:' checkbox is unchecked, and the dropdown menu shows 'Template 1'. The 'Name and Address' section has 'Friendly name:' set to 'Client 1' and 'Address (IP or DNS):' set to '192.168.1.1'. The 'Shared Secret' section has 'Select an existing Shared Secrets template:' set to 'None'. Below this, there is a note: '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.' At the bottom, 'Manual' is selected, and there are fields for 'Shared secret:' and 'Confirm shared secret:' both masked with asterisks. 'OK' and 'Cancel' buttons are at the bottom right.

[https://technet.microsoft.com/en-us/library/ee663945\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee663945(v=ws.10).aspx)

#### QUESTION 161

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The domain contains a server named Server1 that has the Network Policy Server server role and the Remote Access server role installed. The domain contains a server named Server2 that is configured as a RADIUS server. Server1 provides VPN access to external users.



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

What should you run?

- A. Add-RemoteAccessRadius -ServerName Server1 -AccountingOnOffMsg Enabled -SharedSecret "Secret" -Purpose Accounting
- B. Set-RemoteAccessAccounting -AccountingOnOffMsg Enabled -AccountingOnOffMsg Enabled
- C. Add-RemoteAccessRadius -ServerName Server2 -AccountingOnOffMsg Enabled -SharedSecret "Secret" -Purpose Accounting
- D. Set-RemoteAccessAccounting -EnableAccountingType Inbox -AccountingOnOffMsg Enabled

**Correct Answer: C**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

The **Add-RemoteAccessRadius** cmdlet adds a new external RADIUS server for one of the following purposes:

- Accounting Radius configuration applies to both DirectAccess (DA) and VPN.
- One-time password (OTP) RADIUS configuration applies only to DA.
- Authentication Radius configuration applies only to VPN.

Radius server configuration for Accounting and OTP are global in nature, such as the configurations apply to the entire Remote Access deployment. RADIUS server configuration for VPN applies only to a specific VPN server, and all servers in a load balancing cluster, or if multi-site is deployed, to all VPN servers at a site.

Following describes aspects of this cmdlet behavior.

- If a RADIUS server is currently being used for a specific purpose, then it can be added for additional purpose using this cmdlet.
- The RADIUS server properties for authentication and accounting are the same except for the **AccountingOnOffMsg** parameter which is applicable only to accounting RADIUS and the **MsgAuthenticator** parameter which is applicable only to authentication RADIUS. These properties are not relevant for DA OTP authentication.
- If a user tries to add a RADIUS server for a particular purpose but specifies a parameter that is not applicable to that purpose, then this cmdlet will still run but the parameter will be ignored and a warning message will be issued. When adding a RADIUS server for OTP authentication both the above described parameters are ignored if specified.
- If the accounting configuration is Windows Server® 2012 accounting, then a user can switch to external RADIUS accounting by adding an external RADIUS server for the purpose of accounting.
- Following are some pre-requisites for adding a RADIUS server.
  - A RADIUS server cannot be added for authentication when VPN is not even installed.
  - A RADIUS server cannot be added for authentication when the authentication type is Windows or when local NPS is installed.
  - A RADIUS server cannot be added for the purpose of accounting when external RADIUS accounting is not enabled.
  - A RADIUS server cannot be added for purpose of OTP authentication if OTP authentication is not enabled.

Parameters:

**-ServerName<String>**

Specifies the IPv4 or IPv6 address, or host name, of the external RADIUS server.

<https://technet.microsoft.com/en-us/library/hh918425.aspx>

#### **QUESTION 162**

Your network contains four Network Policy Server (NPS) servers named Server1, Server2, Server3, and Server4. Server1 is configured as a RADIUS proxy that forwards connection requests to a remote RADIUS server group named Group1.

You need to ensure that Server2 and Server3 receive connection requests. Server4 must only receive connection requests if both Server2 and Server3 are unavailable.

How should you configure Group1?

- A. Change the Weight of Server4 to 10.
- B. Change the Weight of Server2 and Server3 to 10.
- C. Change the Priority of Server2 and Server3 to 10.
- D. Change the Priority of Server4 to 10.

**Correct Answer: D**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

#### **RADIUS server priority and weight**

During the NPS proxy configuration process, you can create remote RADIUS server groups and then add RADIUS servers to each group. To configure load balancing, you must have more than one RADIUS server per remote RADIUS server group. While adding group members, or after creating a RADIUS server as a group member, you can access the **Add RADIUS server** dialog box to configure the following items on the **Load Balancing** tab:

**Edit RADIUS Server**

Address | Authentication/Accounting | **Load Balancing**

The priority of ranking indicates the status of a server. A primary server has a priority of 1.

Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority.

Priority:  Weight:

Advanced settings

Number of seconds without response before request is considered dropped:

Maximum number of dropped requests before server is identified as unavailable:

Number of seconds between requests when server is identified as unavailable:

OK Cancel Apply

- **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.
- **Weight.** NPS uses this Weight setting to determine how many connection requests to send to each group member when the group members have the same priority level. Weight setting must be assigned a value between 1 and 100, and the value represents a percentage of 100 percent. For example, if the remote RADIUS server group contains two members that both have a priority level of 1 and a weight rating of 50, the NPS proxy forwards 50 percent of the connection requests to each RADIUS server.

<https://technet.microsoft.com/en-us/library/dd197433>

## Remote RADIUS Server Group Commands

### priority

Optional. Specifies whether the server is a primary or backup server. Primary servers are specified as one. The default value is one (primary). The value must be between one and 65535.

[https://technet.microsoft.com/de-de/library/cc731910\(v=ws.10\).aspx](https://technet.microsoft.com/de-de/library/cc731910(v=ws.10).aspx)

### QUESTION 163

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

Server1 has the following role services installed:

- DirectAccess and VPN (RRAS)
- Network Policy Server

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

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

What should you configure on Server1?

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

**Correct Answer: A**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

### Network policy conditions

Every network policy must have at least one configured condition. NPS provides many conditions groups that allow you to clearly define the properties that the connection request received by NPS must have in order to match the policy.

The available condition groups are:

- Groups
- HCAP

- Day and time restrictions
- Network Access Protection
- Connection properties
- RADIUS client properties
- Gateway

Following are the Network Access Protection (NAP) conditions that you can configure in network policy.

- MS-Service Class
- Health Policies
- NAP-Capable Computers
- Operating System
  - Specifies the operating system (operating system version or service pack number), role (client or server), and architecture (x86, x64, or ia64) required for the computer configuration to match the policy.
- Policy Expiration

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

#### QUESTION 164

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:** DE

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

Configuring a template is different than configuring the NPS server directly. Creating a template does not affect the NPS server's functionality. It is only when you select the template in the appropriate location in the NPS console that the template affects the NPS server functionality. For example, if you configure a RADIUS client in the NPS console under **RADIUS Clients and Servers**, you alter the NPS server configuration and take one step in configuring NPS to communicate with one of your network access servers. (The next step is to configure the network access server (NAS) to

communicate with NPS.) However, if you configure a new RADIUS Clients template in the NPS console under **Templates Management**, rather than creating a new RADIUS client under **RADIUS Clients and Servers**, you have created a template, but you have not altered the NPS server functionality yet. To alter the NPS server functionality, you must select the template from the correct location in the NPS console.

<https://technet.microsoft.com/en-us/library/ee663945>

In a multisite deployment two or more Remote Access servers or server clusters are deployed and configured as different entry points in a single location, or in dispersed geographical locations. Deploying multiple entry points in a single location allows for server redundancy, or for the alignment of Remote Access servers with existing network architecture. Deployment by geographical location ensures efficient use of resources, as remote client computers can connect to internal network resources using an entry point closest to them. Traffic across a multisite deployment can be distributed and balanced with an external global load balancer.

A multisite deployment supports client computers running Windows 8 or Windows 7. Client computers running Windows 8 automatically identify an entry point, or the user can manually select an entry point. Automatic assignment occurs in the following priority order:

1. Use an entry point selected manually by the user.
2. Use an entry point identified by an external global load balancer if one is deployed.
3. Use the closest entry point identified by the client computer using an automatic probe mechanism.

Support for clients running Windows 7 must be manually enabled on each entry point, and selection of an entry point by these clients is not supported.

<https://technet.microsoft.com/library/hh831664.aspx>

#### **QUESTION 165**

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?

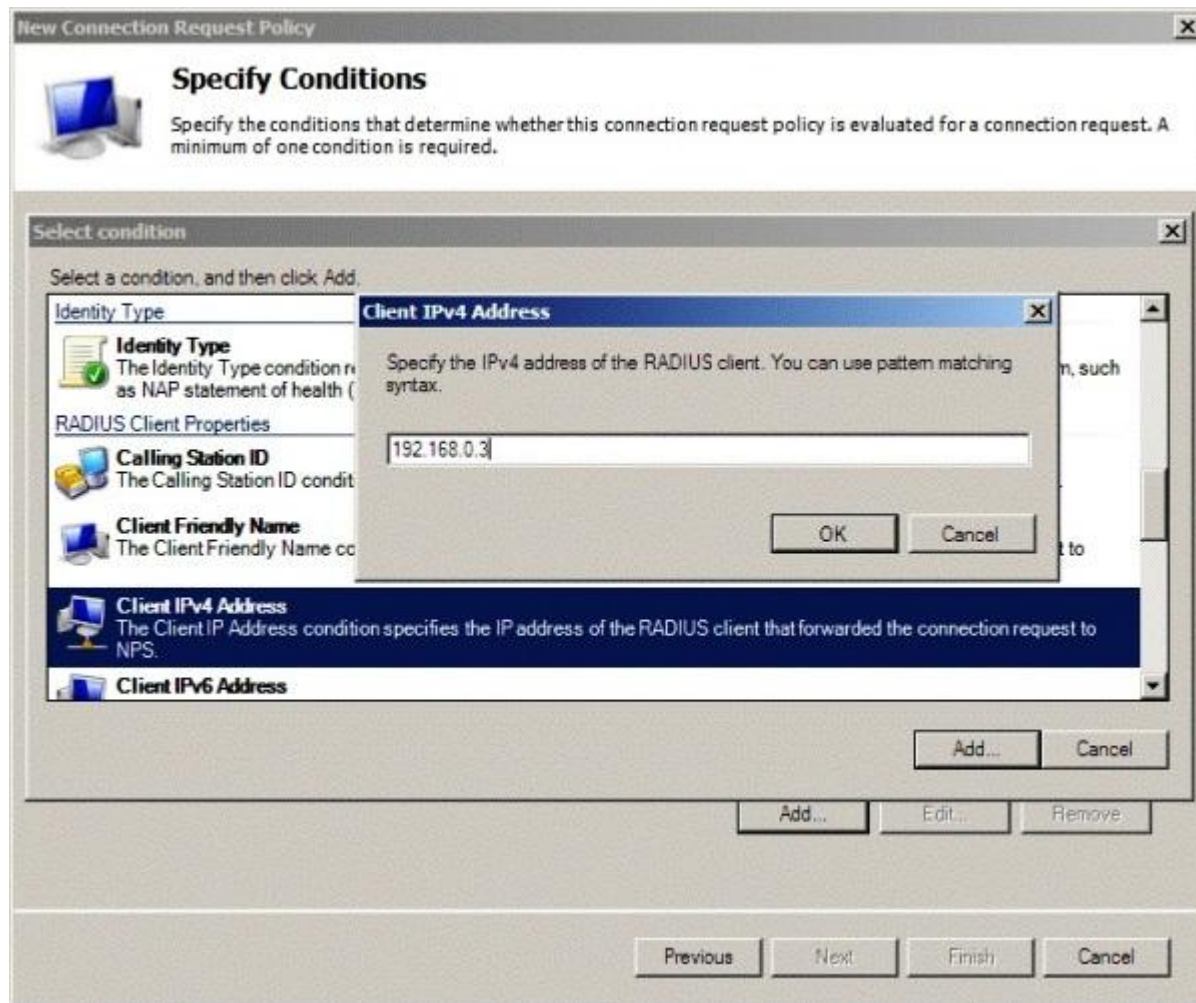
- A. Set the Client IP4 Address condition to 192.168.0.0/24.
- B. Set the Client IP4 Address condition to 192.168.0.
- C. Set the Called Station ID constraint to 192.168.0.0/24.
- D. Set the Called Station ID constraint to 192.168.0.

**Correct Answer: B**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

## Explanation/Reference:



<https://technet.microsoft.com/en-us/library/dd182017.aspx>

## Examples of using pattern-matching syntax to specify network policy attributes

To specify a range of all IP addresses that begin with 192.168.0, the syntax is:

192\ .168\ .0\ . . +

<https://technet.microsoft.com/en-us/library/dd197583>

### Network Prefix Length Representation of Subnet Masks

Because the network ID bits must always be chosen in a contiguous fashion from the high order bits, a shorthand way of expressing a subnet mask is to denote the number of bits that define the network ID as a network prefix using the network prefix notation: /<# of bits>. The following table lists the default subnet masks using the network prefix notation for the subnet mask.

Address Class	Bits for Subnet Mask	Network Prefix
Class A	11111111 00000000 00000000 00000000	/8
Class B	11111111 11111111 00000000 00000000	/16
Class C	11111111 11111111 11111111 00000000	/24

For example, the class C network ID 192.168.0.0 with the subnet mask of 255.255.255.0 would be expressed in network prefix notation as 192.168.0.0/24.

Network prefix notation is also known as **Classless Interdomain Routing (CIDR) notation**.

Because all hosts on the same network must use the same network ID, all hosts on the same network must use the same network ID as defined by the same subnet mask. For example, 192.168.0.0/16 is not the same network ID as 192.168.0.0/24. The network ID 192.168.0.0/16 implies a range of valid host IP addresses from 192.168.0.1 to 192.168.255.254. **The network ID 192.168.0.0/24 implies a range of valid host IP addresses from 192.168.0.1 to 192.168.0.254.** Clearly, these network IDs do not represent the same range of IP addresses.

<https://technet.microsoft.com/en-us/library/cc958832.aspx>

### QUESTION 166

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Network Policy 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-CHAP v2
- C. EAP-TLS
- D. MS-CHAP v2

**Correct Answer: B**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

The following table lists the different types of access and the available EAP methods you can use.

Type of Network Access	Available EAP Methods
Dial-up remote access or site-to-site connections	EAP-MD5 CHAP, EAP-TLS
Virtual private network remote access or site-to-site connections	EAP-MD5 CHAP, EAP-TLS
802.1X authentication to an authenticating switch (wired)	EAP-MD5 CHAP, PEAP-MS-CHAP v2, EAP-TLS, PEAP-TLS
802.1X authentication to a wireless AP	PEAP-MS-CHAP v2, EAP-TLS, PEAP-TLS

<https://technet.microsoft.com/en-us/library/bb457039.aspx>

**PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS** because user authentication is performed by using password-based credentials (user name and password), instead of certificates or smart cards. Only NPS or other RADIUS servers are required to have a certificate. The NPS server certificate is used by the NPS server during the authentication process to prove its identity to PEAP clients.

Server certificates are required when you deploy the PEAP-MS-CHAP v2 certificate-based authentication method.

Successful mutual PEAP-MS-CHAP v2 authentication has two main parts:

1. The client authenticates the NPS server.
2. The NPS server authenticates the user.

Additionally, as part of the PEAP-MS-CHAP v2 mutual authentication, the client validates the credentials of the RADIUS server.

<https://technet.microsoft.com/en-us/library/jj721726.aspx>

#### **QUESTION 167**

Your network contains an Active Directory domain named contoso.com. The domain contains client computers that run either Windows XP or Windows 8. Network Policy Server (NPS) is deployed to the domain.

You plan to create a system health validator (SHV). You need to identify which policy settings CANNOT be applied to the Windows XP computers.

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

- A. Antispyware is up to date.
- B. Automatic updating is enabled.
- C. Antivirus is up to date.
- D. A firewall is enabled for all network connections.
- E. An antispyware application is on.

**Correct Answer:** AE

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

You can only choose **An antispyware application is on** if the client computer is running Windows Vista® or Windows® 7. The WSHA on NAP client computers running Windows XP SP3 does not monitor the status of antispyware applications.





<https://technet.microsoft.com/en-us/library/cc731260.aspx>

#### QUESTION 168

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: Configure a Network Policy Server (NPS) infrastructure**  
**Explanation**

**Explanation/Reference:**

**Logman** creates and manages Event Trace Session and Performance logs and supports many functions of Performance Monitor from the command line.

Syntax:

```
logman [create | query | start | stop | delete | update | import | export | /?] [options]
```

<https://technet.microsoft.com/en-us/library/cc753820.aspx>

**QUESTION 169**

Your network contains three Network Policy Server (NPS) servers named NPS1, NPS2, and NPS3. NPS1 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: Configure a Network Policy Server (NPS) infrastructure**  
**Explanation**

**Explanation/Reference:**

**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.

<https://technet.microsoft.com/en-us/library/dd197433>

**QUESTION 170**

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

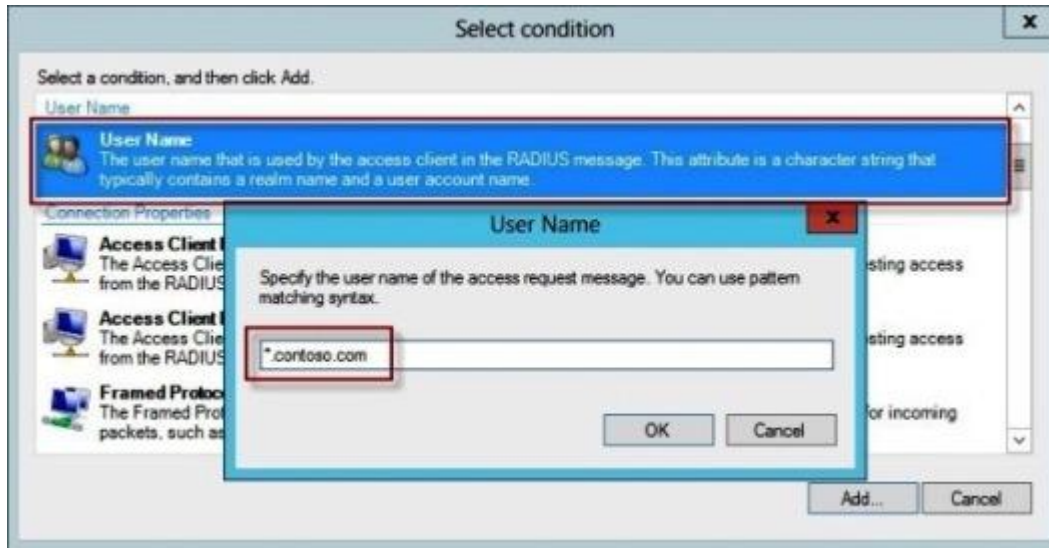
**Correct Answer:** AE

**Section:** Configure a Network Policy Server (NPS) infrastructure

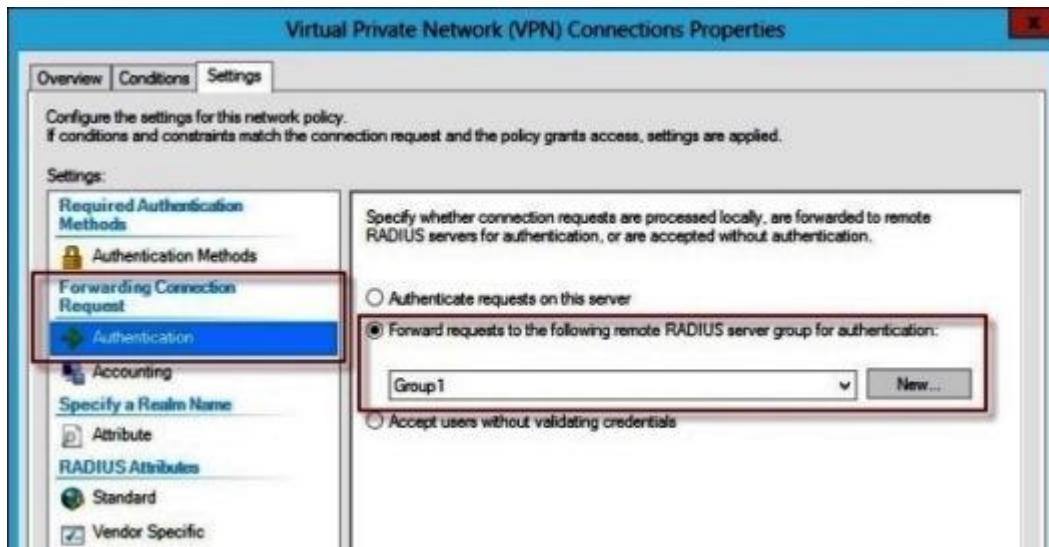
**Explanation**

**Explanation/Reference:**

By using the **User Name** 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 the **Authentication** 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.



<https://technet.microsoft.com/en-us/library/cc753603.aspx>

**QUESTION 171**

Your network contains two Active Directory forests named contoso.com and adatum.com. The contoso.com forest contains a server named Server1.contoso.com. The adatum.com forest contains a server named server2.adatum.com. Both servers have the Network Policy Server role service installed.

The network contains a server named Server3. Server3 is located in the perimeter network and has the Network Policy Server role service installed. You plan to configure Server3 as an authentication provider for several VPN servers. You need to ensure that RADIUS requests received by Server3 for a specific VPN server are always forwarded to Server1.contoso.com.

Which two should you configure on Server3? (Each correct answer presents part of the solution. Choose two.)

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

**Correct Answer:** BC

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

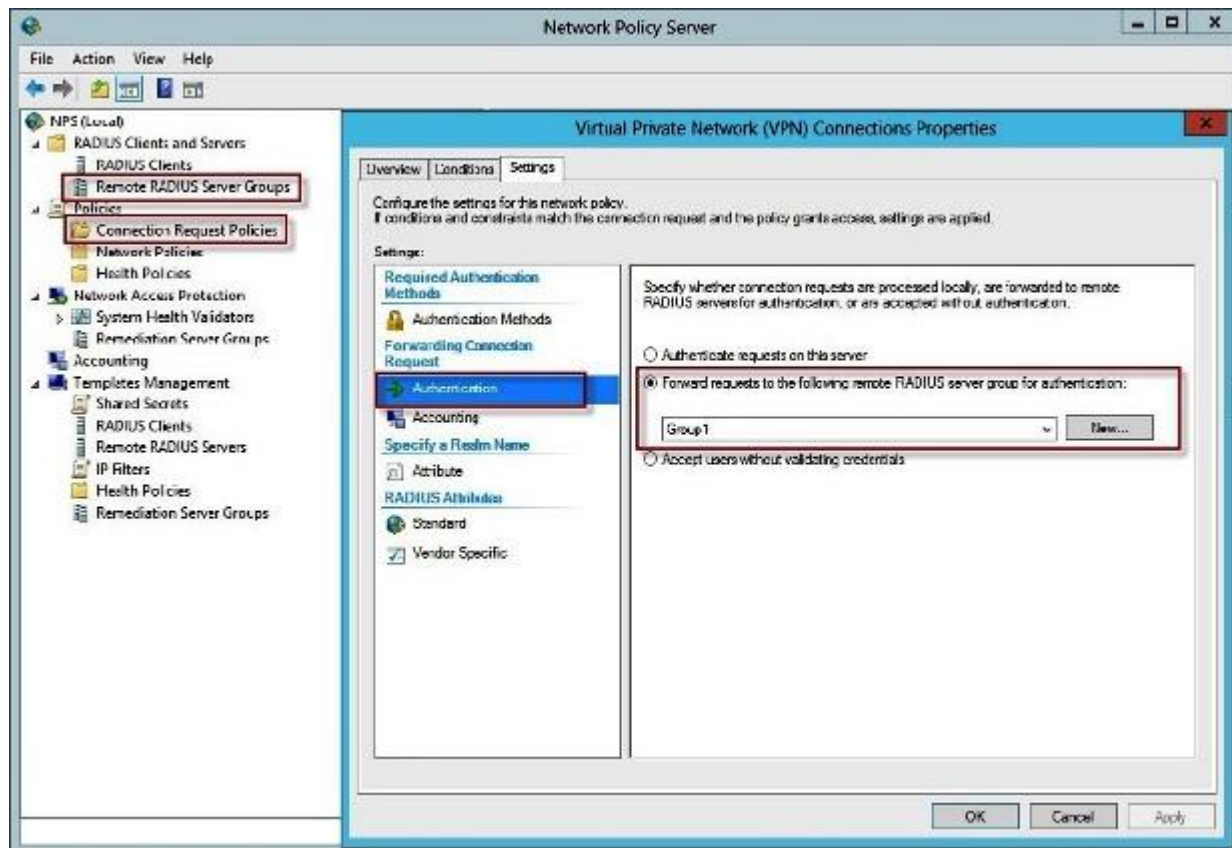
**Explanation/Reference:**

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

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

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





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

### QUESTION 172

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:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

The following table lists the different types of access and the available EAP methods you can use.

Type of Network Access	Available EAP Methods
Dial-up remote access or site-to-site connections	EAP-MD5 CHAP, EAP-TLS
Virtual private network remote access or site-to-site connections	EAP-MD5 CHAP, EAP-TLS
802.1X authentication to an authenticating switch (wired)	EAP-MD5 CHAP, PEAP-MS-CHAP v2, EAP-TLS, PEAP-TLS
802.1X authentication to a wireless AP	PEAP-MS-CHAP v2, EAP-TLS, PEAP-TLS

<https://technet.microsoft.com/en-us/library/bb457039.aspx>

#### QUESTION 173

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:** A

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

The following table lists the different types of access and the available EAP methods you can use.

Type of Network Access	Available EAP Methods
Dial-up remote access or site-to-site connections	EAP-MD5 CHAP, EAP-TLS
Virtual private network remote access or site-to-site connections	EAP-MD5 CHAP, EAP-TLS
802.1X authentication to an authenticating switch (wired)	EAP-MD5 CHAP, PEAP-MS-CHAP v2, EAP-TLS, PEAP-TLS
802.1X authentication to a wireless AP	PEAP-MS-CHAP v2, EAP-TLS, PEAP-TLS

<https://technet.microsoft.com/en-us/library/bb457039.aspx>

#### QUESTION 174

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: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

The 802.1X and VPN enforcement methods have the following AD DS requirements:

The NAP health policy server requires a computer certificate to perform PEAP-based user or computer authentication. After this certificate is acquired, a connection to AD CS is not required for as long as the certificate is valid.

<https://technet.microsoft.com/en-us/library/dd125301>

### **QUESTION 175**

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: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

### **NPS trace logging files**

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.

#### **To create tracing log files on a server running NPS**

1. Open a command line as an administrator.
2. Type **netsh ras set tr \* en**.
3. Reproduce the scenario that you are troubleshooting.
4. Type **netsh ras set tr \* dis**.
5. Close the command prompt window.

<https://technet.microsoft.com/en-us/library/dd348461>

#### **QUESTION 176**

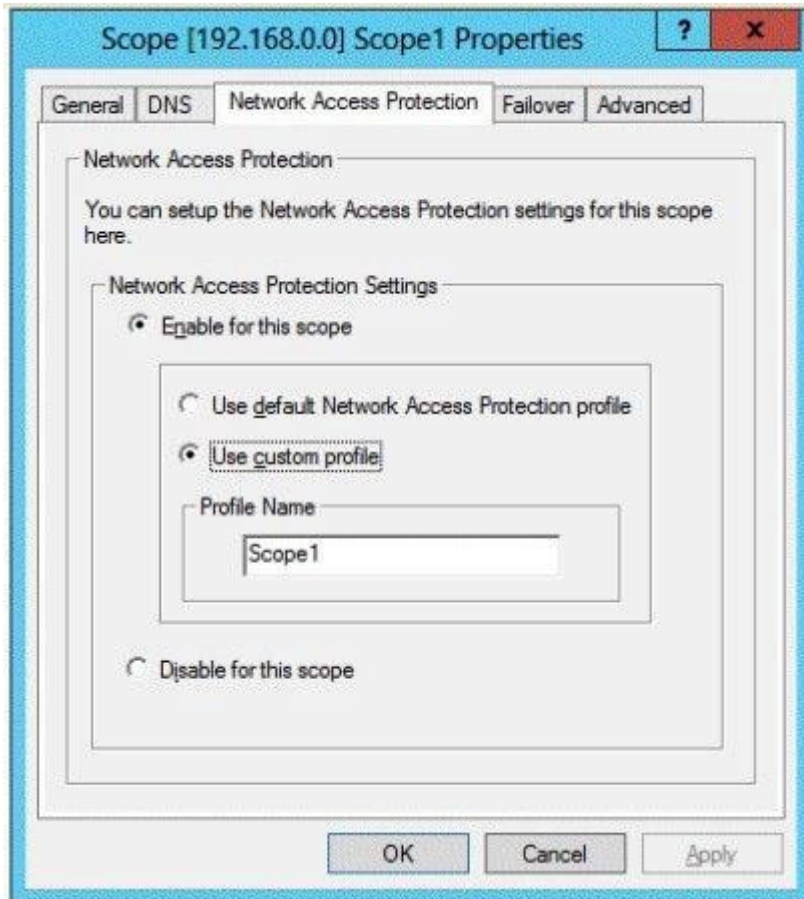
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 has the DHCP Server server role and the Network Policy Server role service installed. Server1 contains three non-overlapping scopes named Scope1, Scope2, and Scope3. Server1 currently 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?

**Exhibit:**



- 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

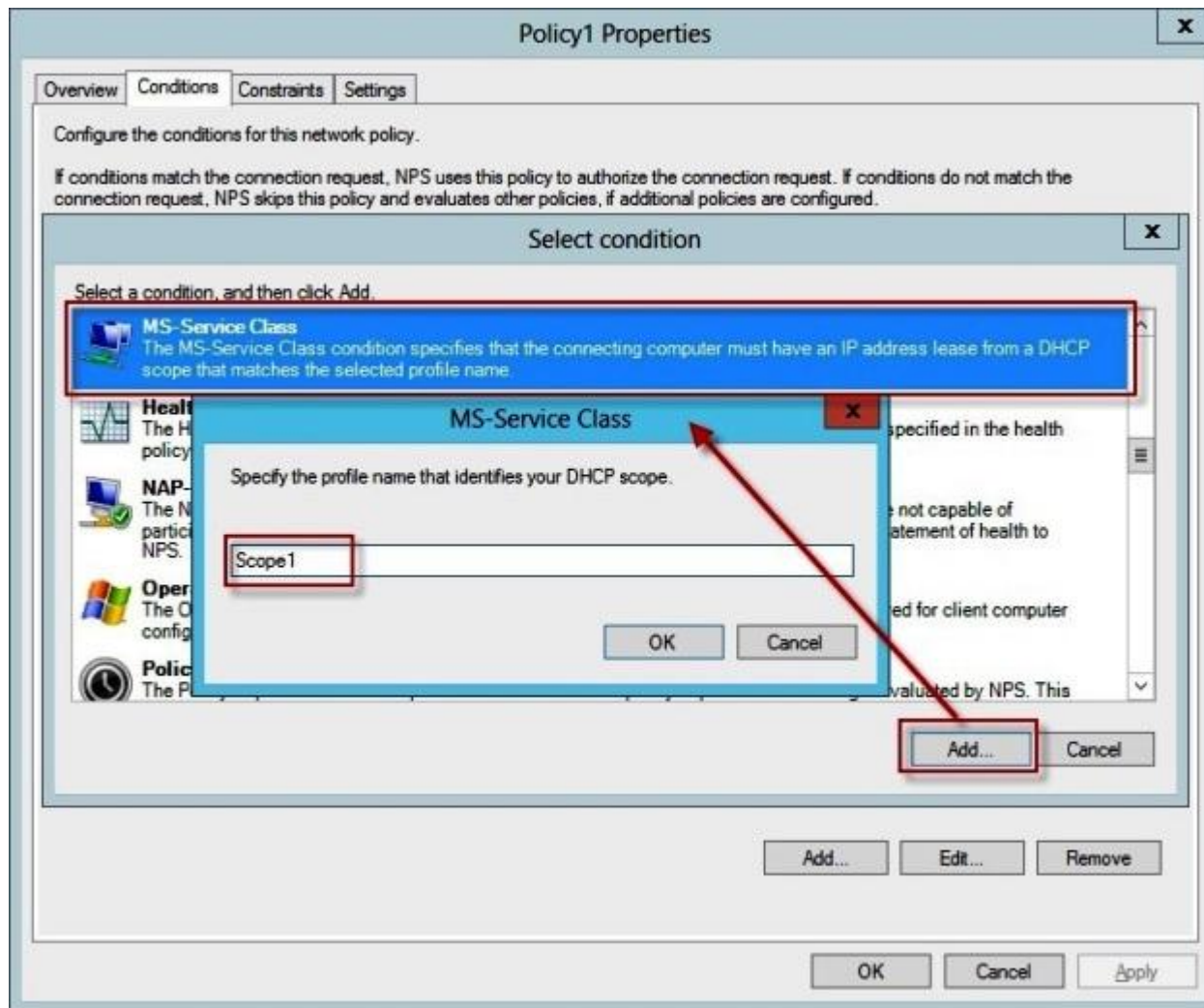
**Correct Answer:** D

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

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. 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.



<https://technet.microsoft.com/en-us/library/cc731220>

## QUESTION 177

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

You configure NPS on Server1 to log accounting data to a database on SQL1. You need to ensure that the accounting data is captured if SQL1 fails. The solution must minimize cost.

What should you do?

- A. Implement Failover Clustering.
- B. Implement database mirroring.
- C. Run the Accounting Configuration Wizard.
- D. Modify the SQL Server Logging properties.

**Correct Answer: C**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

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

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

<https://technet.microsoft.com/en-us/library/ee663943>

## QUESTION 178

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:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

To configure NAP conditions in network policy using the Windows interface

1. Open the NPS console, double-click **Policies**, click **Network Policies**, and then double-click the policy you want to configure.
2. In policy **Properties**, click the **Conditions** tab, and then click **Add**. In **Select condition**, scroll to the **Network Access Protection** group of conditions.
3. 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.

4. 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.

5. If you want to configure the Health Policies condition, click **Health Policies**, and then click **Add**. In **Health Policies**, choose an existing health policy, and then click **OK**. If you have not yet configured health policies, click **New**, and then configure a new health policy.

The Health Policies condition restricts the policy to clients that meet the health criteria in the policy that you specify.

6. If you want to configure the NAP-capable Computers condition, click **NAP-capable Computers**, and then click **Add**. In **Specify the computers**

**required to match this policy**, click either **Only computers that are NAP-capable** or **Only computers that are not NAP-capable**, and then click **OK**.

The NAP-capable Computers condition restricts the policy to either clients that are capable of participating in NAP or clients that are not capable of participating in NAP. This capability is determined by whether the client sends a statement of health (SoH) to NPS.

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

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

8. If you want to configure the Policy Expiration condition, click **Policy Expiration**, and then click **Add**. In **Policy Expiration**, configure the date and time when you want the network policy to expire, and then click **OK**.

The Policy Expiration condition specifies when the network policy expires; after the expiration date and time that you specify, the network policy is no longer evaluated by NPS.

<https://technet.microsoft.com/en-us/library/cc731560>

#### **QUESTION 179**

You deploy two servers named Server1 and Server2. You install Network Policy Server (NPS) on both servers. On Server1, you configure the following NPS settings:

- RADIUS Clients
- Network Policies
- Connection Request Policies
- SQL Server Logging Properties

You export the NPS configurations to a file and import the file to Server2. You need to ensure that the NPS configurations on Server2 are the same as the NPS configurations on Server1.

Which settings should you manually configure on Server2?

- A. SQL Server Logging Properties
- B. Connection Request Policies
- C. RADIUS Clients
- D. Network Policies

**Correct Answer: A**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

If SQL Server logging is configured on the source NPS server, SQL Server logging settings are not exported to the XML file. After you import the file on another NPS server, you must manually configure SQL Server logging.

<https://technet.microsoft.com/en-us/library/cc732059>

**QUESTION 180**

You are the network administrator for your organization. Your company uses a Windows Server 2012 R2 Enterprise Certification Authority to issue certificates.

You need to start using key archival.

What should you do?

- A. Implement a distribution CRL.
- B. Install the smart card key retrieval.
- C. Implement a Group Policy object (GPO) that enables the Online Certificate Status Protocol (OCSP) responder.
- D. Archive the private key on the server.

**Correct Answer: D**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:****Enterprise PKI with Windows Server 2012 R2 Active Directory Certificate Services**

The following six steps form the core process of implementing PKI. The common practices are to first build a root CA with a standalone server, followed by configuring a subordinate CA on a member server for issuing certificates, while securing the root CA by taking it offline and bringing it back online only when issuing a subordinate CA certificate.

1. Build a standalone root CA
2. Create an enterprise subordinate CA
3. Deploy certificate templates
4. Enable certificate auto-enrollment
5. Set certificate revocation policies
6. Configure and verify private key archive and recovery

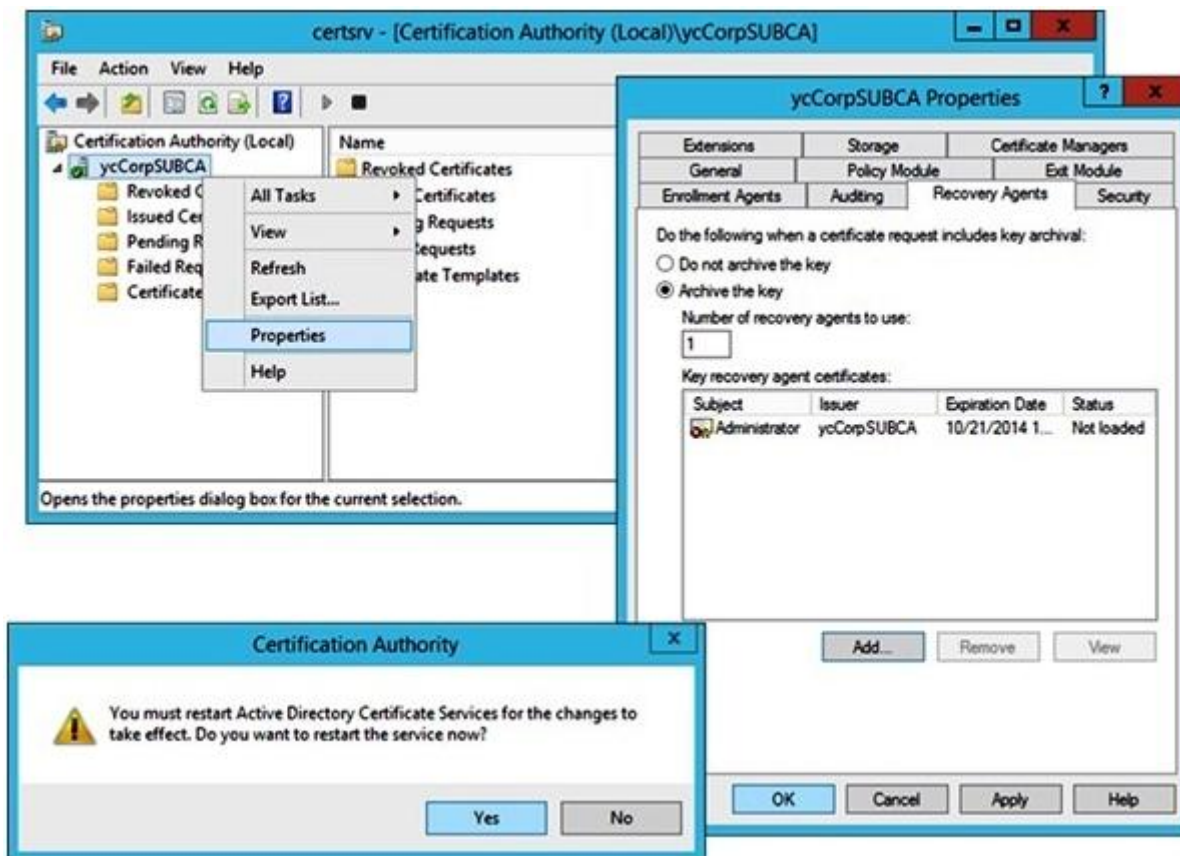
<http://blogs.technet.com/b/yungchou/archive/2013/10/21/enterprise-pki-with-windows-server-2012-r2-active-directory-certificate-services-part-1-of->

## 2.aspx

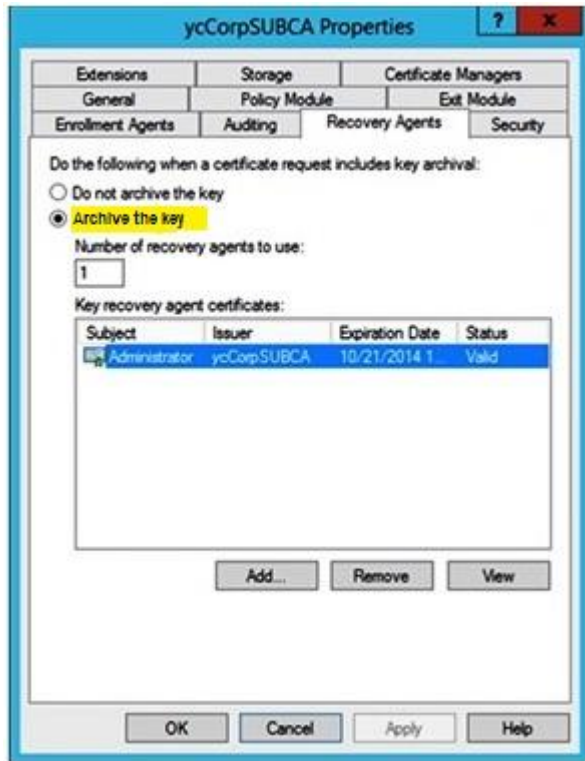
Recovering a private key is a process that needs to be well tested and documented accordingly. The process includes assigning a certificate for a recover agent, i.e. a certificate administrator, and enable specific certificate template to allow archiving a private key. These are the main tasks:

- (a) Configure CA to issue Key Recovery Agent (KRA) certificate
- (b) Request KRA certificate
- (c) Configure CA to allow key recovery
- (d) Configure a template for archiving key

This requires defining and enabling a template with Certificate Template console. Use CA console and go to Certificate Template folder to bring up Certificate Template console. Duplicate and rename the User template and set the settings as shown below.



This option, Archive subject's encryption private key, once enabled allows the KRA to retrieve the private key from a certificate store.



<http://blogs.technet.com/b/yungchou/archive/2013/10/21/enterprise-pki-with-windows-server-2012-r2-active-directory-certificate-services-part-2-of-2.aspx>

#### QUESTION 181

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:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

The following NPS template types are available for configuration in Templates Management:

- **Shared Secrets:** This template type makes it possible for you to specify a shared secret that you can reuse (by selecting the template in the appropriate location in the NPS console) when you configure RADIUS clients and servers.
- **RADIUS Clients:** This template type makes it possible for you to configure RADIUS client settings that you can reuse by selecting the template in the appropriate location in the NPS console.
- **Remote RADIUS Servers:** This template makes it possible for you to configure remote RADIUS server settings that you can reuse by selecting the template in the appropriate location in the NPS console.
- **IP Filters:** This template makes it possible for you to create Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) filters that you can reuse (by selecting the template in the appropriate location in the NPS console) when you configure network policies.
- **Health Policies:** This template makes it possible for you to create health policy settings that you can reuse (by selecting the template in the appropriate location in the NPS console) when you configure health policies.
- **Remediation Server Groups:** This template makes it possible for you to create remediation server group settings that you can be reuse (by selecting the template in the appropriate location in the NPS console) when you configure remediation server groups.

<https://technet.microsoft.com/en-us/library/ee663945>

#### **QUESTION 182**

Your network contains an Active Directory domain named contoso.com. Network Policy Server (NPS) is deployed to the domain.

You plan to deploy Network Access Protection (NAP). You need to configure the requirements that are validated on the NPS client computers.

What should you do?

- A. From the Network Policy Server console, configure a network policy.
- B. From the Network Policy Server console, configure a health policy.

- C. From the Network Policy Server console, configure a Windows Security Health Validator (WSHV) policy.
- D. From a Group Policy object (GPO), configure the NAP Client Configuration security setting.
- E. From a Group Policy object (GPO), configure the Network Access Protection Administrative Templates setting.

**Correct Answer: C**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

The Windows Security Health Agent (WSHA) is included in Windows Vista as part of the operating system. The corresponding Windows Security Health Validator (WSHV) is included in Windows Server 2008 as part of the operating system. By using the NAP API set, other products can also implement SHAs and SHVs to integrate with NAP. For example, an antivirus software vendor can use the API set to create a custom SHA and SHV. These components can then be integrated into the NAP solutions that software vendor's customers deploy.

If you are a network or system administrator planning to deploy NAP, you can deploy NAP with the WSHA and WSHV that are included with the operating system. You can also check with other software vendors to find out if they provide SHAs and SHVs for their products.

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.
- The client computer has antivirus software installed and running.
- The client computer has current antivirus updates installed.
- The client computer has antispyware software installed and running.
- The client computer has current antispyware updates installed.
- Microsoft Update Services is enabled on the client computer.

<https://technet.microsoft.com/en-us/library/cc754378>

#### **QUESTION 183**

Your network contains an Active Directory domain named contoso.com. The domain contains client computers that run either Windows XP or Windows 8. Network Policy Server (NPS) is deployed to the domain.

You plan to create a system health validator (SHV). You need to identify which policy settings can be applied to all of the computers.

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

- A. Antispyware is up to date.
- B. Automatic updating is enabled.
- C. Antivirus is up to date.
- D. A firewall is enabled for all network connections.
- E. An antispyware application is on.

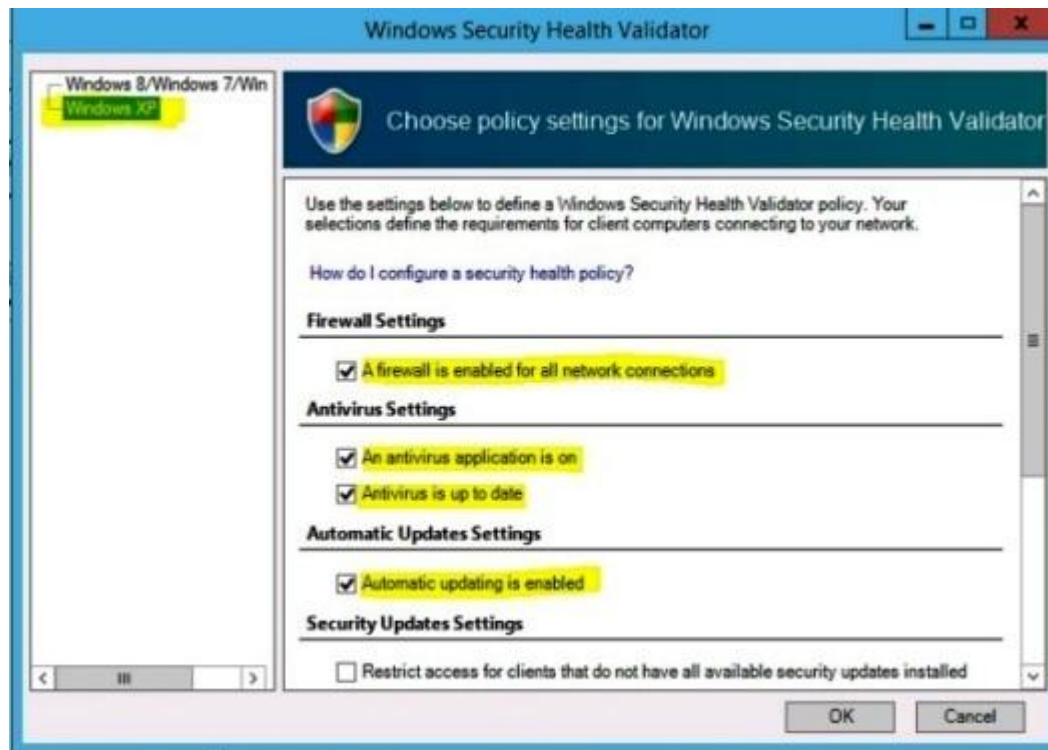
**Correct Answer:** BCD

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

You can only choose **An antispyware application is on** if the client computer is running Windows Vista® or Windows® 7. The WSHA on NAP client computers running Windows XP SP3 does not monitor the status of antispyware applications.







<https://technet.microsoft.com/en-us/library/cc731260.aspx>

#### QUESTION 184

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. The network contains two subnets named Subnet1 and Subnet2. Server1 has a DHCP scope for each subnet.

You need to ensure that noncompliant computers on Subnet1 receive different network policies than noncompliant computers on Subnet2.

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

- A. The NAP-Capable Computers conditions
- B. The NAS Port Type constraints
- C. The Health Policies conditions

- D. The MS-Service Class conditions
- E. The Called Station ID constraints

**Correct Answer:** CD

**Section:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

**Explanation/Reference:**

To configure NAP conditions in network policy using the Windows interface

1. Open the NPS console, double-click **Policies**, click **Network Policies**, and then double-click the policy you want to configure.
2. In policy **Properties**, click the **Conditions** tab, and then click **Add**. In **Select condition**, scroll to the **Network Access Protection** group of conditions.
3. 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.

4. 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.

5. If you want to configure the Health Policies condition, click **Health Policies**, and then click **Add**. In **Health Policies**, choose an existing health policy, and then click **OK**. If you have not yet configured health policies, click **New**, and then configure a new health policy.

The Health Policies condition restricts the policy to clients that meet the health criteria in the policy that you specify.

6. If you want to configure the NAP-capable Computers condition, click **NAP-capable Computers**, and then click **Add**. In **Specify the computers required to match this policy**, click either **Only computers that are NAP-capable** or **Only computers that are not NAP-capable**, and then click **OK**.

The NAP-capable Computers condition restricts the policy to either clients that are capable of participating in NAP or clients that are not capable of participating in NAP. This capability is determined by whether the client sends a statement of health (SoH) to NPS.

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

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

8. If you want to configure the Policy Expiration condition, click **Policy Expiration**, and then click **Add**. In **Policy Expiration**, configure the date and time when you want the network policy to expire, and then click **OK**.

The Policy Expiration condition specifies when the network policy expires; after the expiration date and time that you specify, the network policy is no longer evaluated by NPS.

<https://technet.microsoft.com/en-us/library/cc731560>

#### **QUESTION 185**

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

You enable and configure Routing and Remote Access (RRAS) on Server1. You create a user account named User1. You need to ensure that User1 can establish VPN connections to Server1.

What should you do?

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

**Correct Answer: C**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

Access permission is also granted or denied based on the dial-in properties of each user account.

<https://technet.microsoft.com/en-us/library/cc772123.aspx>

#### **QUESTION 186**

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. Connection Manager Administration Kit (CMAK).
- B. Routing and Remote Access
- C. Network Policy Server (NPS)
- D. Set-RemoteAccessRadius

**Correct Answer: C**

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

You can create connection request policies so that some RADIUS request messages sent from RADIUS clients are processed locally (NPS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (NPS is being used as a RADIUS proxy).

RADIUS Access-Request messages are processed or forwarded by NPS only if the settings of the incoming message match at least one of the connection request policies configured on the NPS server. If the policy settings match and the policy requires that the NPS server process the message, NPS acts as a RADIUS server, authenticating and authorizing the connection request. If the policy settings match and the policy requires that the NPS server forwards the message, NPS acts as a RADIUS proxy and forwards the connection request to a remote RADIUS server for processing.

<https://technet.microsoft.com/en-us/library/cc753603.aspx>

#### **QUESTION 187**

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

On Server1, you create a network policy named PPTP\_Policy. You need to configure PPTP\_Policy to apply only to VPN connections that use the PPTP protocol.

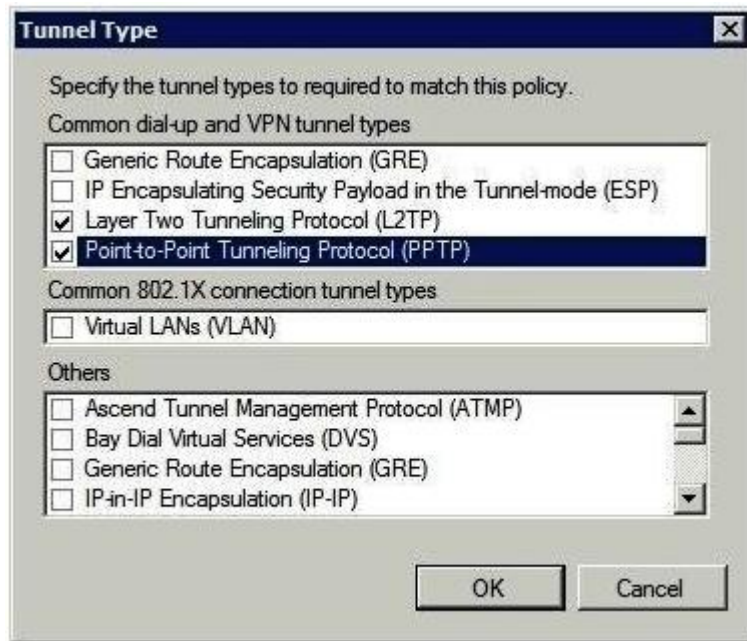
What should you configure in PPTP\_Policy?

- A. The Service Type
- B. The Tunnel Type
- C. The Framed Protocol
- D. The NAS Port Type

**Correct Answer: B**

**Section: Configure a Network Policy Server (NPS) infrastructure****Explanation****Explanation/Reference:**

The **Tunnel Type** restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP. The Tunnel Type attribute is typically used when you deploy virtual local area networks (VLANs).



<https://technet.microsoft.com/en-us/library/cc731220>

**QUESTION 188**

Your network contains two Active Directory domains named contoso.com and adatum.com. The contoso.com domain contains a server named Server1.contoso.com. The adatum.com domain contains a server named server2.adatum.com. Server1 and Server2 run Windows Server 2012 R2 and have the DirectAccess and VPN (RRAS) role service installed. Server1 has the default network policies and the default connection request policies.

You need to configure Server1 to perform authentication and authorization of VPN connection requests to Server2. Only users who are members of Adatum\Group1 must be allowed to connect.

Which two actions should you perform on Server1? (Each correct answer presents part of the solution. Choose two.)

- A. Network policies
- B. Connection request policies
- C. Create a network policy
- D. Create a connection request policy.

**Correct Answer:** AD

**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

If you configure an authentication method in connection request policy that is less secure than the authentication method you configure in network policy, the more secure authentication method that you configure in network policy will be overridden. For example, if you have one network policy that requires the use of Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2), which is a password-based authentication method for secure wireless, and you also configure a connection request policy to allow unauthenticated access, no clients are required to authenticate by using PEAP-MS-CHAP v2. In this example, all clients connecting to your network are granted unauthenticated access.

<https://msdn.microsoft.com/en-us/library/cc753603.aspx>

#### **QUESTION 189**

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 DHCP Server server role installed. The network contains 400 client computers that run Windows 8. All of the client computers are joined to the domain and are configured DHCP clients.

You install a new server named Server2 that runs Windows Server 2012 R2. On Server2, you install the Network Policy Server role service and you configure Network Access Protection (NAP) to use the DHCP enforcement method. You need to ensure that Server1 only provides a valid default gateway to computers that pass the system health validation.

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

- A. From the DHCP console, configure the 016 Swap Server option.
- B. From the DHCP console, create a new policy.
- C. From the NAP Client Configuration console, enable the DHCP Quarantine Enforcement Client.
- D. From the DHCP console, enable NAP on all scopes.
- E. From Server Manager, install the Network Policy Server role service.

**Correct Answer:** DE

**Section: Configure a Network Policy Server (NPS) infrastructure**

## Explanation

### Explanation/Reference:

Dynamic Host Configuration Protocol (DHCP) enforcement is deployed with a DHCP Network Access Protection (NAP) enforcement server component, a DHCP enforcement client component, and Network Policy Server (NPS). By using DHCP NAP enforcement, DHCP servers and NPS can enforce health policy when a computer attempts to lease or renew an IP version 4 (IPv4) address. However, if client computers are configured with a static IP address or are otherwise configured to circumvent the use of DHCP, this enforcement method is not effective.

<https://technet.microsoft.com/en-us/library/cc733020>

A NAP health policy server is a computer running Network Policy Server (NPS) that is acting in the role of a NAP health evaluation server. The NAP health policy server has health policies and network policies that are used to evaluate compliance of NAP client computers. All NAP enforcement methods require that you install a NAP health policy server.

<https://msdn.microsoft.com/en-us/library/dd296890>

## QUESTION 190

You are hired by ABC.com to administer an Active Directory domain named ABC.com which encompasses a RADIUS server by the name of ABC-SR08 running an installation of Windows Server 2012.

Your senior network administrator has provisioned a VPN server added to the network named ABC-VPN05 and thereafter orders the creation of numerous network policies on ABC-SR08.

Which of the following actions need to be taken if you are assigned the task of having ABC-SR08 configured to accept appeals for authentication from ABC-VPN05?

- A. You will need to run the Add-RemoteAccessRadius command on ABC-SR08.
- B. You will need to run the Get-NpsRadiusClient command on ABC-SR08.
- C. You will need to run the Set-RemoteAccessRadius command on ABC-SR08.
- D. You will need to configure the Routing and Remote Access Service (RRAS) role service on ABC-SR08.

**Correct Answer: B**

**Section: Configure a Network Policy Server (NPS) infrastructure**

### Explanation

### Explanation/Reference:

The **Get-NpsRadiusClient** cmdlet gets Remote Authentication Dial-In User Service (RADIUS) clients. A RADIUS client uses a RADIUS server to manage authentication, authorization, and accounting requests that the client sends. A RADIUS client can be an access server, such as a dial-up server or wireless access point, or a RADIUS proxy.

<https://technet.microsoft.com/en-us/library/jj872741.aspx>

### QUESTION 191

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 the Network Policy Server (NPS) templates.

Which three settings should you identify? (Each 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:** Configure a Network Policy Server (NPS) infrastructure

**Explanation**

#### **Explanation/Reference:**

The following NPS template types are available for configuration in Templates Management:

**Shared Secrets:** This template type makes it possible for you to specify a shared secret that you can reuse (by selecting the template in the appropriate location in the NPS console) when you configure RADIUS clients and servers.

**RADIUS Clients:** This template type makes it possible for you to configure RADIUS client settings that you can reuse by selecting the template in the appropriate location in the NPS console.

**Remote RADIUS Servers:** This template makes it possible for you to configure remote RADIUS server settings that you can reuse by selecting the template in the appropriate location in the NPS console.

**IP Filters:** This template makes it possible for you to create Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) filters that you can reuse (by selecting the template in the appropriate location in the NPS console) when you configure network policies.

**Health Policies:** This template makes it possible for you to create health policy settings that you can reuse (by selecting the template in the appropriate location in the NPS console) when you configure health policies.



**Remediation Server Groups:** This template makes it possible for you to create remediation server group settings that you can be reuse (by selecting the template in the appropriate location in the NPS console) when you configure remediation server groups.

[https://technet.microsoft.com/en-us/library/Ee663945\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Ee663945(v=WS.10).aspx)

## QUESTION 192

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:

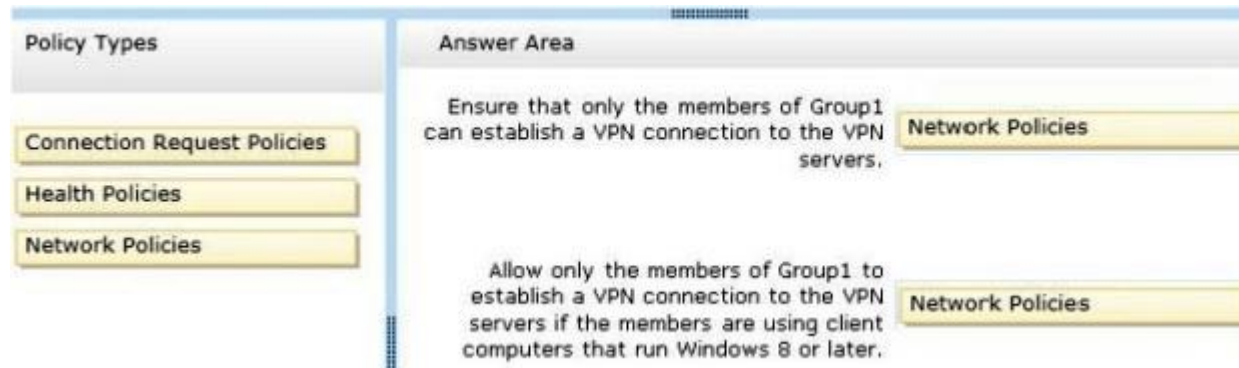
- Ensure that only the members of Group1 can establish a VPN connection to the VPN servers.
- Allow only the members of Group1 to establish a VPN connection to the VPN servers if the members are using client computers that run Windows 8 or later.

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.

**Select and Place:**

Policy Types	Answer Area
<div>Connection Request Policies</div> <div>Health Policies</div> <div>Network Policies</div>	<div> <p>Ensure that only the members of Group1 can establish a VPN connection to the VPN servers.</p> <div>Policy type</div> </div> <div> <p>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.</p> <div>Policy type</div> </div>

**Correct Answer:**



## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

#### Explanation/Reference:

#### Network Policies

*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. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that Network Policy Server (NPS) performs client health checks during the authorization process.

<https://technet.microsoft.com/library/cc754107.aspx>

#### Connection Request Policies

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.

<https://technet.microsoft.com/library/cc753603>

#### Deprecated functionality

With the release of Windows Server 2012 R2, NAP is deprecated. NAP is fully supported in Windows Server 2012 R2 and Windows 8.1.

For the **health policy** creation, enforcement, and remediation features provided by NAP, as well as for monitoring, consider using System Center Configuration Manager to replace and enhance NAP's monitoring functionality.

<https://technet.microsoft.com/library/hh831683>

### QUESTION 193

Your network contains an Active Directory forest named contoso.com. The forest contains a Network Policy Server (NPS) server named NPS1 and a VPN server named VPN1. VPN1 forwards all authentication requests to NPS1. A partner company has an Active Directory forest named adatum.com. The adatum.com forest contains an NPS server named NPS2.

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

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

Select and Place:

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

Correct Answer:

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

Section: Configure a Network Policy Server (NPS) infrastructure

## Explanation

### Explanation/Reference:

#### Connection Request Policies

*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.

You can create connection request policies so that some RADIUS request messages sent from RADIUS clients are processed locally (NPS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (NPS is being used as a RADIUS proxy).

<https://msdn.microsoft.com/en-us/library/cc753603.aspx>

#### Remote RADIUS Server Groups

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

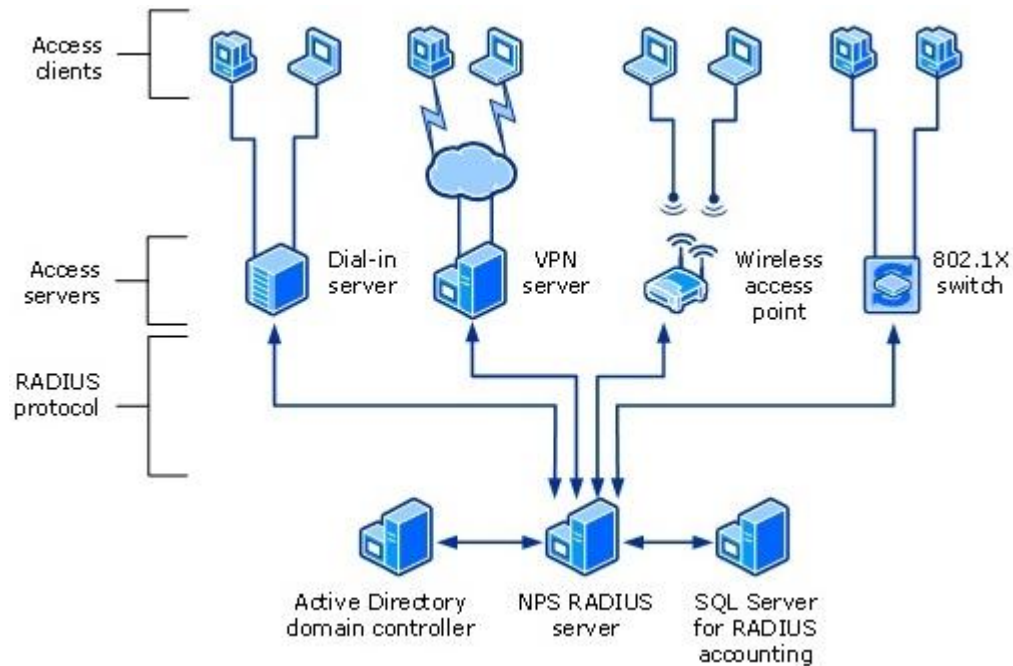
To configure NPS as a RADIUS proxy, you must create a connection request policy that contains all of the information required for NPS to evaluate which messages to forward and where to send the messages.

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

<https://msdn.microsoft.com/en-us/library/cc754518.aspx>

Network Policy Server (NPS) can be used as a Remote Authentication Dial-In User Service (RADIUS) server to perform authentication, authorization, and accounting for RADIUS clients. A **RADIUS client** can be an access server, such as a dial-up server or wireless access point, or a RADIUS proxy.

The following illustration shows NPS as a RADIUS server for a variety of access clients, and also shows a RADIUS proxy. NPS uses an AD DS domain for user credential authentication of incoming RADIUS Access-Request messages.



<https://msdn.microsoft.com/en-us/library/cc755248.aspx>

#### QUESTION 194

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

Correct Answer:

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

## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

Explanation/Reference:

### Windows Security Health Validator

The **Windows Security Health Validator** (WSHV) provides settings that you can configure based on the requirements of your deployment. When you enable requirements in the WSHV, client computers that do not meet all of these requirements are evaluated as noncompliant with the WSHV. Depending on settings in **network policy** and **health policy**, client computers that are noncompliant with the WSHV might have their network access restricted and be automatically remediated. Whether or not a client computer that is noncompliant with the WSHV is ultimately noncompliant with NAP health policy depends on the System Health Validators (SHVs) that are configured in health policy as required for compliance.

If a client computer is noncompliant with one of the requirements of the WSHV, it is considered noncompliant with the WSHV as a whole.

If you select **A firewall is enabled for all network connections**, firewall settings on client computer are verified.

<https://technet.microsoft.com/en-us/library/cc731260>

## Health Policies

*Health policies* consist of one or more system health validators (SHVs) and other settings that allow you to define client computer configuration requirements for the Network Access Protection (NAP)-capable computers that attempt to connect to your network.

When NAP-capable clients attempt to connect to the network, the client computer sends a statement of health (SoH) to Network Policy Server (NPS). The SoH is a report of the client configuration state, and NPS compares the SoH to the requirements defined in health policy. If the client configuration state does not match the requirements defined in health policy, NPS takes one of the following actions, depending on how NAP is configured:

- The connection request by the NAP client is rejected.
- The NAP client is placed on a restricted network where it can receive updates from remediation servers that bring the client into compliance with health policy. After the client is compliant with health policy, it is allowed to connect.
- The NAP client is allowed to connect to the network despite being noncompliant with health policy.

You can define client health policies in NPS by adding one or more SHVs to the health policy.

After a health policy is configured with one or more SHVs, you can add the health policy to the Health Policies condition of a network policy that you want to use to enforce NAP when client computers connect to your network.

<https://technet.microsoft.com/en-us/library/cc771934.aspx>

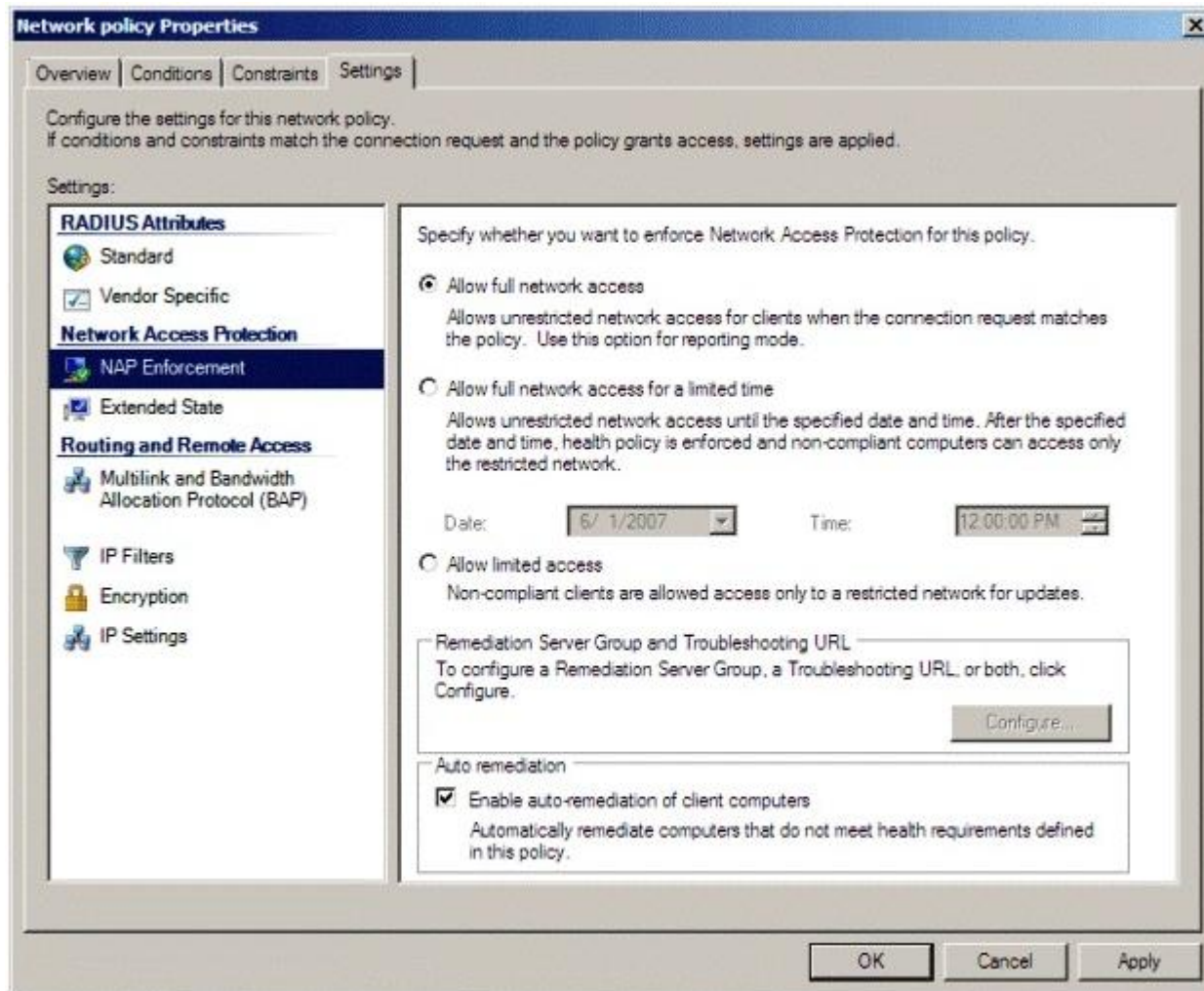
## Configure Network Policy for Reporting Mode

Reporting mode is one of the three primary phases of a NAP deployment. Data obtained from this stage allows you to estimate the impact to your user base when enforcement is enabled and to adjust policy settings or correct network infrastructure, as appropriate. Data also allows you to verify that NAP is working correctly and make infrastructure changes, if necessary. During this phase, NAP notifications are not presented to users and the network access of noncompliant client computers is not restricted. You can use the reporting mode stage to begin training technical support personnel. If your goals for deploying NAP are only to track overall client health and monitor elements of the security infrastructure that are leveraged by NAP system health agents (SHAs) and system health validators (SHVs), you might decide to leave your NAP deployment in reporting mode indefinitely.

To configure network policy for reporting mode:

1. Click **Start**, click **Run**, type **nps.msc**, and then press ENTER.
2. In the Network Policy Server console tree, open **Policies\Network Policies**.
3. In the details pane, under **Policy Name**, double-click the name of the network policy for noncompliant NAP client computers.
4. In the policy properties window, on the **Settings** tab, click **NAP Enforcement**, choose **Allow full network access**, and then click **OK**. See the following example.





<https://technet.microsoft.com/pt-pt/library/dd314198>

#### QUESTION 195

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



User name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

What should you identify? To answer, select the appropriate policy for each user in the answer area.

**Hot Area:**

Answer Area

User1:

Policy1
Policy2
Policy3

User2:

Policy1
Policy2
Policy3

User3:

Policy1
Policy2
Policy3

Correct Answer:

Answer Area

User1:

Policy1
Policy2
Policy3

User2:

Policy1
Policy2
Policy3

User3:

Policy1
Policy2
Policy3

## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

#### Explanation/Reference:

The policy is assigned a **Processing Order**. Policies are evaluated in the order shown in this column. *The first policy to match the conditions of the connection request is the one used* to authorize and configure the connection. When troubleshooting connection failures, ensure that the policy order is not causing an unexpected policy to be used.

<https://technet.microsoft.com/en-us/library/ff687703>

#### QUESTION 196

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Server1 has the Network Policy Server server role installed. Server2 has the DHCP Server server role installed. Both servers run Windows Server 2012 R2.

You are configuring Network Access Protection (NAP) to use DHCP enforcement. You configure a DHCP scope as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that non-compliant NAP clients receive different DHCP options than compliant NAP clients.

What should you configure on each server? To answer, select the appropriate options for each server in the answer area.

#### Exhibit:

Scope [192.168.10.0] Scope1 Properties

General DNS Network Access Protection Advanced

Network Access Protection

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

Network Access Protection Settings

☒ Enable for this scope

☐ Use default Network Access Protection profile

☒ Use custom profile

Profile Name

Profile1

☐ Disable for this scope

OK Cancel Apply

Hot Area:

Answer Area

Server1:

Server2:

Correct Answer:

Answer Area

Server1:

Server2:

Section: Configure a Network Policy Server (NPS) infrastructure  
Explanation

**Explanation/Reference:**

If policies are filtered by DHCP scope, then **MS-Service Class** is configured in policy conditions.

The administrator must define the following settings on the NAP DHCP server:

- **Remote RADIUS server groups:** If connection requests are forwarded from the DHCP server to a NAP health policy server on another computer, you must configure the NPS service on the NAP DHCP server to forward connection requests to the NAP health policy server. This setting is not required if the NAP DHCP server is also the NAP health policy server.
- **NAP-enabled scopes:** In order to use a DHCP scope with NAP, you must enable it specifically for NAP in scope properties under NAP settings.
- **Default user class:** You must configure any required **scope options** for computers that are compliant with health requirements.
- **Default NAP class:** You must configure any required **scope options** for computers that are noncompliant with health requirements. A default gateway is not provided to noncompliant computers regardless of whether the 003 Router option is configured here.

<https://msdn.microsoft.com/en-us/library/dd125315>

**QUESTION 197**

Your network contains an Active Directory named contoso.com. You have users named User1 and user2. The Network Access Permission for User1 is set to Control access through NPS Network Policy. The Network Access Permission for User2 is set to Allow access.

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

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

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

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

**Exhibit1 (exhibit):**

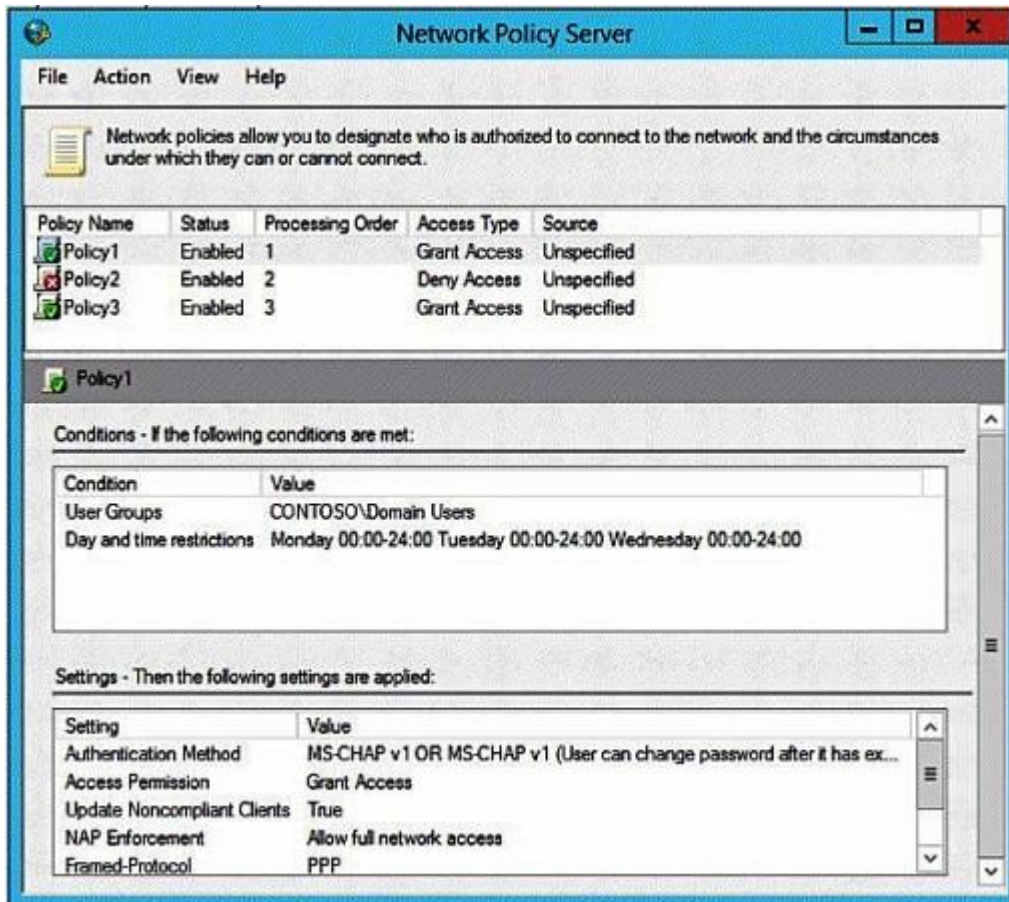


Exhibit2 (exhibit):

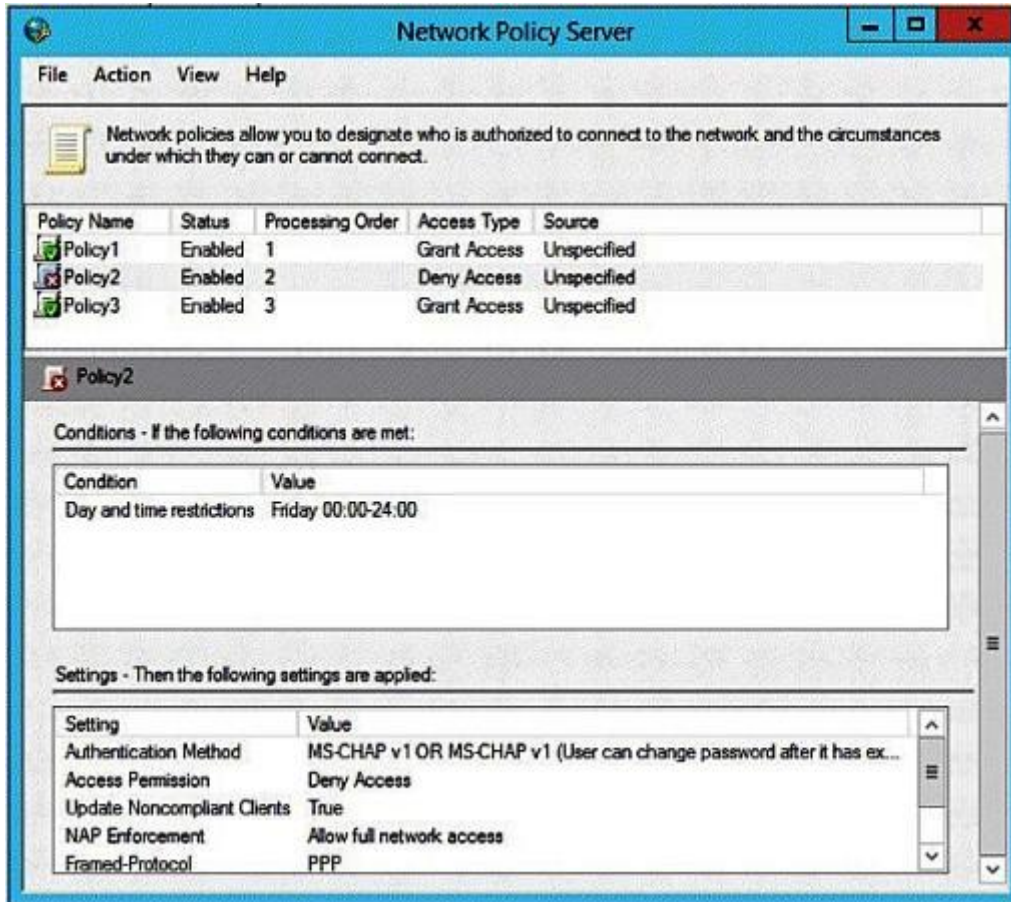
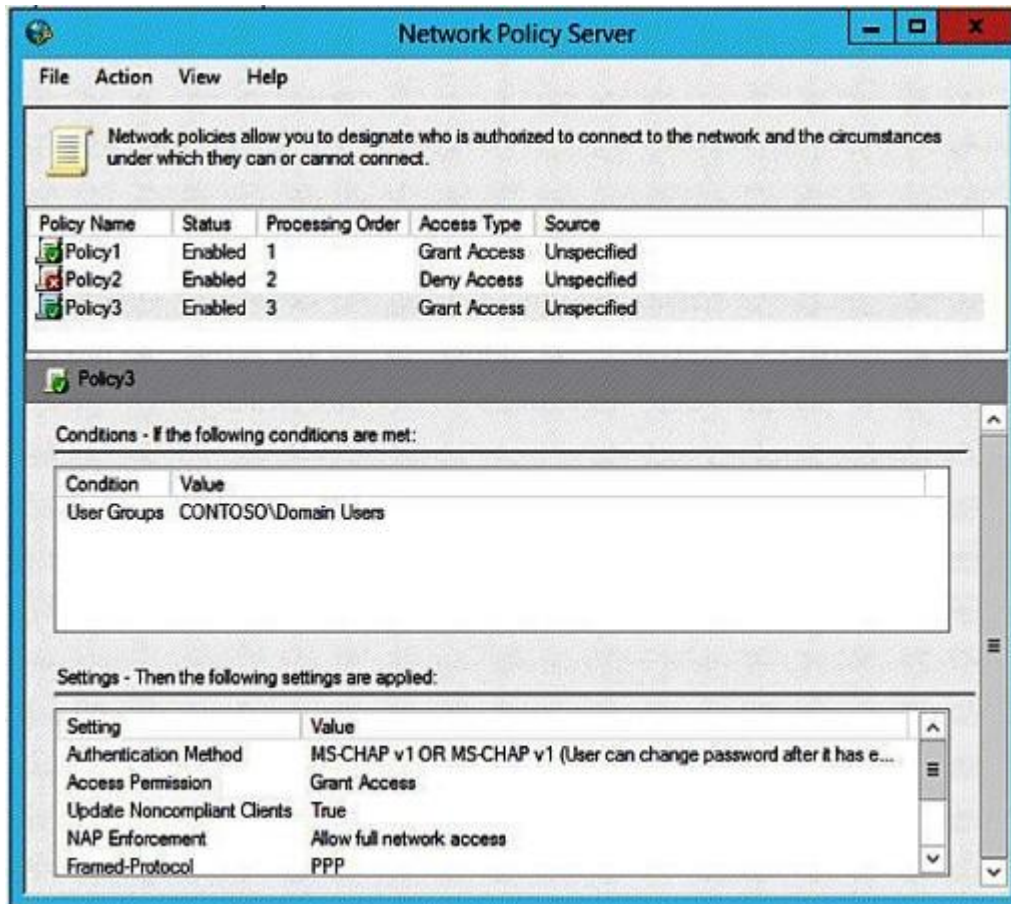


Exhibit3 (exhibit):





Hot Area:

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

**Correct Answer:**

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

**Section: Configure a Network Policy Server (NPS) infrastructure**  
**Explanation**

**Explanation/Reference:**

The policy is assigned a **Processing Order**. Policies are evaluated in the order shown in this column. *The first policy to match the conditions of the connection request is the one used* to authorize and configure the connection. When troubleshooting connection failures, ensure that the policy order is not causing an unexpected policy to be used.

<https://technet.microsoft.com/en-us/library/ff687703>

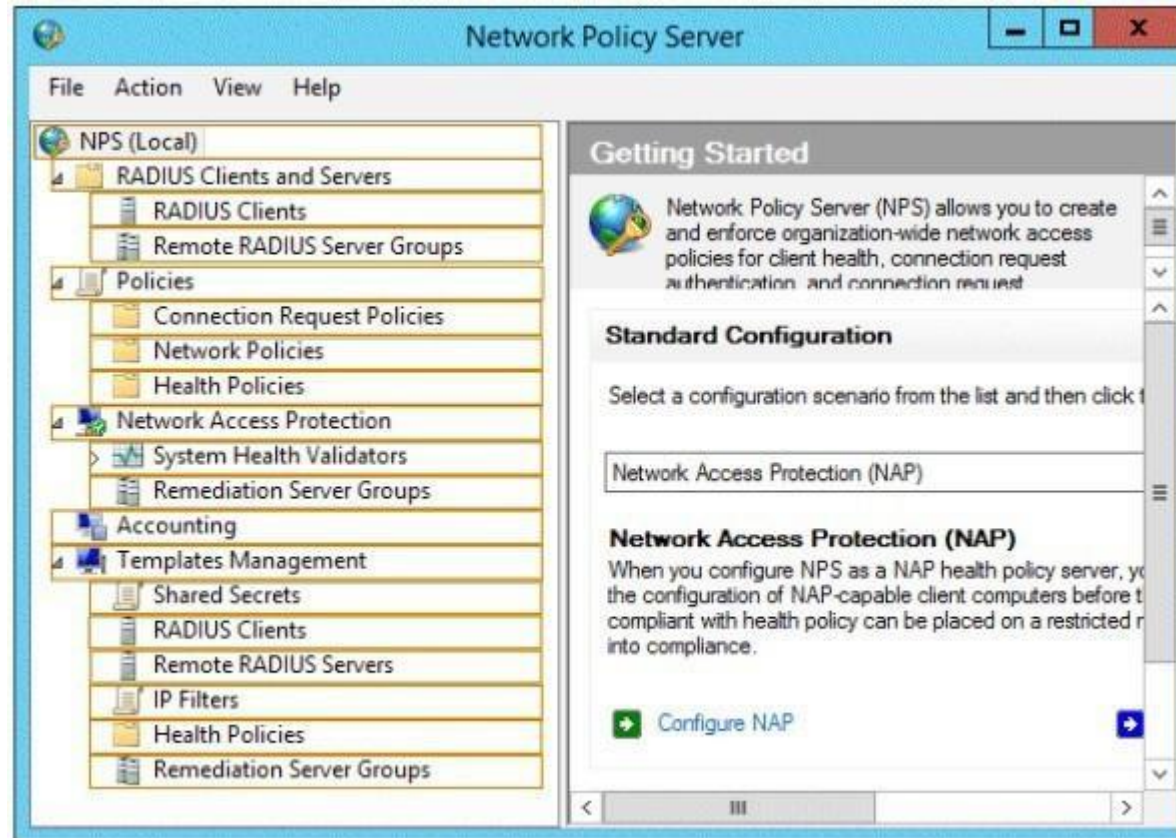
**QUESTION 198**

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.

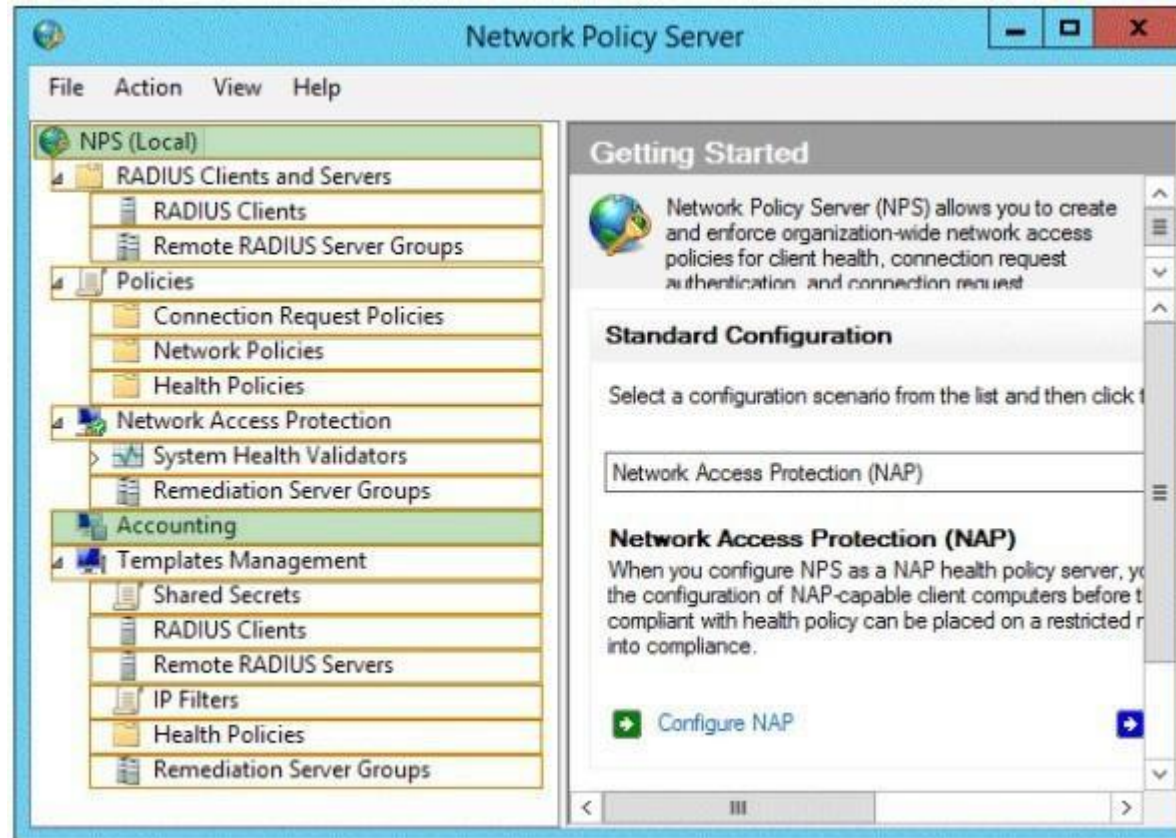
You need to ensure that only Server2 contains event information about authentication requests from connections to Server1.

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:**



Correct Answer:



## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

#### Explanation/Reference:

To configure NPS event logging using the Windows interface

1. Open the Network Policy Server (NPS) snap-in.
2. Right-click **NPS (Local)**, and then click **Properties**.
3. On the **General** tab, select each required option, and then click **OK**.

<https://technet.microsoft.com/en-us/library/cc731085>

You can log user authentication and accounting requests to log files in text format or database format, or you can log to a stored procedure in a SQL Server database. Request logging is used primarily for connection analysis and billing purposes, and is also useful as a security investigation tool, providing you with a method of tracking down the activity of an attacker.

<https://technet.microsoft.com/en-us/library/cc755120>

### **To configure SQL Server logging in NPS**

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. In the console tree, click **Accounting**.

<https://technet.microsoft.com/en-US/library/cc754123.aspx>

### **QUESTION 199**

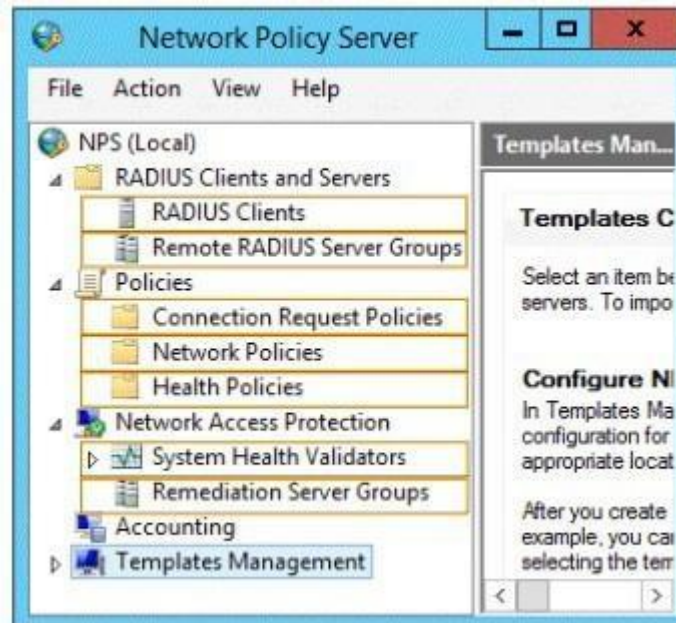
You have a server named Server1 that runs Windows Server 2012 R2. You configure Network Access Protection (NAP) on Server1. Your company implements a new security policy stating that all client computers must have the latest updates installed. The company informs all employees that they have two weeks to update their computer accordingly.

You need to ensure that if the client computers have automatic updating disabled, they are provided with full access to the network until a specific date and time.

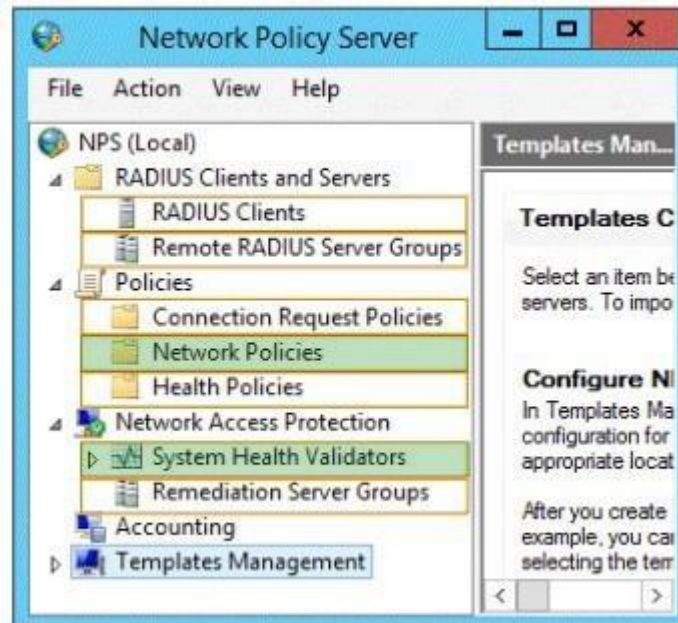
Which two nodes should you configure? To answer, select the appropriate two nodes in the answer area.

**Hot Area:**





Correct Answer:



## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

#### Explanation/Reference:

#### To configure a network policy to grant or deny access

1. Open the Network Policy Server (NPS) Microsoft Management Console (MMC) snap-in, double-click **Policies**, and then double-click **Network Policies**.
2. In the details pane, double-click the network policy that you want to configure.
3. In the network policy **Properties** dialog box, on the **Overview** tab, change **Access Permission** to either **Grant access** or **Deny access**.

<https://technet.microsoft.com/en-us/library/cc771864>

System health validators (SHVs) define configuration requirements for NAP client computers. All SHVs include five error code conditions. If an error code is returned to the SHV, you can choose to have the SHV evaluate the client as either compliant or noncompliant.

#### To configure system health validators



1. On the NAP health policy server, click **Start**, click **Run**, type **nps.msc**, and then press ENTER.
2. In the NPS console tree, open **Network Access Protection**, and then click **System Health Validators**.
3. In the NPS console tree, expand the name of the SHV you want to configure.

<https://msdn.microsoft.com/en-us/library/dd314150>

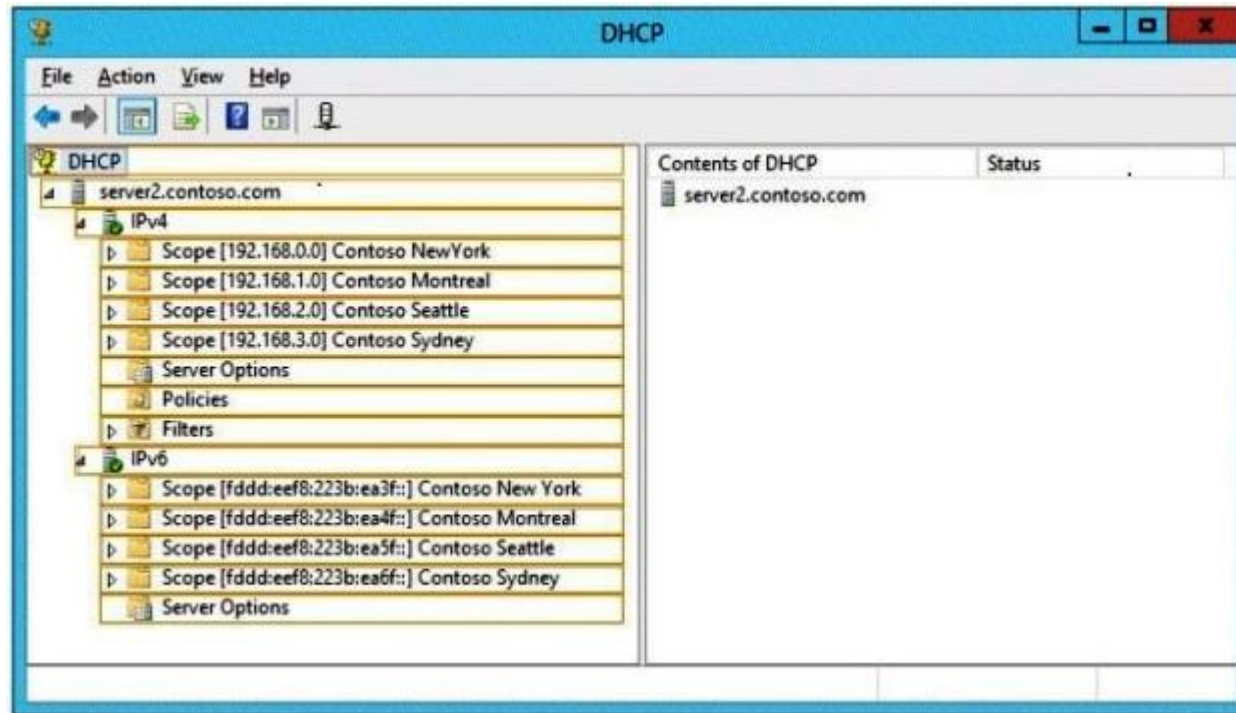
#### **QUESTION 200**

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.

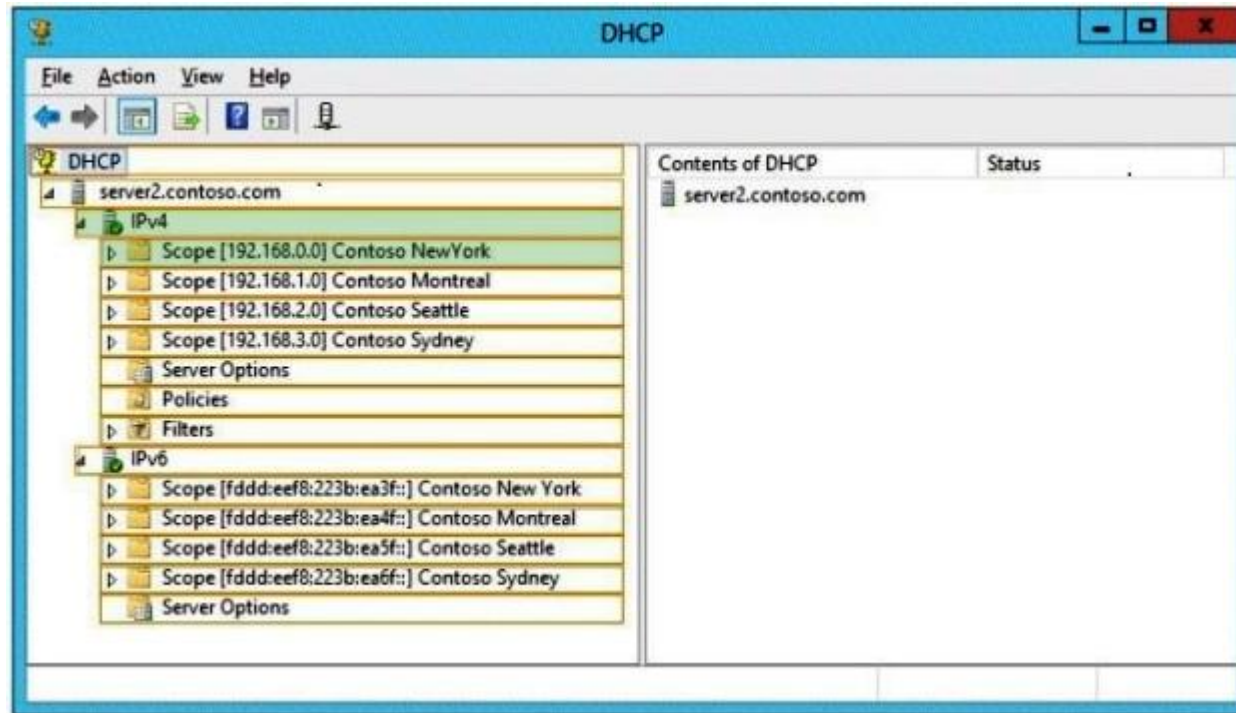
You need to ensure that Network Access Protection (NAP) enforcement for DHCP applies to all of the client computers except for the client computers in the New York office.

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

**Hot Area:**



Correct Answer:



## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

#### Explanation/Reference:

To configure DHCP scopes for NAP, do one of the following:

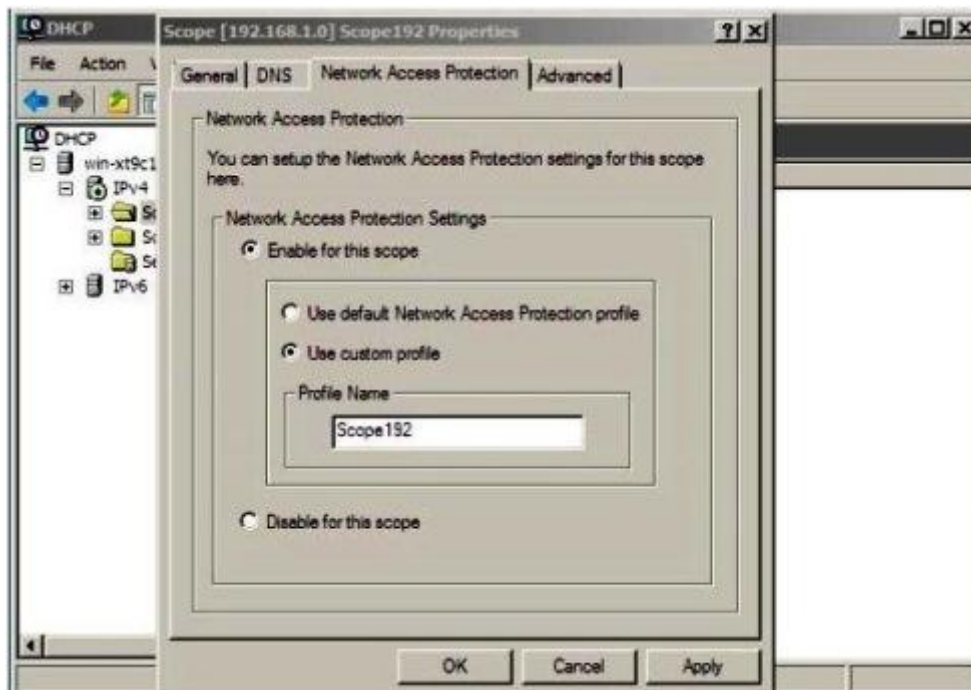
- To enable NAP for all scopes on a DHCP server, obtain the Internet Protocol version 4 (**IPv4**) properties of the server, click the **Network Access Protection** tab, and configure NAP.
- To enable NAP for individual scopes on a DHCP server, obtain the scope properties, click the **Network Access Protection** tab, and configure NAP.

<https://technet.microsoft.com/en-us/library/cc754977>

Open the properties page of the scope by right clicking the scope.



Open the 'Network Access Protection' tab in the properties page and set the custom profile name to the Scope name itself. We would be using the Name of the scope here and while creating the NPS profile for consistency.



<http://blogs.technet.com/b/teamdhcp/archive/2008/05/28/configuring-custom-nps-policies-per-dhcp-scope.aspx>

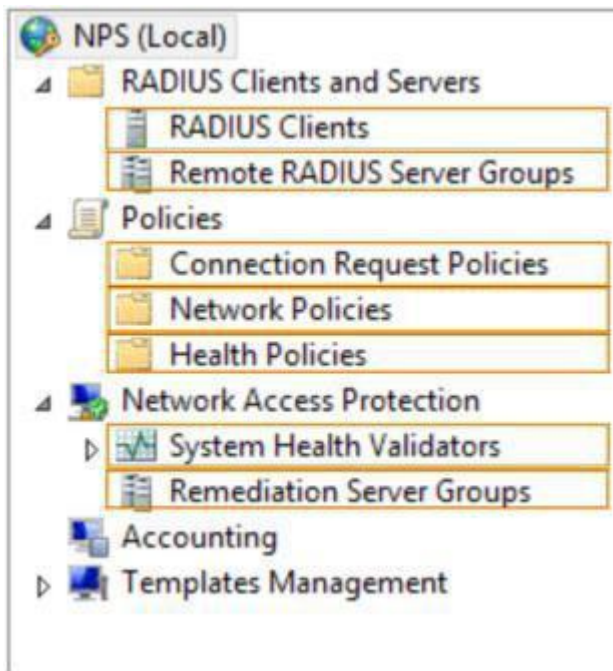
#### QUESTION 201

Your network contains a RADIUS server named Admin1.

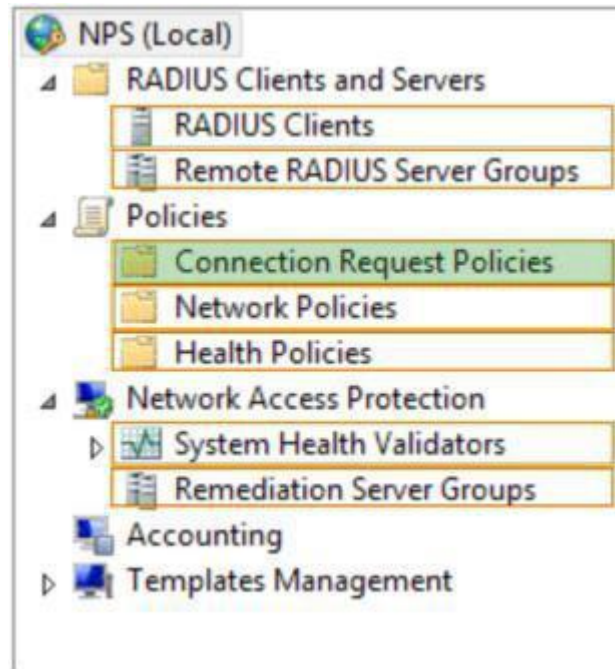
You install a new server named Server2 that runs Windows Server 2012 R2 and has Network Policy Server (NPS) installed. You need to ensure that all accounting requests for Server2 are forwarded to Admin1. On Server2, you create a new remote RADIUS server group named Group1 that contains Admin1.

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

**Hot Area:**



**Correct Answer:**



## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

#### Explanation/Reference:

*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.

<https://technet.microsoft.com/en-us/library/cc753603.aspx>

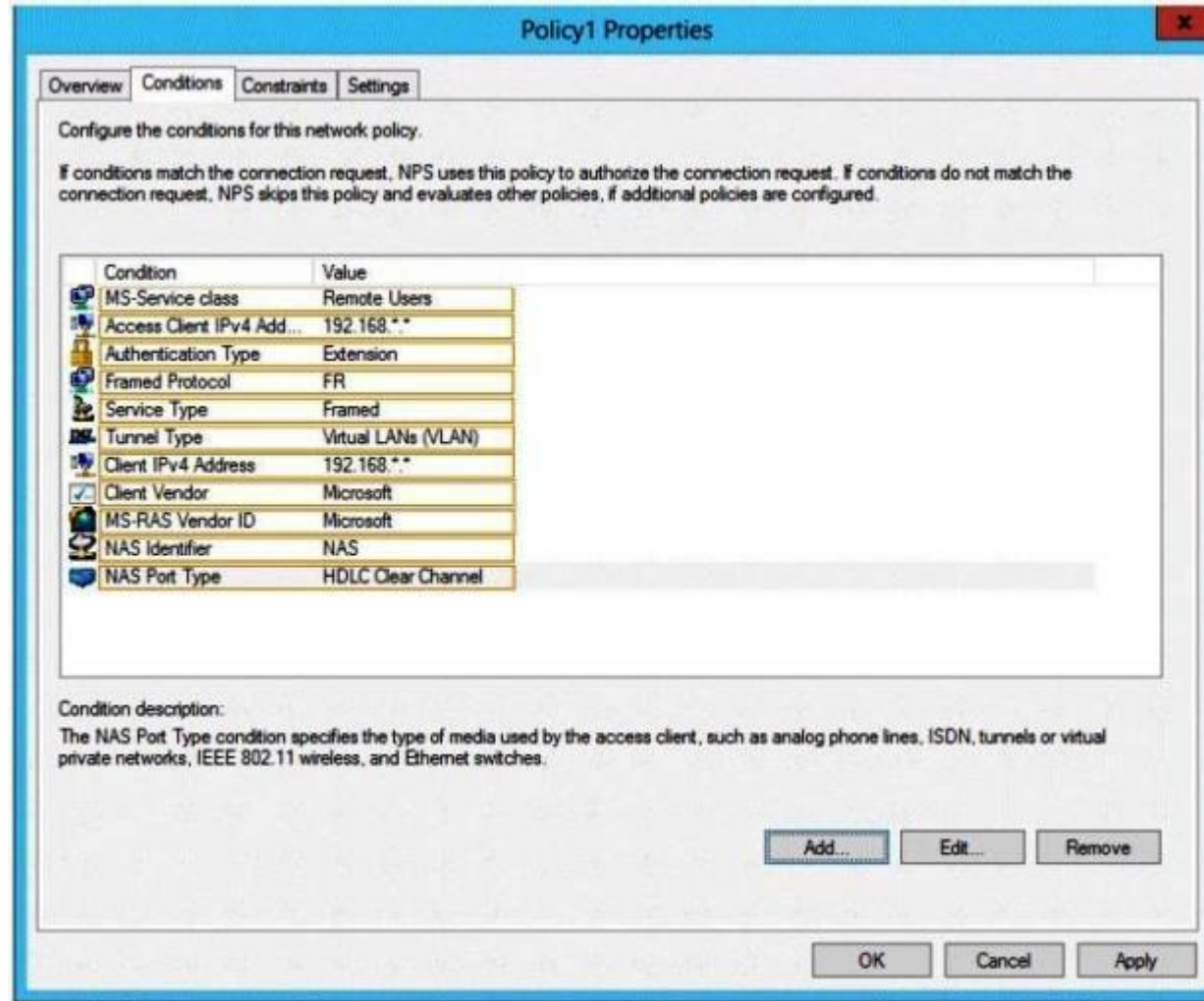
### QUESTION 202

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

An administrator creates a Network Policy Server (NPS) network policy named Policy1. You need to ensure that Policy1 applies to L2TP connections only.

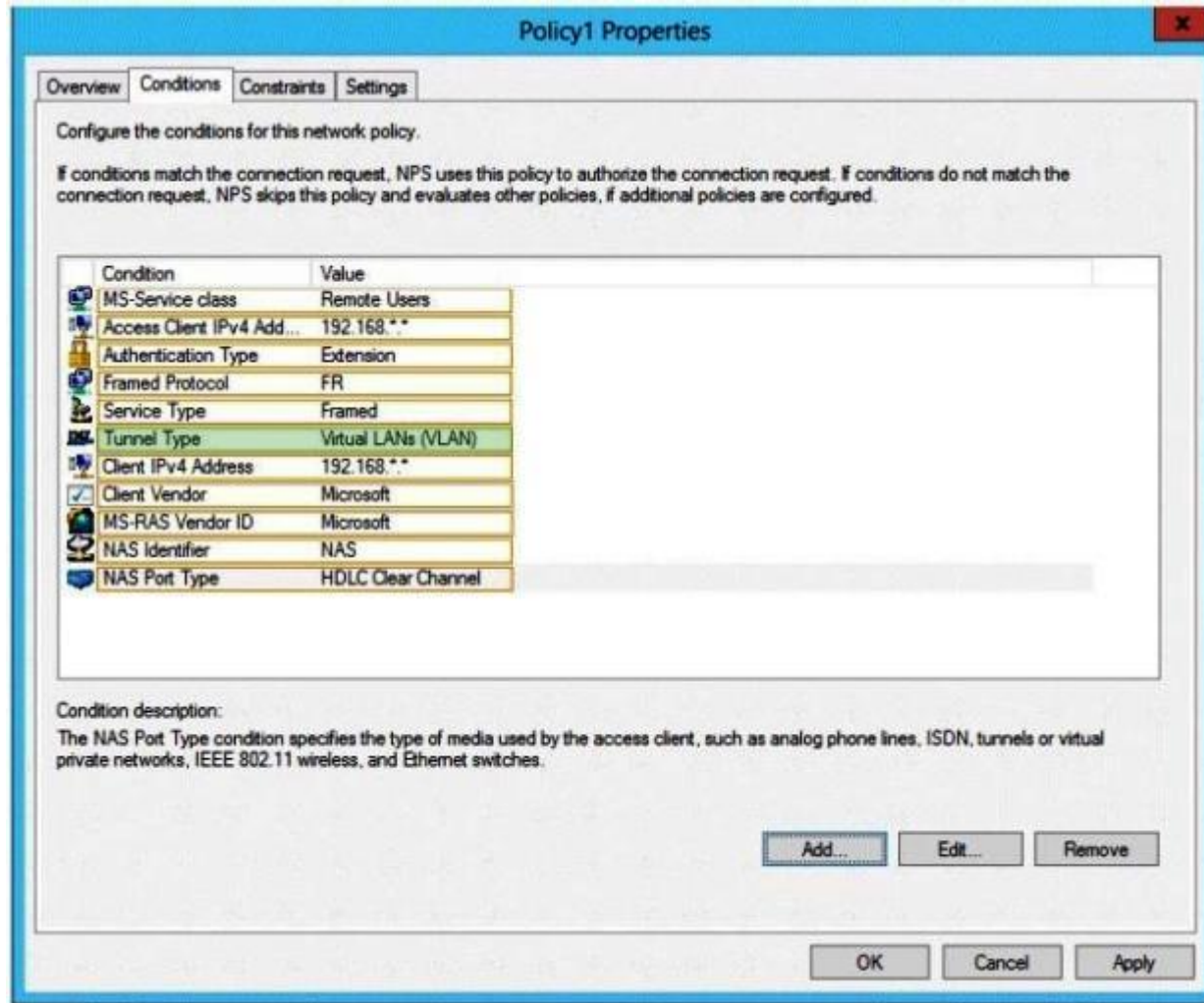
Which condition should you modify? To answer, select the appropriate object in the answer area.

Hot Area:



Correct Answer:





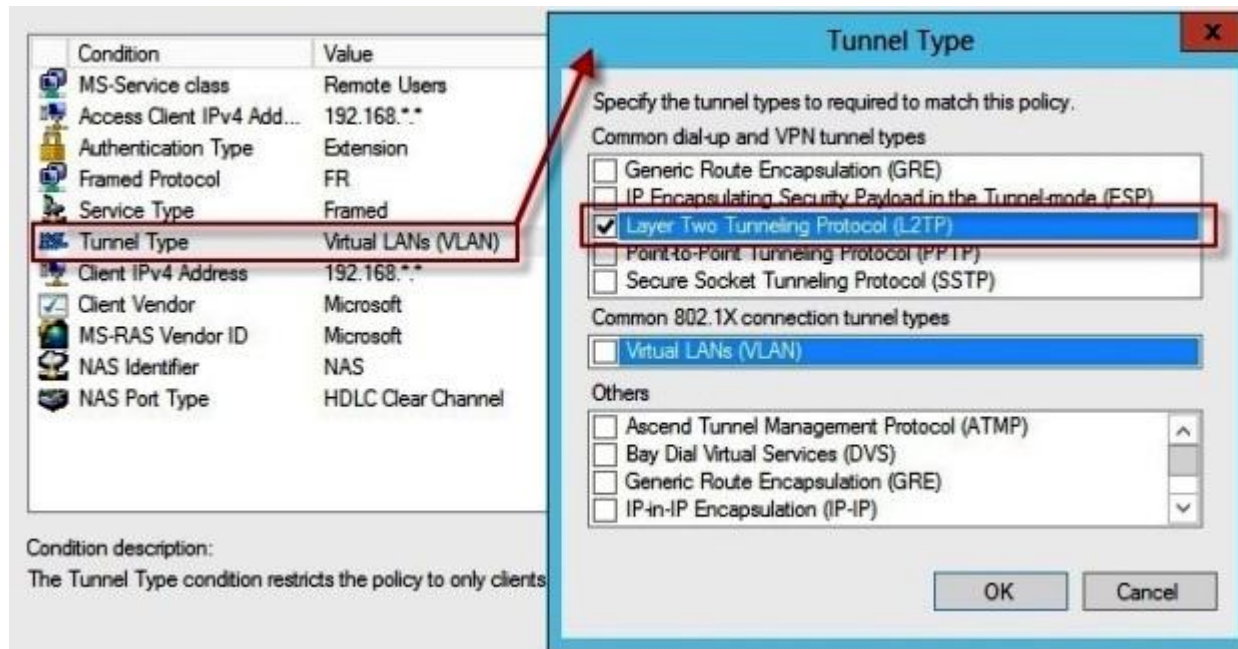
## Section: Configure a Network Policy Server (NPS) infrastructure

### Explanation

#### Explanation/Reference:

*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.

**Tunnel Type** — Used to designate the type of tunnel that is being created by the requesting client. Tunnel types include the Point-to-Point Tunneling Protocol (PPTP) and the Layer Two Tunneling Protocol (L2TP).



<https://msdn.microsoft.com/en-us/library/cc753603.aspx>

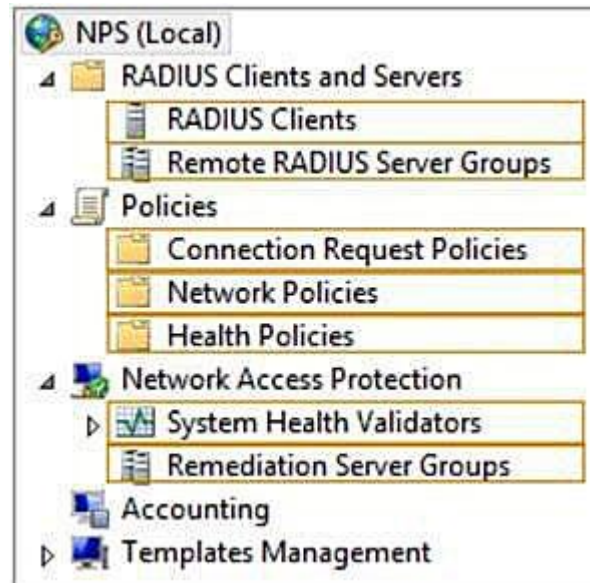
### QUESTION 203

Your network contains a RADIUS server named Server1.

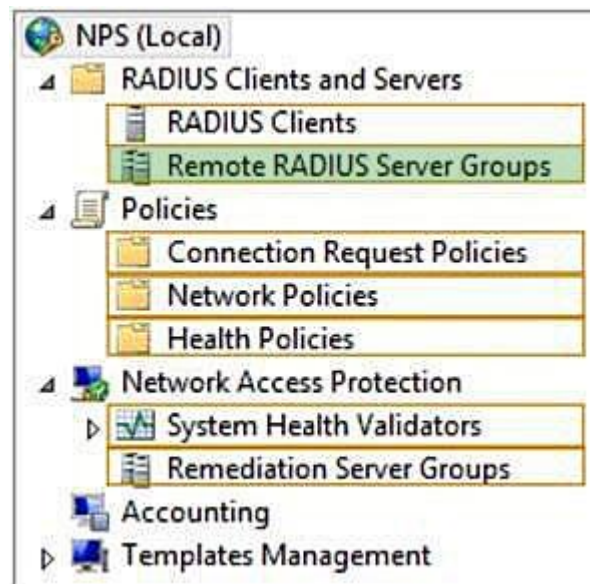
You install a new server named Server2 that runs Windows Server 2012 R2 and has Network Policy Server (NPS) installed. You need to ensure that all accounting requests for Server2 are forwarded to Server1. On Server2, you configure a Connection Request Policy.

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

**Hot Area:**



Correct Answer:



Section: Configure a Network Policy Server (NPS) infrastructure

## Explanation

### Explanation/Reference:

#### Configuring RADIUS servers for a group

A *remote RADIUS server group* is a named group that contains one or more RADIUS servers. If you configure more than one server, you can specify load balancing settings to either determine the order in which the servers are used by the proxy or to distribute the flow of RADIUS messages across all servers in the group to prevent overloading one or more servers with too many connection requests.

Each server in the group has the following settings:

- Name or address

Each group member must have a unique name within the group. The name can be an IP address or a name that can be resolved to its IP address.

- Authentication and accounting

You can forward authentication requests, accounting requests, or both to each remote RADIUS server group member.

- Load balancing

A priority setting is used to indicate which member of the group is the primary server (the priority is set to 1). For group members that have the same priority, a weight setting is used to calculate how often RADIUS messages are sent to each server. You can use additional settings to configure the way in which the NPS server detects when a group member first becomes unavailable and when it becomes available after it has been determined to be unavailable.

After a remote RADIUS server group is configured, it can be specified in the authentication and accounting settings of a connection request policy. Because of this, you can configure a remote RADIUS server group first. Next, you can configure the connection request policy to use the newly configured remote RADIUS server group. Alternatively, you can use the New Connection Request Policy Wizard to create a new remote RADIUS server group while you are creating the connection request policy.

<https://msdn.microsoft.com/en-us/library/cc754518.aspx>

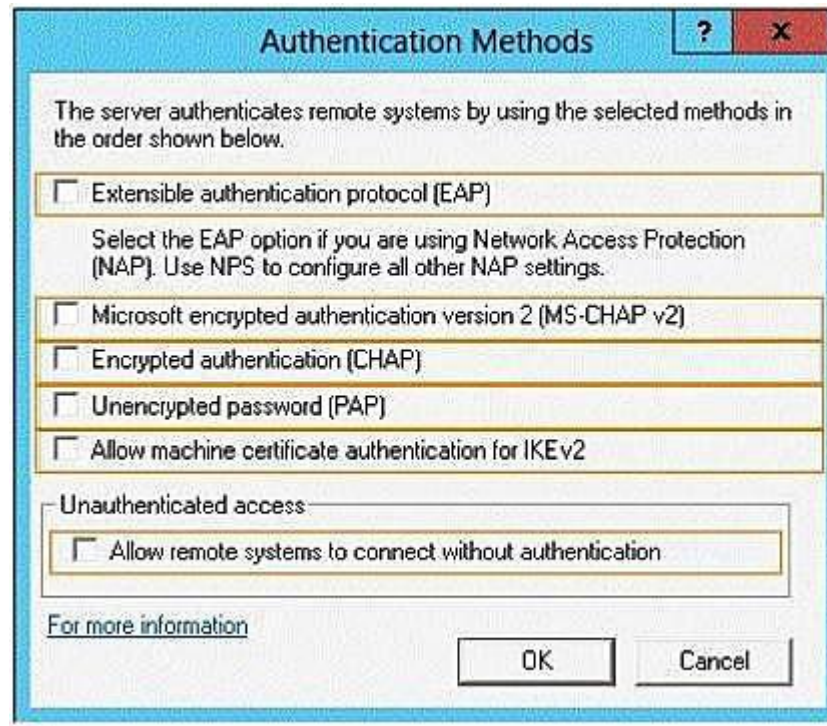
#### QUESTION 204

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Remote Access server role installed. You have a client named Client1 that is configured as an 802.1X supplicant.

You need to configure Server1 to handle authentication requests from Client1. The solution must minimize the number of authentication methods enabled on Server1.

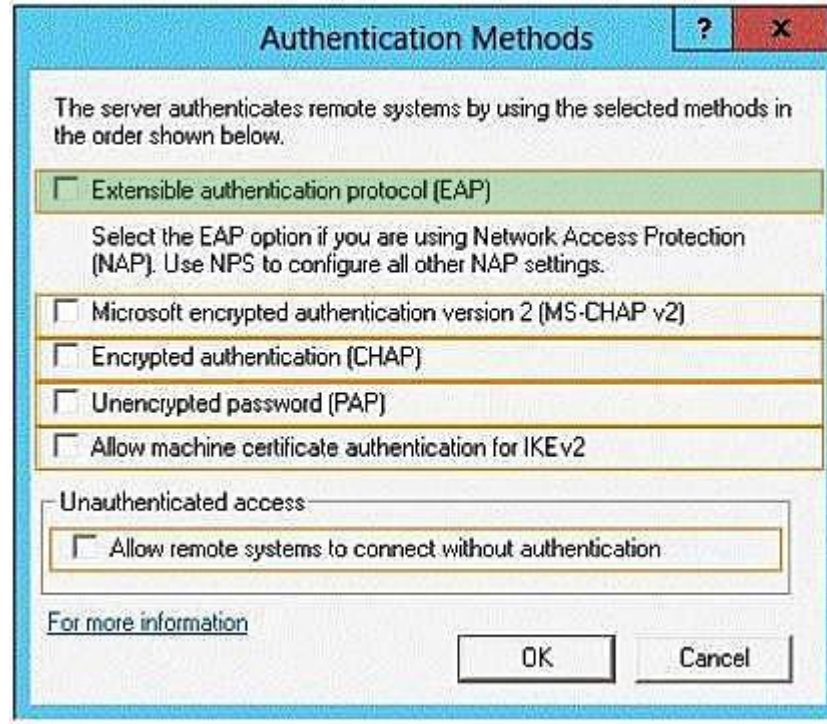
Which authentication method should you enable? To answer, select the appropriate authentication method in the answer area.

Hot Area:



Correct Answer:





### Section: Configure a Network Policy Server (NPS) infrastructure

#### Explanation

#### Explanation/Reference:

Extensible Authentication Protocol (EAP) extends Point-to-Point Protocol (PPP) by allowing arbitrary authentication methods that use credential and information exchanges of arbitrary lengths. EAP was developed in response to demand for authentication methods that use security devices, such as smart cards, token cards, and crypto calculators. EAP provides an industry-standard architecture for supporting additional authentication methods within PPP.

Using EAP, you can support additional authentication schemes, known as EAP types. These schemes include token cards, one-time passwords, public key authentication using smart cards, and certificates. EAP, in conjunction with strong EAP types, is a critical technology component for secure virtual private network (VPN) connections, 802.1X wired connections, and 802.1X wireless connections. Both the network access client and the authenticator, such as the NPS server, must support the same EAP type for successful authentication to occur.

<https://technet.microsoft.com/en-us/library/cc770622>

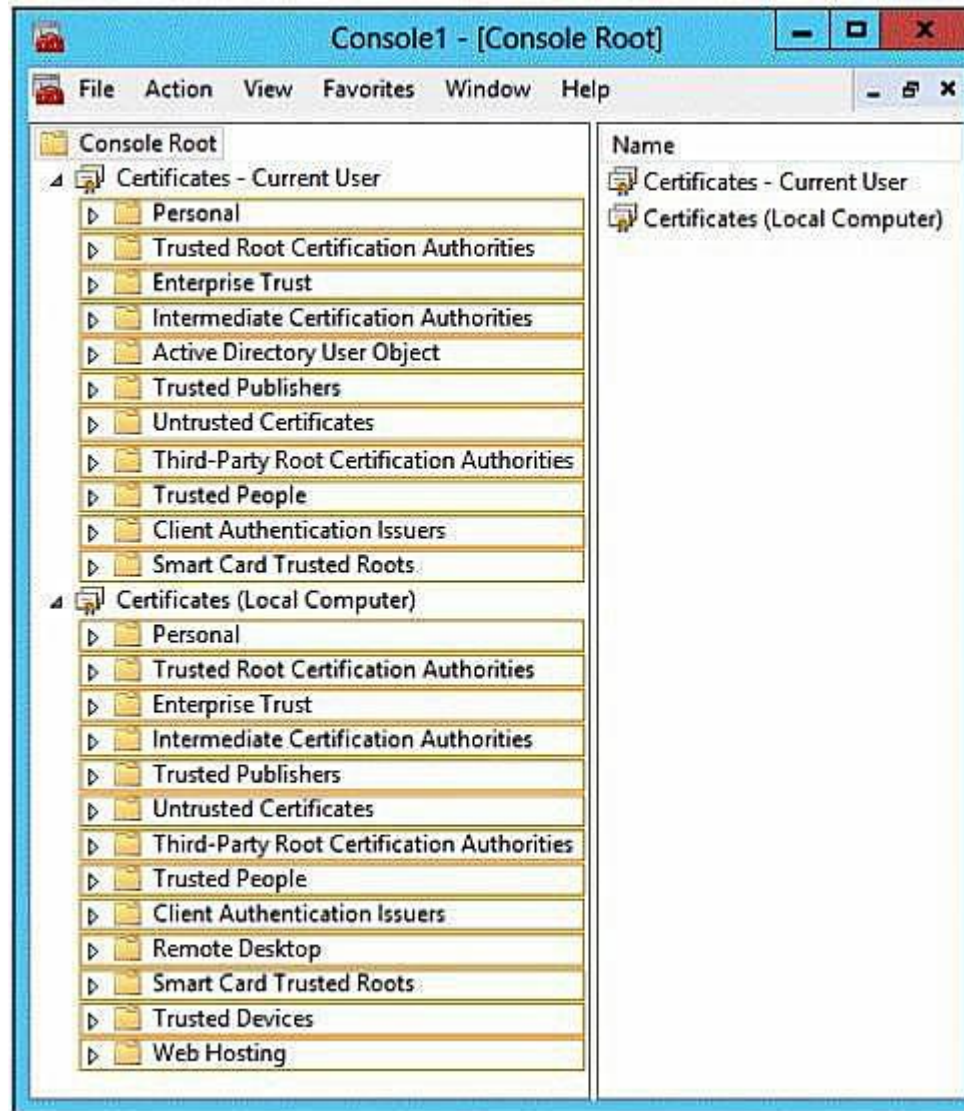
**QUESTION 205**

You have a server named Server1 that has the Network Policy and Access Services server role installed.

You plan to configure Network Policy Server (NPS) on Server1 to use certificate-based authentication for VPN connections. You obtain a certificate for NPS. You need to ensure that NPS can perform certificate-based authentication.

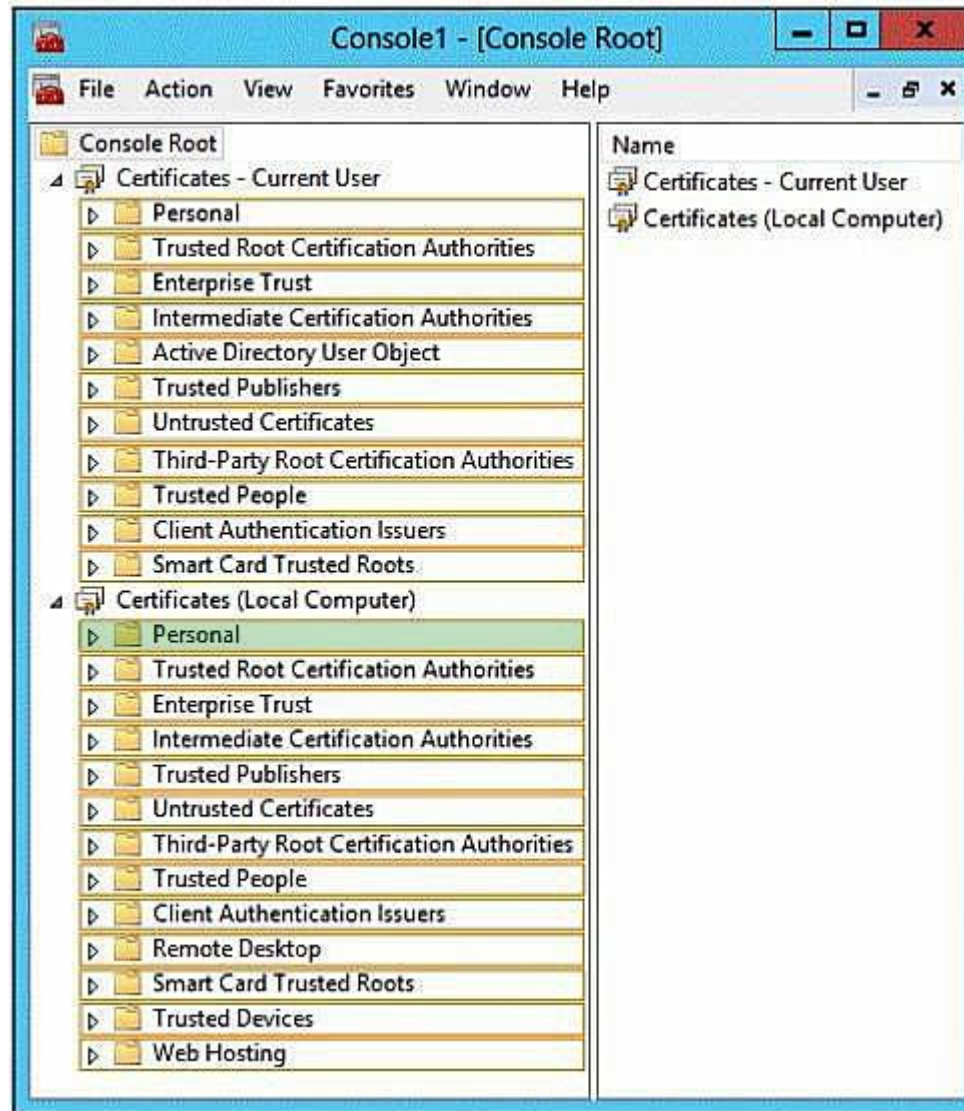
To which store should you import the certificate? To answer, select the appropriate store in the answer area.

**Hot Area:**



Correct Answer:





**Section: Configure a Network Policy Server (NPS) infrastructure**

**Explanation**

**Explanation/Reference:**

## Certificate store

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

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

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

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

<https://technet.microsoft.com/en-us/library/ee407543>

## QUESTION 206

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. A local account named Admin1 is a member of the Administrators group on Server1.

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

What should you run?

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

**Correct Answer: B**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**Auditpol.exe /set**

Sets the per-user audit policy, system audit policy, or auditing options.

## Syntax

```
Auditpol /set  
[/user[:<username>|<{sid}>][ /include][ /exclude]]  
[/category:<name>|<{guid}>[, :<name|<{guid}>...]]  
[/success:<enable>|<disable>][ /failure:<enable>|<disable>]
```

## Parameters

/user

The security principal for whom the per-user audit policy specified by the category or subcategory is set. Either the category or subcategory option must be specified, as a security identifier (SID) or name.

/category

One or more audit categories specified by globally unique identifier (GUID) or name. If no user is specified, the system policy is set.

/success

Specifies success auditing. This setting is the default and is automatically applied if neither the /success nor /failure parameters are explicitly specified. This setting must be used with a parameter indicating whether to enable or disable the setting.

/failure

Specifies failure auditing. This setting must be used with a parameter indicating whether to enable or disable the setting.

## Example

To set the per-user audit policy for all subcategories under the Detailed Tracking category for the user mikedan so that all the user's successful attempts will be audited, type:

```
Auditpol /set /user:mikedan /category:"Detailed Tracking" /success:enable
```

<https://technet.microsoft.com/en-us/library/cc755264.aspx>

**/resourceSACL** (applies to the two wrong answer options)

Configures global resource system access control lists (SACLs).

**Note:** Applies only to Windows 7 and Windows Server 2008 R2.

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

## QUESTION 207

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: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

Applies To: Windows Server 2008

The Active Directory database mounting tool makes it possible for deleted AD DS or Active Directory Lightweight Directory Services (AD LDS) data to be preserved in the form of snapshots of AD DS that are taken by the Volume Shadow Copy Service (VSS). The tool does not actually recover the deleted objects and containers. The administrator must perform data recovery as a subsequent step.

You can use a Lightweight Directory Access Protocol (LDAP) tool such as Ldp.exe, which is a tool that is built into Windows Server 2008, to view the data that is exposed in the snapshots. This data is read-only data.

<https://technet.microsoft.com/en-us/library/cc753246>

**Note:** *The above explanation is for the MOST correct answer option available, but references an obsolete procedure. A more correct process, but not available as an answer option, is explained below.*

Applies To: Windows Server 2012

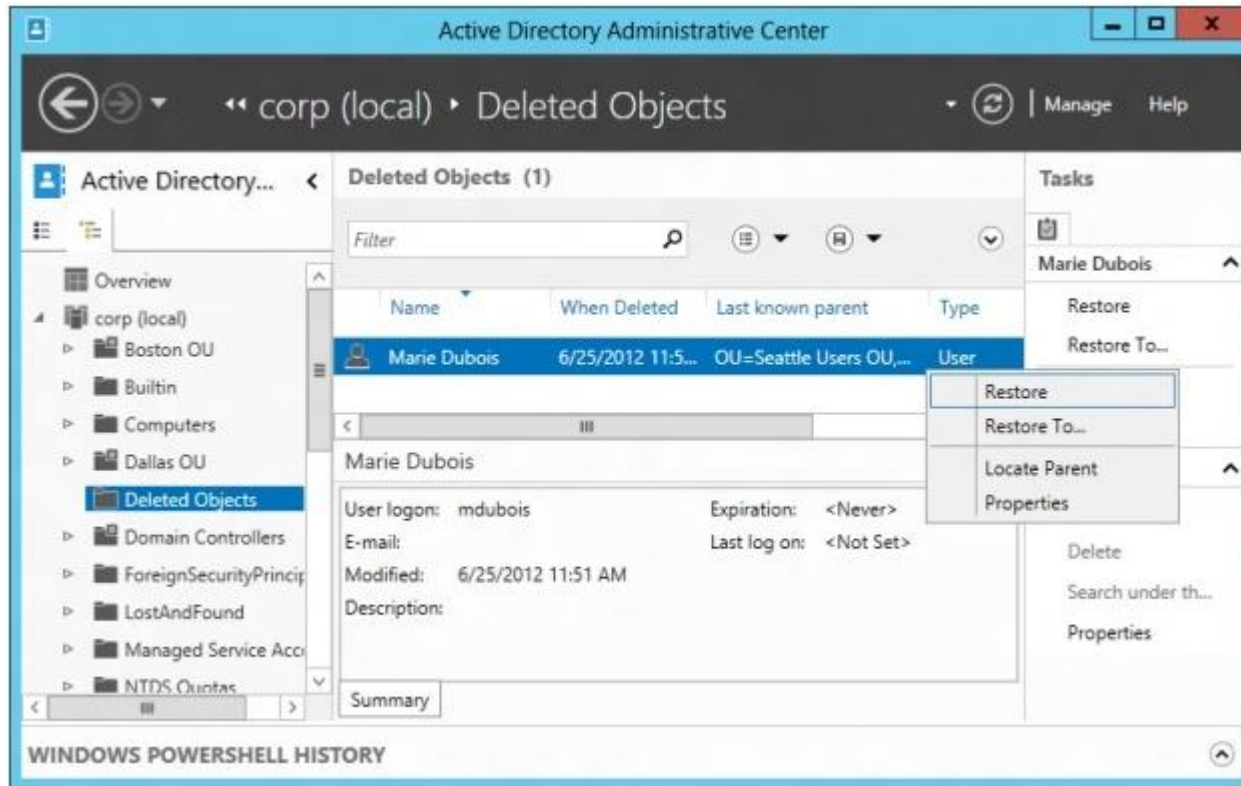
In Windows Server 2008, you could use the Windows Server Backup feature and **ntdsutil** authoritative restore command to mark objects as authoritative to ensure that the restored data was replicated throughout the domain. The drawback to the authoritative restore solution was that it had to be performed in Directory Services Restore Mode (DSRM). During DSRM, the domain controller being restored had to remain offline. Therefore, it was not able to service client requests.

In Windows Server 2003 Active Directory and Windows Server 2008 AD DS, you could recover deleted Active Directory objects through tombstone reanimation. However, reanimated objects' link-valued attributes (for example, group memberships of user accounts) that were physically removed and

non-link-valued attributes that were cleared were not recovered. Therefore, administrators could not rely on tombstone reanimation as the ultimate solution to accidental deletion of objects.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion.

In Windows Server 2012, the Active Directory Recycle Bin feature has been enhanced with a new graphical user interface for users to manage and restore deleted objects. Users can now visually locate a list of deleted objects and restore them to their original or desired locations.



<https://technet.microsoft.com/en-us/library/hh831702.aspx>

#### QUESTION 208

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: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

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 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, but it does not have to be running on a hypervisor.

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

#### QUESTION 209

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

2008 R2.

You deploy a new domain controller named DC1 that runs Windows Server 2012 R2. You log on to DC1 by using an account that is a member of the Domain Admins group. You discover that you cannot create Password Settings objects (PSOs) by using Active Directory Administrative Center. You need to ensure that you can create PSOs from Active Directory Administrative Center.

What should you do?

- A. Modify the membership of the Group Policy Creator Owners group.
- B. Transfer the PDC emulator operations master role to DC1.
- C. Upgrade all of the domain controllers that run Window Server 2008.
- D. Raise the functional level of the domain.

**Correct Answer: D**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

Fine-grained password policies apply only global security groups and user objects. By default, only members of the Domain Admins group can set fine-grained password policies. However, you can also delegate the ability to set these policies to other users. The domain functional level must be Windows Server 2008 or higher.

<https://technet.microsoft.com/en-us/library/hh831702.aspx>

#### **QUESTION 210**

Your network contains an Active Directory forest named contoso.com. The functional level of the forest is Windows Server 2008 R2. All of the user accounts in the marketing department are members of a group named Contoso\MarketingUsers. All of the computer accounts in the marketing department are members of a group named Contoso\MarketingComputers.

A domain user named User1 is a member of the Contoso\MarketingUsers group. A computer named Computer1 is a member of the Contoso\MarketingComputers group. You have five Password Settings objects (PSOs). The PSOs are defined as shown in the following table.

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

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

What should you tell User1?

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

**Correct Answer: A**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

If multiple PSOs are linked to a user or group, the resultant PSO that is applied is determined as follows:

1. A PSO that is linked directly to the user object is the resultant PSO. (Multiple PSOs should not be directly linked to a user object.)
2. If no PSO is linked directly to the user object, the global security group memberships of the user, and all PSOs that are applicable to the user based on those global group memberships, are compared. The PSO with the lowest precedence value is the resultant PSO.
3. If no PSO is obtained from conditions (1) and (2), the Default Domain Policy is applied.

<https://technet.microsoft.com/en-us/library/cc770394>



**QUESTION 211**

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: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**Introduction to Active Directory Administrative Center Enhancements**

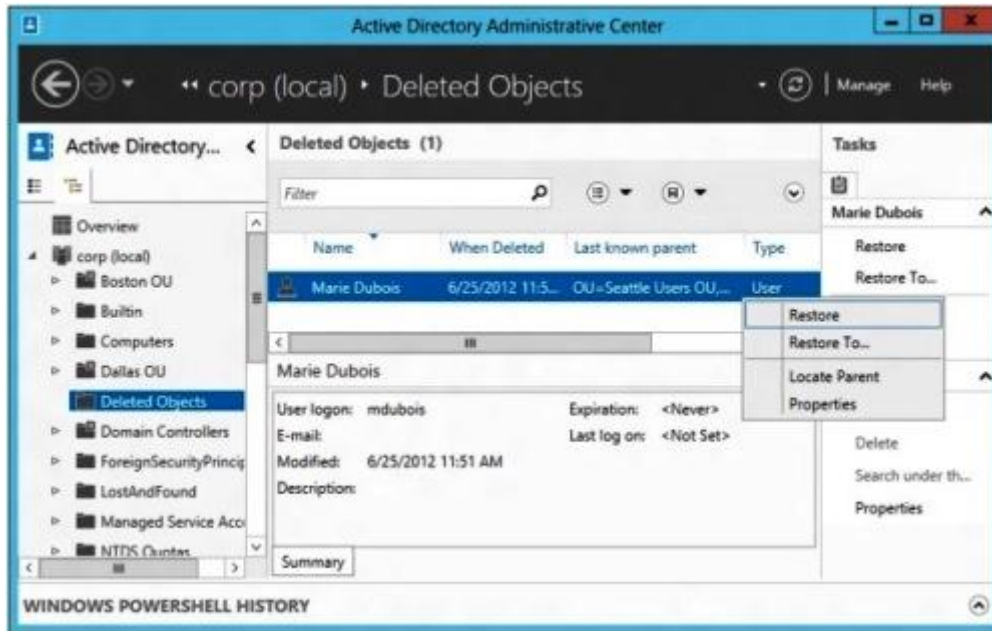
Applies To: Windows Server 2012

In Windows Server 2008, you could use the Windows Server Backup feature and **ntdsutil** authoritative restore command to mark objects as authoritative to ensure that the restored data was replicated throughout the domain. The drawback to the authoritative restore solution was that it had to be performed in Directory Services Restore Mode (DSRM). During DSRM, the domain controller being restored had to remain offline. Therefore, it was not able to service client requests.

In Windows Server 2003 Active Directory and Windows Server 2008 AD DS, you could recover deleted Active Directory objects through tombstone reanimation. However, reanimated objects' link-valued attributes (for example, group memberships of user accounts) that were physically removed and non-link-valued attributes that were cleared were not recovered. Therefore, administrators could not rely on tombstone reanimation as the ultimate solution to accidental deletion of objects.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion.

In Windows Server 2012, the Active Directory Recycle Bin feature has been enhanced with a new graphical user interface for users to manage and restore deleted objects. Users can now visually locate a list of deleted objects and restore them to their original or desired locations.



<https://technet.microsoft.com/en-us/library/hh831702.aspx>

#### QUESTION 212

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 is Recycled attribute of Group1.
- C. Perform tombstone reanimation.
- D. Perform an authoritative restore.

**Correct Answer: D**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

Logic: No Active Directory object has been deleted. One Active Directory object, a group named Group1, has had its membership altered. So, the Active Directory Recycle Bin will not contain a copy of the unaltered group. An authoritative restore from a snapshot made previous to the group's membership alteration is necessary to restore the state of the group.

#### **authoritative restore**

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

This is a subcommand of Ntdsutil and Dsdbutil. Ntdsutil and Dsdbutil are command-line tools that are built into Windows Server 2008 and Windows Server 2008 R2.

<https://technet.microsoft.com/en-us/library/cc732211.aspx>

#### **QUESTION 213**

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

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

What should you do?

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

**Correct Answer: C**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

To specify the delegated RODC administrator after installation, you can use either of the following options:

- Modify the **Managed By** tab of the RODC account properties in the Active Directory Users and Computers snap-in, as shown in the following figure. You can click **Change** to change which security principal is the delegated RODC administrator. You can choose only one security principal. Specify a security group rather than an individual user so you can control RODC administration permissions most efficiently. This method changes the **managedBy** attribute of the computer object that corresponds to the RODC to the SID of the security principal that you specify. This is the recommended way to specify the delegated RODC administrator account because the information is stored in AD DS, where it can be centrally managed by domain administrators.



- Use the **ntdsutil local roles** command or the **dsmanagement local roles** command. You can use this command to view, add, or remove members from the Administrators group and other built-in groups on the RODC.

Using **ntdsutil** or **dsmanagement** to specify the delegated RODC administrator account is not recommended because the information is stored only locally on the RODC. Therefore, when you use **ntdsutil local roles** to delegate an administrator for the RODC, the account that you specify does not appear on the **Managed By** tab of the RODC account properties. As a result, using the Active Directory Users and Computers snap-in or a similar tool will not reveal that the RODC has a delegated administrator.

<https://technet.microsoft.com/en-us/library/cc755310>

#### QUESTION 214

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

You create an Active Directory snapshot of DC1 each day. You need to view the contents of an Active Directory snapshot from two days ago.

What should you do first?

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

**Correct Answer: D**

**Section: Configure and manage Active Directory**  
**Explanation**

#### Explanation/Reference:

Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). You can use the **ntdsutil** commands to perform database maintenance of AD DS, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.

A sampling of ntdsutil sub-commands:

**authoritative restore** – Authoritatively restores the Active Directory database or AD LDS instance.

**DS behavior** – Views and modifies AD DS or AD LDS behavior.

**snapshot** – Manages snapshots of the volumes that contain the Active Directory database and log files.

<https://technet.microsoft.com/en-us/library/cc753343.aspx>

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

The file path to the database file must point to the database file, which might be on read-only media, such as a mounted snapshot; in a backup; or on another server, such as a domain controller or an AD LDS server. The database must be in a consistent state; that is, the Extensible Storage Engine (ESE) logs must be replayed. If you run the **Ntdsutil snapshot** subcommand or if you run Windows Server Backup on a server running Windows Server 2008, the resulting snapshot or backup will be in a consistent state.

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

### QUESTION 215

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: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**Staged installation.** This is a new installation method that is specifically designed to make it easier to deploy RODCs in remote locations. This new method does not require a member of the Domain Admins group to complete the installation in the remote location. You can delegate the installation to any domain user.

Staged installation is designed specifically to help you deploy RODCs to remote branch offices by separating the RODC installation process into two stages.

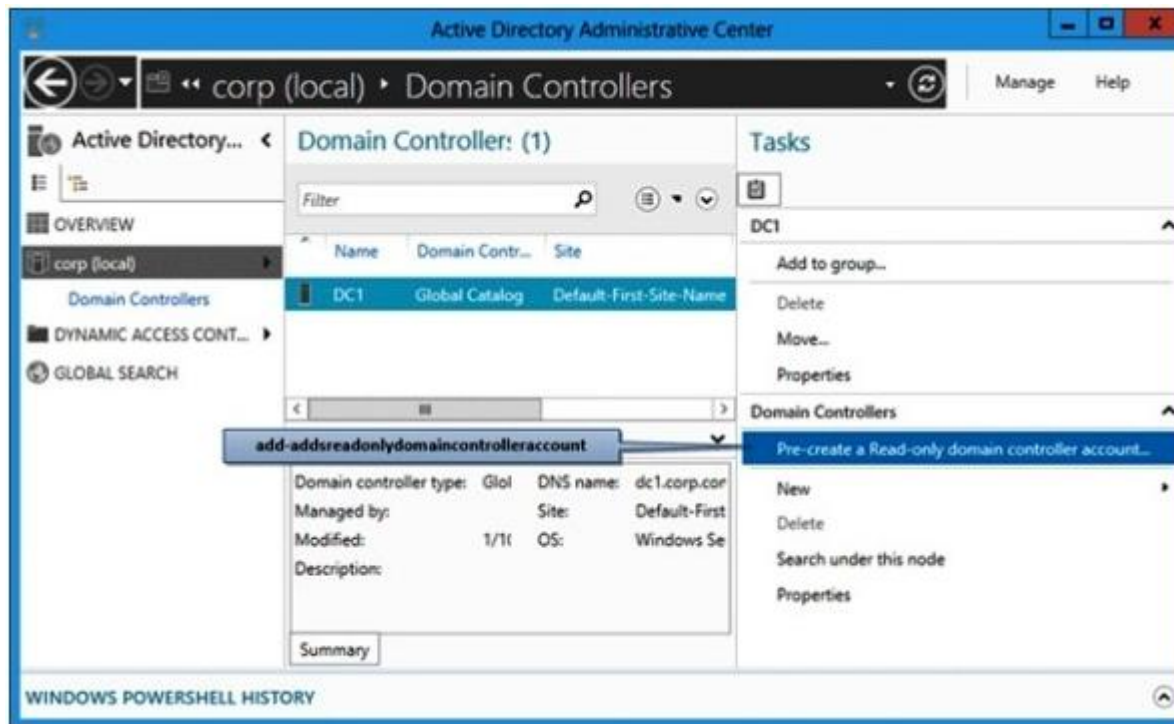
1. A Domain Admin creates a computer account for the RODC and (as an option) delegates a user or group the ability perform the second stage of the installation and be the server administrator for the RODC after the installation is complete. A Domain Admin will typically complete this stage in a central

location, such as a datacenter or hub site.

2. The delegated RODC server administrator joins the server to the RODC account that the Domain Admin created for it. A staged AD DS installation makes it unnecessary to use a highly privileged Domain Admin account in the branch office to complete the installation of AD DS. The delegated RODC server administrator will typically complete this stage in branch office where the organization plans to deploy the RODC.

<https://technet.microsoft.com/en-us/library/cc731970>

You perform the staging operation of a read-only domain controller computer account by opening the Active Directory Administrative Center (**Dsac.exe**). Click the name of the domain in the navigation pane. Double-click **Domain Controllers** in the management list. Click **Pre-create a Read-only domain controller account** in the tasks pane.



<https://technet.microsoft.com/en-us/library/jj574152.aspx>

#### QUESTION 216

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.

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: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

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 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, but it does not have to be running on a hypervisor.

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

**QUESTION 217**



Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2003, Windows Server 2008 R2, or Windows Server 2012 R2.

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

Which tool should you use?

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

**Correct Answer: C**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

You can use Ldp.exe to restore a single, deleted Active Directory object.

<https://technet.microsoft.com/nl-nl/library/dd379509>

LDP is a Windows Explorer-like utility for working with Active Directory. LDP was originally designed by the Active Directory development team to test its LDAP code while Active Directory was under development. Now part of the Windows Server 2003 Support tools, LDP has evolved into a robust tool for working with Active Directory.

Even though tombstones are invisible to normal directory operations, you can find tombstone objects in Active Directory using LDAP search operations and special LDAP extensions called controls. Controls are a mechanism, defined in the LDAP standard, used to extend the LDAP protocol to provide additional functionality beyond what is defined in the LDAP standard while remaining compatible with other LDAP-compliant software. Active Directory supports 22 controls, including the Return Deleted Objects control. When used to extend an LDAP search operation, this control retrieves deleted objects that would otherwise be invisible.

<https://technet.microsoft.com/en-us/magazine/2007.09.tombstones.aspx>

In Windows Server 2003 Active Directory and Windows Server 2008 AD DS, you could recover deleted Active Directory objects through tombstone reanimation. In Windows Server 2003 and Windows Server 2008, a deleted Active Directory object was not physically removed from the database immediately. Instead, the object's distinguished name (also known as DN) was mangled, most of the object's non-link-valued attributes were cleared, all of the object's link-valued attributes were physically removed, and the object was moved to a special container in the object's naming context (also known as NC) named Deleted Objects. The object, now called a tombstone, became invisible to normal directory operations. Tombstones could be reanimated anytime within the tombstone lifetime period and become live Active Directory objects again. The default tombstone lifetime was 180 days in Windows Server 2003 and Windows Server 2008. You could use tombstone reanimation to recover deleted objects without taking your domain controller or your AD LDS instance offline. However, reanimated objects' link-valued attributes (for example, group memberships of user accounts) that were physically removed and non-link-valued attributes that were cleared were not recovered. Therefore, administrators could not rely on tombstone

reanimation as the ultimate solution to accidental deletion of objects.

<https://technet.microsoft.com/en-us/library/dd391916>

### Active Directory Administrative Center Enhancements

In Windows Server 2012, the Active Directory Recycle Bin feature has been enhanced with a new graphical user interface for users to manage and restore deleted objects. Users can now visually locate a list of deleted objects and restore them to their original or desired locations.

<https://technet.microsoft.com/en-us/library/hh831702.aspx>

### QUESTION 218

Your network contains an Active Directory domain named contoso.com. The domain contains an Organizational Unit (OU) named IT and an OU named Sales. All of the help desk user accounts are located in the IT OU. All of the sales user accounts are located in the Sales OU. The Sales OU contains a global security group named G\_Sales. The IT OU contains a global security group named G\_HelpDesk.

You need to ensure that members of G\_HelpDesk can perform the following tasks:

- Reset the passwords of the sales users.
- Force the sales users to change their password at their next logon.

What should you do?

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

**Correct Answer: B**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

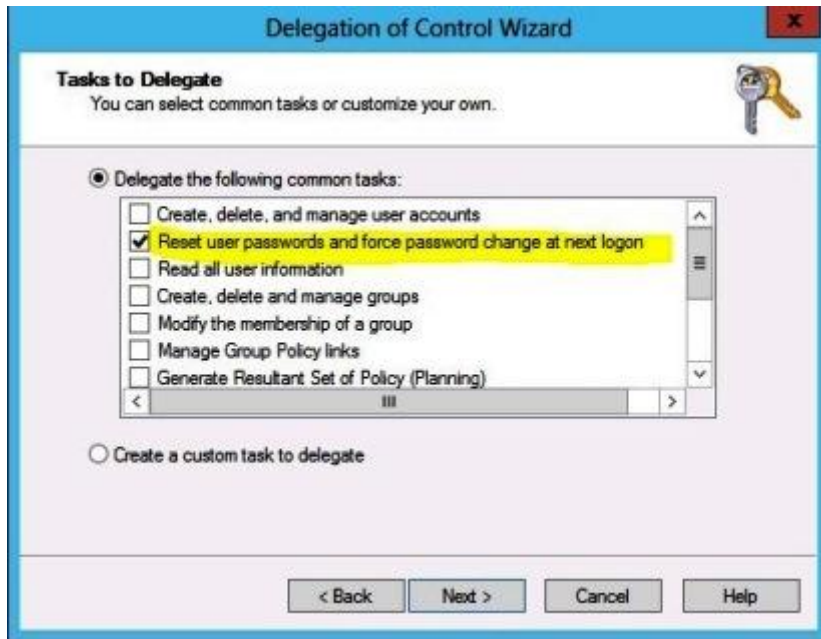
To delegate control of an organizational unit

1. To open Active Directory Users and Computers, click **Start** , click **Control Panel** , double-click **Administrative Tools** , and then double-click **Active Directory Users and Computers**.

To open Active Directory Users and Computers in Windows Server® 2012, click **Start** , type **dsa.msc**.

2. In the console tree, right-click the organizational unit (OU) **for which you want to delegate control**. In the case of this question, it will be the Sales OU.

3. Click **Delegate Control** to start the Delegation of Control Wizard, and then follow the instructions in the wizard.



<https://technet.microsoft.com/en-us/library/cc732524.aspx>

### QUESTION 219

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.

**Correct Answer: C**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

Any incompatible program or service not uninstalled or added to the **CustomDCCloneAllowList.xml** prevents cloning.

The **CustomDCCloneAllowList.xml** file is optional unless you install applications or potentially incompatible Windows services on the source domain controller. The files require precise naming, formatting, and placement; otherwise, cloning fails.

The following locations can contain the **CustomDCCloneAllowList.xml** file:

1. HKey\_Local\_Machine\System\CurrentControlSet\Services\NTDS\Parameters  
AllowListFolder (*REG\_SZ*)
2. DSA Working Directory
3. %windir%\NTDS
4. Removable read/write media, in order of drive letter, at the root of the drive

<https://technet.microsoft.com/en-us/library/jj574223.aspx>

#### **QUESTION 220**

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?

**Exhibit:**

The image shows the 'User1 Properties' dialog box with the 'General' tab selected. The tabs at the top are: Member Of, Dial-in, Environment, Sessions, Remote control, Remote Desktop Services Profile, and CDM+. The 'General' tab contains a user icon and the name 'User1'. Below this are input fields for: First name, Initials, Last name, Display name, Description, Office, Telephone number (with an 'Other...' button), E-mail, and Web page (with an 'Other...' button). At the bottom are buttons for OK, Cancel, Apply, and Help.

- 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**

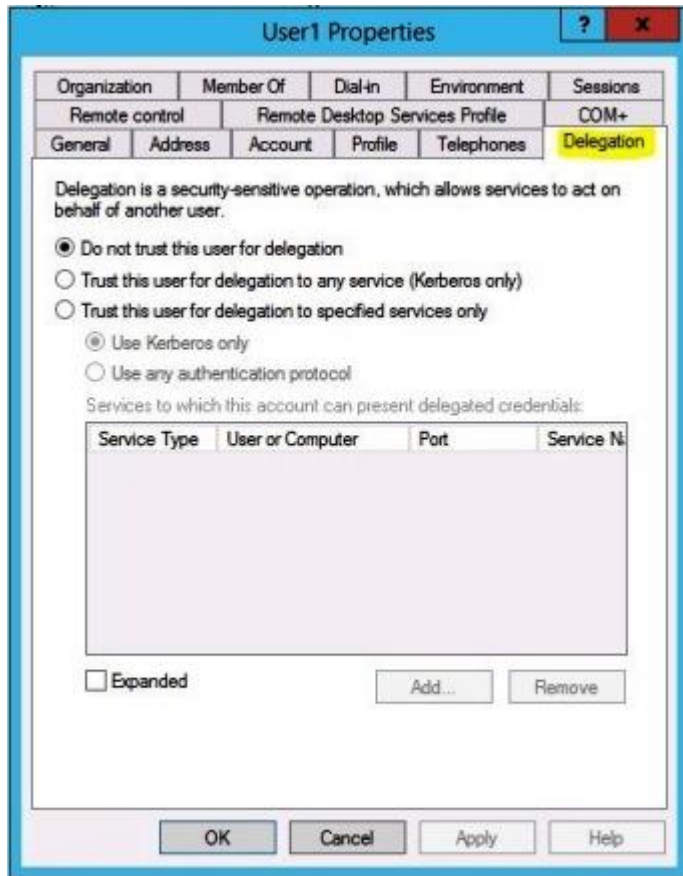
**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

If you cannot see the **Delegation** tab... 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.



<https://technet.microsoft.com/en-us/library/cc757194>

#### QUESTION 221

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: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

If you plan to use fine-grained password policies in Windows Server 2012, consider the following:

- Fine-grained password policies apply only global security groups and user objects (or inetOrgPerson objects if they are used instead of user objects). By default, only members of the Domain Admins group can set fine-grained password policies. However, you can also delegate the ability to set these policies to other users. The domain functional level must be Windows Server 2008 or higher.
- You must use the Windows Server 2012 version of Active Directory Administrative Center to administer fine-grained password policies through a graphical user interface.

<https://technet.microsoft.com/en-us/library/hh831702.aspx>

#### **QUESTION 222**

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

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

All client computers run Windows 8 Enterprise.

You plan to deploy Network Access Protection (NAP) by using IPsec enforcement. A Group Policy object (GPO) named GPO1 is configured to deploy a trusted server group to all of the client computers. You need to ensure that the client computers can discover HRA servers automatically.

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

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

**Correct Answer:** ABE

**Section:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

#### **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.

<https://technet.microsoft.com/en-us/library/dd296901.aspx>

#### **QUESTION 223**

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: B**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**Folder Redirection** lets administrators redirect the path of a folder to a new location. The location can be a folder on the local computer or a directory on a network file share. Users can work with documents on a server as if the documents were based on a local drive. The documents in the folder are available to the user from any computer on the network. Folder Redirection is located under **Windows Settings** in the console tree when you edit domain-based Group Policy by using the Group Policy Management Console (GPMC). The path is **[Group Policy Object Name]\User Configuration\Policies\Windows Settings\Folder Redirection**.

<https://technet.microsoft.com/en-us/library/cc732275.aspx>

**Folder Redirection** and Offline Files are used together to redirect the path of local folders (such as the Documents folder) to a network location, while caching the contents locally for increased speed and availability. Roaming User Profiles is used to redirect a user profile to a network location.

- **Folder Redirection** enables users and administrators to redirect the path of a known folder to a new location, manually or by using Group Policy. The new location can be a folder on the local computer or a directory on a file share. Users interact with files in the redirected folder as if it still existed on the local drive. For example, you can redirect the Documents folder, which is usually stored on a local drive, to a network location. The files in the folder are then available to the user from any computer on the network.
- **Offline Files** makes network files available to a user, even if the network connection to the server is unavailable or slow. When working online, file access performance is at the speed of the network and server. When working offline, files are retrieved from the Offline Files folder at local access speeds.
- **Roaming User Profiles** redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers. When a user signs in to a computer by using an account that is set up with a file share as the profile path, the user's profile is downloaded to the local computer and merged with the local profile (if present). When the user signs out of the computer, the local copy of their profile, including any changes, is merged with the server copy of the profile.

<https://technet.microsoft.com/en-us/library/hh848267.aspx>

If you decide to use Roaming User Profiles across multiple versions of Windows, we recommend taking the following actions:

- Configure Windows to maintain separate profile versions for each operating system version. This helps prevent undesirable and unpredictable issues such as profile corruption.
- Use **Folder Redirection** to store user files such as documents and pictures outside of user profiles. This enables the same files to be available to users across operating system versions. It also keeps profiles small and sign-ins quick.
- Allocate sufficient storage for Roaming User Profiles. If you support two operating system versions, profiles will double in number (and thus total space consumed) because a separate profile is maintained for each operating system version.
- Don't use Roaming User Profiles across computers running Windows Vista/Windows Server 2008 and Windows 7/Windows Server 2008 R2. Roaming between these operating system versions isn't supported due to incompatibilities in their profile versions.
- Inform your users that changes made on one operating system version won't roam to another operating system version.
- When moving your environment to a new version of Windows users will receive a new, empty profile. There isn't a supported method of migrating user profiles from one operating system version to another.

<https://technet.microsoft.com/en-us/library/jj649079.aspx>

#### **QUESTION 224**

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:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

If you plan to use fine-grained password policies in Windows Server 2012, consider the following:

- Fine-grained password policies apply only **global security groups** and **user objects** (or inetOrgPerson objects if they are used instead of user objects). By default, only members of the Domain Admins group can set fine-grained password policies. However, you can also delegate the ability to set these policies to other users. The domain functional level must be Windows Server 2008 or higher.
- You must use the Windows Server 2012 version of Active Directory Administrative Center to administer fine-grained password policies through a graphical user interface.

<https://technet.microsoft.com/en-us/library/hh831702.aspx>

### QUESTION 225

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?

- In GPO1, configure the Advanced Audit Policy Configuration settings for Audit User Account Management. Link GPO1 to the Domain Controllers organizational unit (OU).
- 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.
- In GPO1, configure the Advanced Audit Policy Configuration settings for Audit Sensitive Privilege Use. Link GPO1 to the Domain Controllers organizational unit (OU).
- 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: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

#### **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.

<https://technet.microsoft.com/en-us/library/dd772693>

For a group Managed Service Account the Windows Server 2012 **domain controller** computes the password on the key provided by the Key Distribution Services in addition to other attributes of the group Managed Service Account. Windows Server 2012 and Windows 8 member hosts can obtain the current and preceding password values by contacting a Windows Server 2012 **domain controller**.

<https://technet.microsoft.com/en-us/library/hh831782.aspx>

#### QUESTION 226

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

You mount an Active Directory snapshot on DC1. You need to expose the snapshot as an LDAP server.

Which tool should you use?

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

**Correct Answer: C**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**Dsomain.exe** is a command-line tool that exposes Active Directory data that is stored in a snapshot or backup as a Lightweight Directory Access Protocol (LDAP) server. To use Dsomain, you must run the **dsomain** command from an elevated command prompt.

**Syntax:** dsamain /dbpath <filepath> /ldapPort <number>

/dbpath <filepath> specifies the file path to the database file. <filepath> must point to the database file, which might be on read-only media, such as a mounted snapshot; in a backup; or on another server, such as a domain controller or an AD LDS server.

/ldapPort <number> specifies the LDAP port value. Only the LDAP port is required. If you do not specify the other ports, they use LDAP+1, LDAP+2, and LDAP+3, respectively. For example, if you specify LDAP port 41389 without specifying other port values, the LDAP-SSL port uses port 41390 by default, and so on. You cannot specify ports that are currently in use. If you run the command on a domain controller, specify different ports than those that are used by the local domain controller.

The following example exposes the data in a snapshot \$SNAP\_200704181137 as an LDAP server, using LDAP port 51389:

```
dsamain /dbpath E:\$SNAP_200704181137_VOLUMED$\WINDOWS\NTDS\ntds.dit /ldapport 51389
```

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

#### QUESTION 227

Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2. You have a Password Settings object (PSOs) named PSO1.

You need to view the settings of PSO1.

Which tool should you use?

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

**Correct Answer: B**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

In Windows Server 2012, fine-grained password policy management is made easier and more visual by providing a user interface for AD DS administrators to manage them in ADAC. Administrators can now view a given user's resultant policy, view and sort all password policies within a given domain, and manage individual password policies visually.

If you plan to use fine-grained password policies in Windows Server 2012, consider the following:

Fine-grained password policies apply only global security groups and user objects (or inetOrgPerson objects if they are used instead of user objects). By default, only members of the Domain Admins group can set fine-grained password policies. However, you can also delegate the ability to set these policies to other users. The domain functional level must be Windows Server 2008 or higher.

You must use the Windows Server 2012 version of Active Directory Administrative Center to administer fine-grained password policies through a graphical user interface.

The screenshot displays the Active Directory Administrative Center interface. The breadcrumb navigation shows the path: home (local) > System > Password Settings Container. The main window is titled 'PSO1' and contains a 'Password Settings' tab. On the left, a sidebar lists 'Password Settings', 'Directly Applies To', and 'Extensions'. The 'Password Settings' section includes fields for 'Name' (PSO1) and 'Precedence' (4). It features several checkboxes: 'Enforce minimum password length' (checked, with a value of 7), 'Enforce password history' (checked, with a value of 24), 'Password must meet complexity requirements' (checked), and 'Protect from accidental deletion' (checked). The 'Store password using reversible encryption' checkbox is unchecked. The 'Password age options' section includes 'Enforce minimum password age' (checked, with a value of 1), 'Enforce maximum password age' (checked, with a value of 42), and 'Enforce account lockout policy' (unchecked). The lockout policy details show 'Number of failed logon attempts' (30) and 'Reset failed logon attempts counter' (30). The 'Account will be locked out' section has two radio buttons: 'For a duration of (mins):' (selected, with a value of 30) and 'Until an administrator manually unlocks' (unselected). The 'Directly Applies To' section shows a table with columns 'Name' and 'Mail', containing one entry: 'AdminOU-PRT'. 'Add...' and 'Remove' buttons are located at the bottom right of this section.

[https://technet.microsoft.com/en-us/library/hh831702.aspx#fine\\_grained\\_pswd\\_policy\\_mgmt](https://technet.microsoft.com/en-us/library/hh831702.aspx#fine_grained_pswd_policy_mgmt)

**QUESTION 228**

Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. A domain controller named DC1 runs Windows Server 2012 R2. DC1 is backed up daily.

During routine maintenance, you delete a group named Group1. You need to recover Group1 and identify the names of the users who were members of Group1 prior to its deletion. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do first?

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

**Correct Answer: B**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

Applies To: Windows Server 2008

The Active Directory database mounting tool makes it possible for deleted AD DS or Active Directory Lightweight Directory Services (AD LDS) data to be preserved in the form of snapshots of AD DS that are taken by the Volume Shadow Copy Service (VSS). The tool does not actually recover the deleted objects and containers. The administrator must perform data recovery as a subsequent step.

You can use a Lightweight Directory Access Protocol (LDAP) tool such as Ldp.exe, which is a tool that is built into Windows Server 2008, to view the data that is exposed in the snapshots. This data is read-only data.

<https://technet.microsoft.com/en-us/library/cc753246>

**Note:** *The above explanation is for the MOST correct answer option available, but references an obsolete procedure. A more correct process, but not available as an answer option, is explained below.*

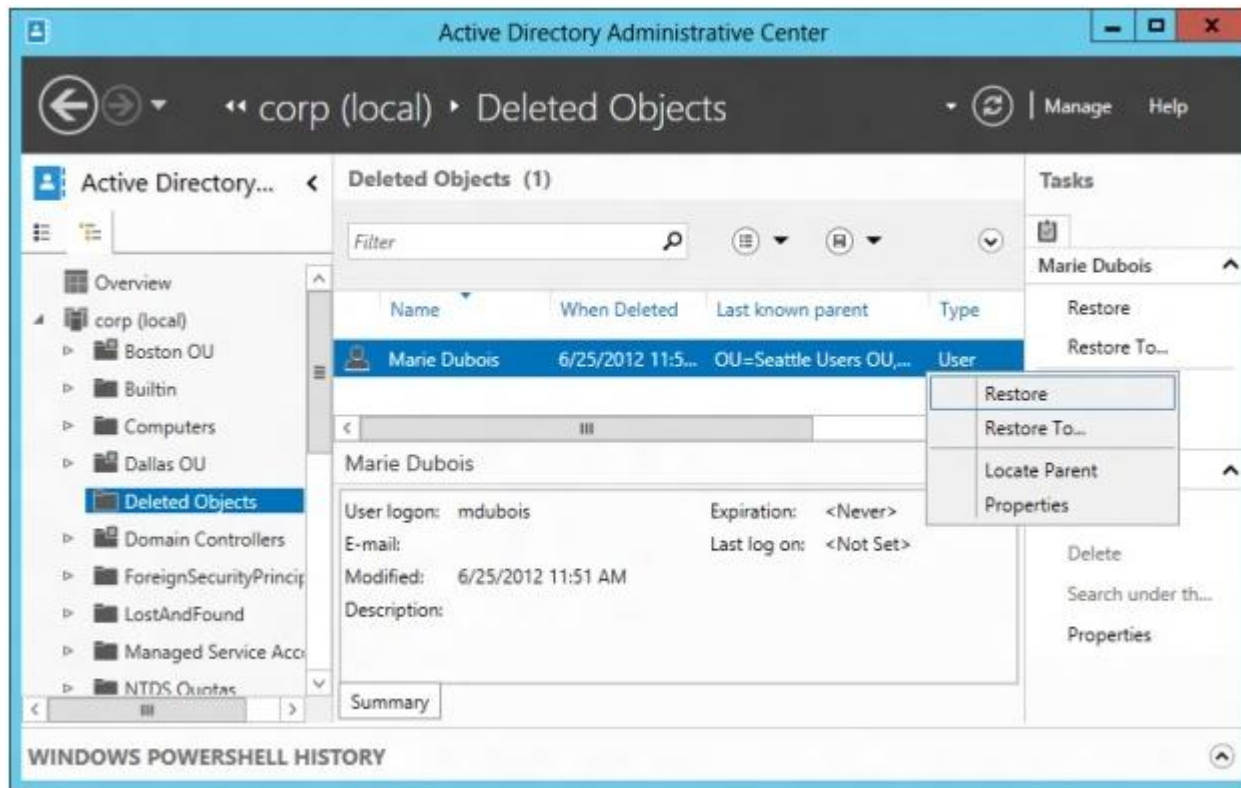
Applies To: Windows Server 2012

In Windows Server 2008, you could use the Windows Server Backup feature and **ntdsutil** authoritative restore command to mark objects as authoritative to ensure that the restored data was replicated throughout the domain. The drawback to the authoritative restore solution was that it had to be performed in Directory Services Restore Mode (DSRM). During DSRM, the domain controller being restored had to remain offline. Therefore, it was not able to service client requests.

In Windows Server 2003 Active Directory and Windows Server 2008 AD DS, you could recover deleted Active Directory objects through tombstone reanimation. However, reanimated objects' link-valued attributes (for example, group memberships of user accounts) that were physically removed and non-link-valued attributes that were cleared were not recovered. Therefore, administrators could not rely on tombstone reanimation as the ultimate solution to accidental deletion of objects.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion.

In Windows Server 2012, the Active Directory Recycle Bin feature has been enhanced with a new graphical user interface for users to manage and restore deleted objects. Users can now visually locate a list of deleted objects and restore them to their original or desired locations.



<https://technet.microsoft.com/en-us/library/hh831702.aspx>

#### QUESTION 229

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



virtual machine named DC2.

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

Name	Type
App1	Service

You need to ensure that you can clone DC2.

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

- A. Create an empty file named DCCloneConfig.xml.
- B. Add the following information to the DCCloneConfigSchema.xsd file:

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

- C. Create an empty file named CustomDCCloneConfig.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>
```

**Correct Answer: AE**

## Section: Configure and manage Active Directory

### Explanation

#### Explanation/Reference:

**DCCloneConfig.xml** – To successfully clone a virtualized domain controller, this file must be present in the directory where the DIT resides, *%windir%\NTDS*, or the root of a removable media drive. Besides being used as one of the triggers to detect and initiate cloning, it also provides a means to specify configuration settings for the clone domain controller.

The schema and a sample file for the DCCloneConfig.xml file are stored on all Windows Server 2012 computers at:

- *%windir%\system32\DCCloneConfigSchema.xsd*
- *%windir%\system32\SampleDCCloneConfig.xml*

It is recommended that you use the New-ADDCCloneConfigFile cmdlet to create the DCCloneConfig.xml file. Although you could also use the schema file with an XML-aware editor to create this file, manually editing the file increases the likelihood of errors. If you edit the file, it must be done by using XML-aware editors, such as Visual Studio, XML Notepad, or third-party applications (do not use Notepad).

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

Any incompatible program or service not uninstalled or added to the **CustomDCCloneAllowList.xml** prevents cloning.

The **CustomDCCloneAllowList.xml** file is optional unless you install applications or potentially incompatible Windows services on the source domain controller. The files require precise naming, formatting, and placement; otherwise, cloning fails.

The following locations can contain the **CustomDCCloneAllowList.xml** file:

1. HKey\_Local\_Machine\System\CurrentControlSet\Services\NTDS\Parameters  
AllowListFolder (*REG\_SZ*)
2. DSA Working Directory
3. *%windir%\NTDS*
4. Removable read/write media, in order of drive letter, at the root of the drive

<https://technet.microsoft.com/en-us/library/jj574223.aspx>

### QUESTION 230

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

Domain Controller Name	Operating system	Operation master role
DC1	Windows Server 2008	PDC emulator Infrastructure master RID master
DC2	Windows Server 2008 R2	Schema master Domain naming master

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

What should you do?

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

**Correct Answer: A**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

Fine-grained password policies apply only global security groups and user objects. By default, only members of the Domain Admins group can set fine-grained password policies. However, you can also delegate the ability to set these policies to other users. The domain functional level must be Windows Server 2008 or higher.

<https://technet.microsoft.com/en-us/library/hh831702.aspx>

#### **QUESTION 231**

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:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

#### **Audit Policy\Audit object access**

This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.

You can configure this security setting by opening the appropriate policy and expanding the console tree as such:  
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\

<https://technet.microsoft.com/en-us/library/cc776774>

#### **Advanced Audit Policy Configuration\Object Access**

Object Access policy settings and audit events allow you to track attempts to access specific objects or types of objects on a network or computer. To audit attempts to access a file, directory, registry key, or any other object, you must enable the appropriate Object Access auditing subcategory for success and/or failure events.

<https://technet.microsoft.com/en-us/library/dd772646>

- Audit File Share

This security policy setting determines whether the operating system generates audit events when a file share is accessed.

Audit events are not generated when shares are created, deleted, or when share permissions change.

Combined with File System auditing, File Share auditing allows you to track what content was accessed, the source (IP address and port) of the request, and the user account used for the access.

<https://technet.microsoft.com/en-us/library/dd772690>

- Audit File System

This security policy setting determines whether the operating system audits user attempts to access file system objects. Audit events are only generated for objects that have configured system access control lists (SACLs), and only if the type of access requested (such as Write, Read, or Modify) and the account making the request match the settings in the SACL.

If success auditing is enabled, an audit entry is generated each time any account successfully accesses a file system object that has a matching SACL. If failure auditing is enabled, an audit entry is generated each time any user unsuccessfully attempts to access a file system object that has a matching SACL.

These events are essential for tracking activity for file objects that are sensitive or valuable and require extra monitoring.

<https://technet.microsoft.com/en-us/library/dd772661>

#### QUESTION 232

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.

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:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

If multiple PSOs are linked to a user or group, the resultant PSO that is applied is determined as follows:

1. A PSO that is linked directly to the user object is the resultant PSO. (Multiple PSOs should not be directly linked to a user object.)
2. If no PSO is linked directly to the user object, the global security group memberships of the user, and all PSOs that are applicable to the user based on those global group memberships, are compared. The PSO with the lowest precedence value is the resultant PSO.
3. If no PSO is obtained from conditions (1) and (2), the Default Domain Policy is applied.

<https://technet.microsoft.com/en-us/library/cc770394>

### **QUESTION 233**

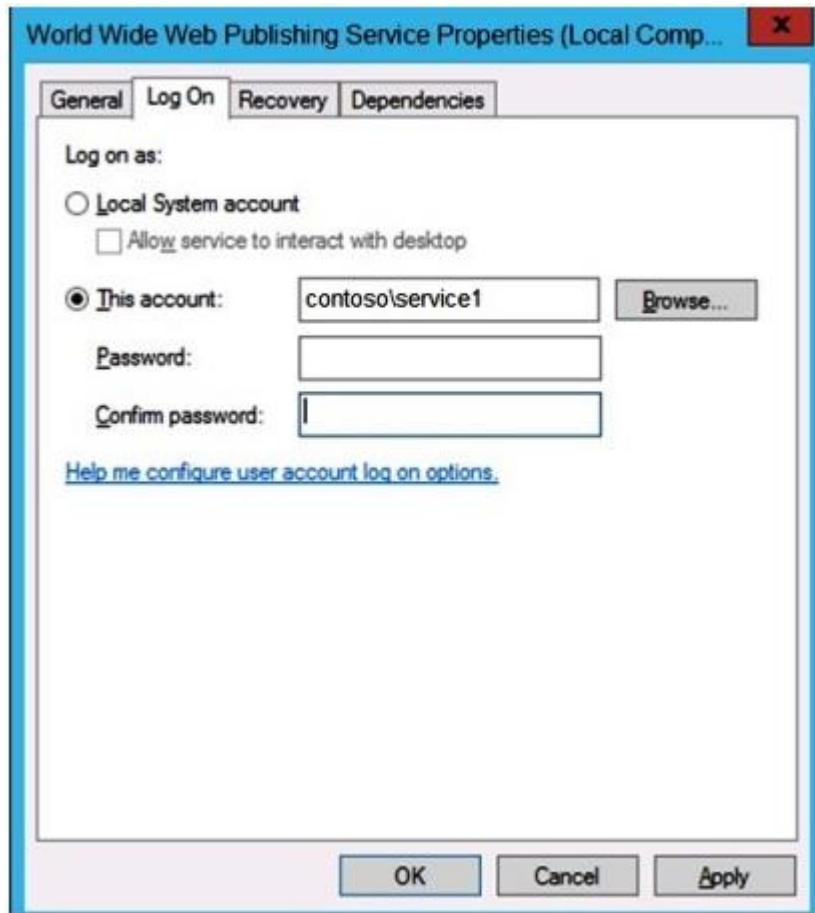
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 has the Web Server (IIS) server role installed.

On Server1, you install a managed service account named Service1. You attempt to configure the World Wide Web Publishing Service as shown in the exhibit. (Click the Exhibit button.)

You receive the following error message: "The account name is invalid or does not exist, or the password is invalid for the account name specified." You need to ensure that the World Wide Web Publishing Service can log on by using the managed service account.

What should you do?

**Exhibit:**



- A. Specify contoso\service1\$ as the account name.
- B. Specify service1@contoso.com as the account name.
- C. Reset the password for the account.
- D. Enter and confirm the password for the account.

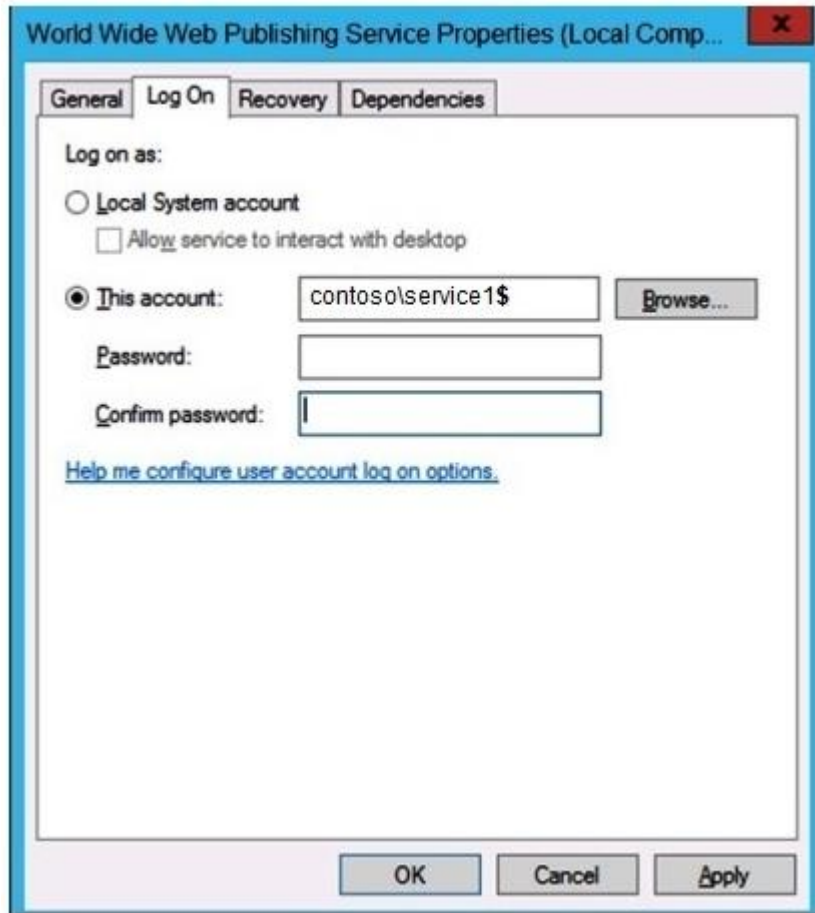
**Correct Answer:** A

**Section:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

If you are going to use the gMSA for a Service, an IIS Application Pool, or SQL 2012, you would simply plug it in the Logon/Credentials UI. The trick is to append a \$ after the account name, and leave the password blank:



<http://blogs.technet.com/b/askpfeplat/archive/2012/12/17/windows-server-2012-group-managed-service-accounts.aspx>

#### QUESTION 234

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

On DC1, you add a new volume and you stop the Active Directory Domain Services (AD DS) service. You run ntdsutil.exe and you set NTDS as the



active instance. You need to move the Active Directory database to the new volume.

Which Ntdsutil context should you use?

- A. Configurable Settings
- B. Partition management
- C. IFM
- D. Files

**Correct Answer: D**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). You can use the **ntdsutil** commands to perform database maintenance of AD DS, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.

<https://technet.microsoft.com/en-us/library/cc753343.aspx>

**files**

This is a subcommand of **Ntdsutil** and Dsdbutil. Ntdsutil and Dsdbutil are command-line tools that are built into Windows Server 2008 and Windows Server 2008 R2. Ntdsutil is available if you have the Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS) server role installed. Dsdbutil is available if you have the AD LDS server role installed. These tools are also available if you install the Active Directory Domain Services Tools that are part of the Remote Server Administration Tools (RSAT).

**move logs to %s** (where %s identifies a target directory) is a parameter of the **files** subcommand that moves the Ntds.dit data file to the new directory specified by %s and updates the registry so that, upon service restart, the directory service uses the new location.

<https://technet.microsoft.com/en-us/library/cc753900.aspx>

#### **QUESTION 235**

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2008 R2. The domain contains three servers that run Windows Server 2012 R2. The servers are configured as shown in the following table.

Server name	Configuration
Server1	Web Server (IIS) server role
Server2	Web Server (IIS) server role
Server3	Microsoft SQL Server

Server1 and Server2 are configured in a Network Load Balancing (NLB) cluster. The NLB cluster hosts a website named Web1 that uses an application pool named App1. Web1 uses a database named DB1 as its data store.

You create an account named User1. You configure User1, as the identity of App1. You need to ensure that contoso.com domain users accessing Web1 connect to DB1 by using their own credentials.

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

- A. Configure the delegation settings of Server3.
- B. Create a Service Principal Name (SPN) for User1.
- C. Configure the delegation settings of User1.
- D. Create a matching Service Principal Name (SPN) for Server1 and Server2.
- E. Configure the delegation settings of Server1 and Server2.

**Correct Answer:** BE

**Section:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

Service principal names are associated with the security principal (user or groups) in whose security context the service executes. SPNs are used to support mutual authentication between a client application and a service. An SPN is assembled from information that a client knows about a service. Or, it can obtain information from a trusted third party, such as Active Directory. A service principal name is associated with an account and an account can have many service principal names.

<https://technet.microsoft.com/en-us/library/cc961723.aspx>

The identity of an application pool is the name of the service account under which the application pool's worker process runs. By default, application pools operate under the Network Service user account, which has low-level user rights.

You can also configure a custom account to serve as an application pool's identity. Any custom account you choose should have only the minimum rights that your application requires. A custom account is useful in the following situations:

- When you want to improve security and make it easier to trace security events to the corresponding application.
- When you are hosting Web sites for multiple customers on a single Web server. If you use the same process account for multiple customers, source code from one customer's application may be able to access source code from another customer's application. In this case, you should also configure a custom account for the anonymous user account.
- When an application requires rights or permissions in addition to the default permissions for an application pool. In this case, you can create an application pool and assign a custom identity to the new application pool.

<https://technet.microsoft.com/en-us/library/cc771170>

### QUESTION 236

The contoso.com domain contains 2 domain controllers running Server 2012 R2. AD recycle bin is enabled for the domain. DC1 is configured to take AD snapshots daily. DC2 is set to take snapshots weekly.

Someone deletes a group containing 100 users. You need to recover this group.

What should you do?

- A. Authoritative Restore
- B. Non Authoritative Restore
- C. Tombstone Reanimation
- D. Modify attribute isdeleted=true

**Correct Answer: C**

**Section: Configure and manage Active Directory**

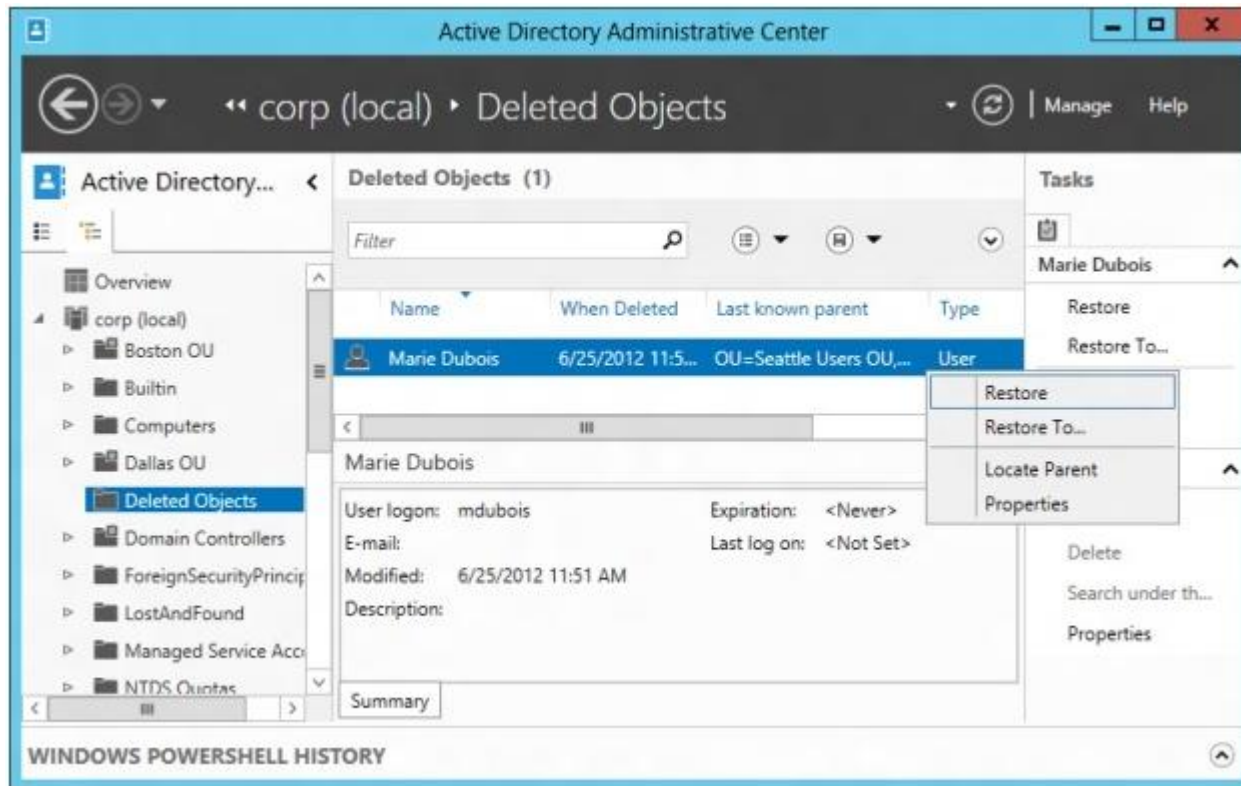
**Explanation**

#### **Explanation/Reference:**

In Windows Server 2003 Active Directory and Windows Server 2008 AD DS, you could recover deleted Active Directory objects through tombstone reanimation. However, reanimated objects' link-valued attributes (for example, group memberships of user accounts) that were physically removed and non-link-valued attributes that were cleared were not recovered. Therefore, administrators could not rely on tombstone reanimation as the ultimate solution to accidental deletion of objects.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion.

In Windows Server 2012, the Active Directory Recycle Bin feature has been enhanced with a new graphical user interface for users to manage and restore deleted objects. Users can now visually locate a list of deleted objects and restore them to their original or desired locations.



<https://technet.microsoft.com/en-us/library/hh831702.aspx>

#### QUESTION 237

You have a RODC named Server1 running Windows Server 2012 R2.

You need to add a RODC Administrator.

How do you complete the task?

- A. dsrmgmt.exe
- B. ntdsutil
- C. Add user to Local Administrator Group on Server1
- D. Use Security Group and modify RODC Delegated Administrator

**Correct Answer:** D

**Section:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

Administrator Role Separation (ARS) is an RODC feature that you can use to delegate the ability to administer an RODC to a user or a security group. When you delegate the ability to log on to an RODC to a user or a security group, the user or group is not added the Domain Admins group and therefore does not have additional rights to perform directory service operations.

<https://technet.microsoft.com/en-us/library/cc755310>

#### **QUESTION 238**

You need to create a new user account using the command prompt.

Which command would you use?

- A. dsmodify
- B. dscreate
- C. dsnew
- D. dsadd

**Correct Answer:** D

**Section:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

**Dsadd user**

Adds a single user to the directory.

**Dsadd** is a command-line tool that is built into Windows Server 2008. It is available if you have the Active Directory Domain Services (AD DS) server role installed. To use **dsadd**, you must run the **dsadd** command from an elevated command prompt.

<https://technet.microsoft.com/en-us/library/cc731279>

#### **QUESTION 239**

You need to enable three of your domain controllers as global catalog servers.

Where would you configure the domain controllers as global catalogs?

- A. Forest, NTDS settings
- B. Domain, NTDS settings
- C. Site, NTDS settings
- D. Server, NTDS settings

**Correct Answer: D**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**To add or remove the global catalog**

1. Open Active Directory Sites and Services. To open Active Directory Sites and Services, click **Start** , click **Administrative Tools** , and then click **Active Directory Sites and Services** .

To open Active Directory Sites and Services in Windows Server® 2012, click **Start** , type **dssite.msc** .

2. In the console tree, **click the server object to which you want to add the global catalog** or from which you want to remove the global catalog.

**Where?** Active Directory Sites and Services\Sites\SiteName\Servers

3. In the details pane, right-click **NTDS Settings** of the selected server object, and then click **Properties** .

4. Select the **Global Catalog** check box to add the global catalog, or clear the check box to remove the global catalog.

<https://technet.microsoft.com/en-us/library/cc755257.aspx>

#### **QUESTION 240**

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012. The domain contains a file server named Server1. All client computers run Windows 8. Users share the client computers and frequently log on to different client computers.

You need to ensure that when the users save files in the Documents folder, the files are saved automatically to \\Server1\Users\. The solution must minimize the amount of network traffic that occurs when the users log on to the client computers.

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: B**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**Folder Redirection** lets administrators redirect the path of a folder to a new location. The location can be a folder on the local computer or a directory on a network file share. Users can work with documents on a server as if the documents were based on a local drive. The documents in the folder are available to the user from any computer on the network. Folder Redirection is located under **Windows Settings** in the console tree when you edit domain-based Group Policy by using the Group Policy Management Console (GPMC). The path is **[Group Policy Object Name]\User Configuration\Policies\Windows Settings\Folder Redirection**.

<https://technet.microsoft.com/en-us/library/cc732275.aspx>

#### **QUESTION 241**

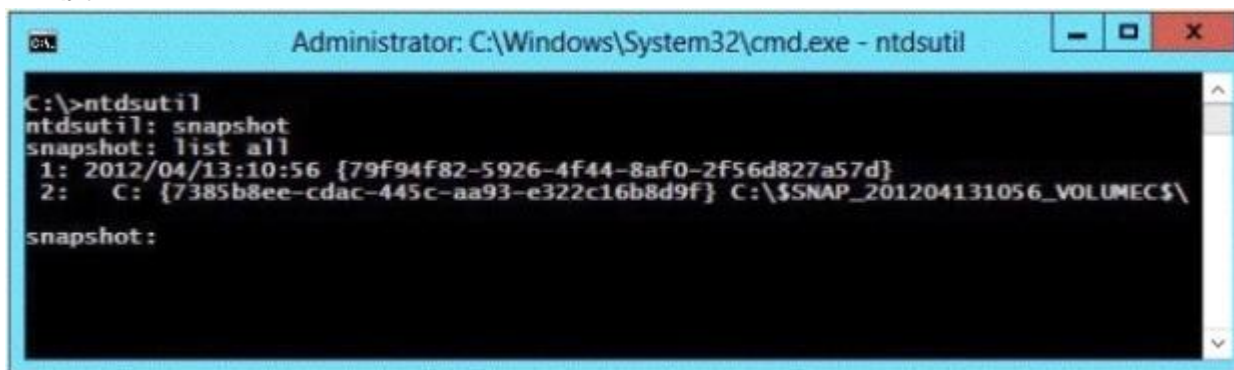
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1.

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

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

What should you do?

**Exhibit:**



```
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:
```

- A. From the snapshot context of ntdsutil, run activate instance "NTDS".

- B. From a command prompt, run `dsamain.exe -dbpath c:\$snap_201204131056_volumeec$\windows\ntds\ntds.dit -ldapport 389`.
- C. From the snapshot context of `ntdsutil`, run `mount {79f94f82-5926-4f44-8af0-2f56d827a57d}`.
- D. From a command prompt, run `dsamain.exe -dbpath c:\$snap_201204131056_volumeec$\windows\ntds\ntds.dit -ldapport 33389`.

**Correct Answer: D**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

In the command-line tool `Ntdsutil.exe`, you can use the `snapshot` subcommand to manage the snapshots, but you must use `Dsamain.exe` to expose the snapshot as a Lightweight Directory Access Protocol (LDAP) server.

<https://technet.microsoft.com/en-us/library/cc731620.aspx>

**Dsamain.exe** is a command-line tool that exposes Active Directory data that is stored in a snapshot or backup as a Lightweight Directory Access Protocol (LDAP) server. To use `Dsamain`, you must run the **dsamain** command from an elevated command prompt.

**Syntax:** `dsamain /dbpath <filepath> /ldapPort <number>`

`/dbpath <filepath>` specifies the file path to the database file. `<filepath>` must point to the database file, which might be on read-only media, such as a mounted snapshot; in a backup; or on another server, such as a domain controller or an AD LDS server.

`/ldapPort <number>` specifies the LDAP port value. Only the LDAP port is required. If you do not specify the other ports, they use LDAP+1, LDAP+2, and LDAP+3, respectively. For example, if you specify LDAP port 41389 without specifying other port values, the LDAP-SSL port uses port 41390 by default, and so on. You cannot specify ports that are currently in use. If you run the command on a domain controller, specify different ports than those that are used by the local domain controller.

The following example exposes the data in a snapshot `$SNAP_200704181137` as an LDAP server, using LDAP port 51389:

```
dsamain /dbpath E:\$SNAP_200704181137_VOLUMED$\WINDOWS\NTDS\ntds.dit /ldapport 51389
```

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

The answer option using `"-ldapport 389"` is not correct because clients use LDAP to query, create, update, and delete information that is stored in a directory service over a TCP connection through the TCP default port 389.

[https://technet.microsoft.com/en-us/library/how-global-catalog-servers-work\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/how-global-catalog-servers-work(v=ws.10).aspx)

**QUESTION 242**



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 Users and Computers, run the **Delegation of Control Wizard**.
- B. From a command prompt, run the dsadd computer command.
- C. From Active Directory Users and Computers, configure the **Managed By** settings of the RODC1 account.
- D. From Active Directory Site and Services, configure the **Security** settings of the RODC1 server object.

**Correct Answer: C**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

To specify the delegated RODC administrator after installation, you can use either of the following options:

- Modify the **Managed By** tab of the RODC account properties in the Active Directory Users and Computers snap-in, as shown in the following figure. You can click **Change** to change which security principal is the delegated RODC administrator. You can choose only one security principal. Specify a security group rather than an individual user so you can control RODC administration permissions most efficiently. This method changes the **managedBy** attribute of the computer object that corresponds to the RODC to the SID of the security principal that you specify. This is the recommended way to specify the delegated RODC administrator account because the information is stored in AD DS, where it can be centrally managed by domain administrators.



- Use the **ntdsutil local roles** command or the **dsmgmt local roles** command. You can use this command to view, add, or remove members from the Administrators group and other built-in groups on the RODC.

Using **ntdsutil** or **dsmgmt** to specify the delegated RODC administrator account is not recommended because the information is stored only locally on the RODC. Therefore, when you use **ntdsutil local roles** to delegate an administrator for the RODC, the account that you specify does not appear on the **Managed By** tab of the RODC account properties. As a result, using the Active Directory Users and Computers snap-in or a similar tool will not reveal that the RODC has a delegated administrator.

<https://technet.microsoft.com/en-us/library/cc755310>

### QUESTION 243

Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2. You have a Password Settings object (PSOs) named PSO1.

You need to view the settings of PSO1.

Which tool should you use?

- A. Get-ADFineGrainedPasswordPolicy
- B. Get-ADAccountResultantPasswordReplicationPolicy
- C. Get-ADDomainControllerPasswordReplicationPolicy
- D. Get-ADDefaultDomainPasswordPolicy

**Correct Answer:** A

**Section:** Configure and manage Active Directory

**Explanation**

**Explanation/Reference:**

The Get-ADFineGrainedPasswordPolicy cmdlet gets a fine grained password policy or performs a search to retrieve multiple fine grained password policies.

This cmdlet retrieves a default set of fine grained password policy object properties. To retrieve additional properties use the Properties parameter.

<https://technet.microsoft.com/en-us/library/ee617231.aspx>

#### **QUESTION 244**

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 (RODC) account named RODC1. You export the settings of RODC1 to a file named File1.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:** Configure and manage Active Directory

**Explanation**

### Explanation/Reference:

Beginning with Windows Server 2012, you can install AD DS using Windows PowerShell. `Dcpromo.exe` is deprecated beginning with Windows Server 2012, but you can still run `dcpromo.exe` by using an answer file (`dcpromo /unattend:<answerfile>` or `dcpromo /answer:<answerfile>`). The ability to continue running `dcpromo.exe` with an answer file provides organizations that have resources invested in existing automation time to convert the automation from `dcpromo.exe` to Windows PowerShell.

<https://technet.microsoft.com/en-us/library/Hh472162.aspx>

### QUESTION 245

You work as a Network Administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain named ABC.com. All servers in the ABC.com domain have Microsoft Windows Server 2012 R2 installed.

You want to clone a domain controller to create another domain controller.

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

- A. You should run the `Install-ADDSDomainController` PowerShell cmdlet.
- B. You should run the `New-ADDCCloneConfigFile` PowerShell cmdlet.
- C. You should run the `sysprep.exe /oobe` command.
- D. You should run the `dcpromo.exe /adv` command.
- E. You should place a `DCCloneConfig.xml` file in the `%Systemroot%\NTDS` folder.
- F. You should place an `Unattend.xml` file in the `%Systemroot%\SYSVOL` folder.

**Correct Answer:** BE

**Section:** Configure and manage Active Directory

**Explanation**

### Explanation/Reference:

The `New-ADDCCloneConfigFile` cmdlet performs prerequisite checks for cloning a domain controller when run locally on the domain controller being prepared for cloning. This cmdlet generates a clone configuration file, `DCCloneConfig.xml`, at an appropriate location, if all prerequisite checks succeed.

There are two modes of operation for this cmdlet, depending on where it is executed. When run on the domain controller that is being prepared for cloning, it will run the following pre-requisite checks to make sure this domain controller is adequately prepared for cloning:

- Is the PDC emulator FSMO role hosted on a domain controller running Windows Server 2012?
- Is this computer authorized for domain controller cloning (i.e. is the computer a member of the Cloneable Domain Controllers group)?
- Are all program and services listed in the output of the `Get-ADDCCloneExcludedApplicationList` cmdlet captured in

CustomDCCloneAllowList.xml?

If these pre-requisite checks all pass, the `New-ADDCCloneConfigFile` cmdlet will generate a `DCCloneConfig.xml` file at a suitable location based on the parameter values supplied. This cmdlet can also be run from a client (with Remote Server Administration Tools) and used to generate a `DCCloneConfig.xml` against offline media of the domain controller being cloned; however, none of the pre-requisite checks is performed in this usage mode. This usage is intended to generate `DCCloneConfig.xml` files with specific configuration values for each clone on copies of the offline media.

[https://technet.microsoft.com/en-us/%5Clibrary/JJ158947\(v=WPS.630\).aspx](https://technet.microsoft.com/en-us/%5Clibrary/JJ158947(v=WPS.630).aspx)

The clone domain controller uses the following criteria to detect that it is a copy of another domain controller:

1. The value of the VM-Generation ID supplied by the virtual machine is different than the value of the VM-Generation ID stored in the DIT.
2. Presence of a file called `DCCloneConfig.xml` in one of the following locations:

The directory where the DIT resides

`%windir%\NTDS`

The root of a removable media drive

<https://technet.microsoft.com/en-us/library/Hh831734.aspx>

#### QUESTION 246

You work as a Network Administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain named ABC.com. The ABC.com network has a Windows Server 2012 R2 domain controller named ABC-DC10 which hosts the Web Server, DNS, and DHCP services.

You create a snapshot backup of ABC-DC10 using the `Ntfsutil` utility and mount the snapshot.

How would you access the contents of the snapshot?

- A. You should run the `Ntfsutil.exe` utility with the partition management parameter.
- B. You should run the `Dsadmin.exe` utility with the `/allowupgrade` parameter.
- C. You should run the `Dsadmin.exe /dbpath` command from the command prompt.
- D. You should run the `Ntfsutil.exe` utility with the files parameter.

**Correct Answer: C**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

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

The **/dbpath <filepath>** parameter specifies the file path to the database file. **<filepath>** must point to the database file, which might be on read-only media, such as a mounted snapshot; in a backup; or on another server, such as a domain controller or an AD LDS server.

<https://technet.microsoft.com/en-us/library/Cc772168.aspx>

#### QUESTION 247

Your network contains an Active Directory forest named contoso.com. The forest contains two domains named contoso.com and child1.contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains four domain controllers. The domain controllers are configured as shown in the following table.

Domain Controller Name	Domain Name	Role
DC1	contoso.com	PDC Emulator RID Master Schema Master Domain Naming Master
DC2	contoso.com	Infrastructure Master
DC10	child1.contoso.com	PDC Emulator RID Master
DC11	child1.contoso.com	Infrastructure Master

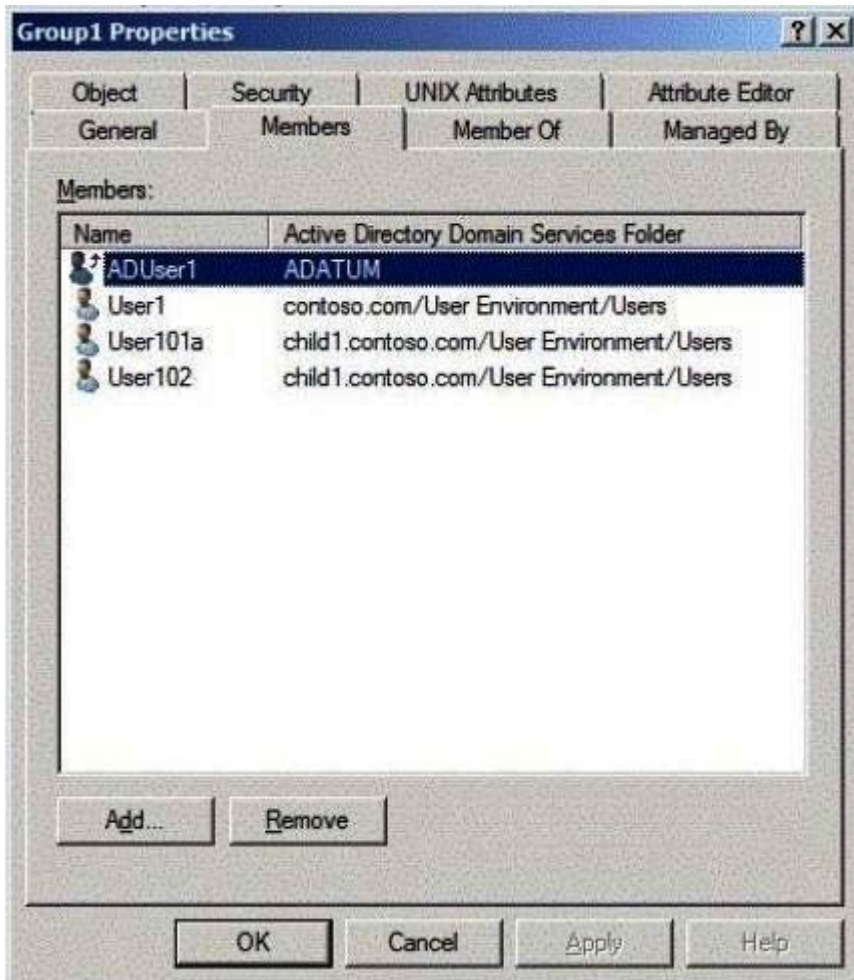
You open Active Directory Users and Computers on a client computer and connect to DC1. You display the members of a group named Group1 as shown in the Group1 Members exhibit. (Click the Exhibit button.)

When you view the properties of a user named User102, you receive the error message shown in the Error exhibit. (Click the Exhibit button.)

The error message does not display for any other members of Group1. You need to identify which domain controller causes the issue shown in the error message.

Which domain controller should you identify?

**Group 1 (exhibit):**



Error Message (exhibit):



- A. DC1
- B. DC2
- C. DC10
- D. DC11

**Correct Answer: B**

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

The infrastructure master is responsible for updating the group-to-user references when the members of a group are renamed or changed within a domain.

The domain controller that holds the infrastructure master role for the group's domain is responsible for updating the cross-domain group-to-user reference to reflect the user's name change. Periodically, the infrastructure master scans its database for group members from other domains. For each member from a foreign domain that the infrastructure master finds, it compares the name and the security identifier (SID) of the member against a global catalog. If the name or the SID does not match, the local reference is updated with the values in the global catalog. For example, if a user account is moved to a new domain, the infrastructure master updates the local reference's name and SID because they do not match the values in the global catalog. After the infrastructure master updates these references locally, it uses replication to update all other replicas of the domain. If the infrastructure master is not available, these updates are delayed.

[https://technet.microsoft.com/en-us/library/Ff646933\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Ff646933(v=WS.10).aspx)

#### **QUESTION 248**

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 identify the setspn.exe command that you must run to configure the appropriate 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:**

The interface consists of two main panes. The left pane, titled 'Objects', contains a list of items: `-f`, `*S`, `AppPool1`, `http/contoso`, `https/contoso`, `http/secure.contoso.com`, and `https/secure.contoso.com`. The right pane, titled 'Answer Area', shows the command `setspn.exe` followed by three empty boxes labeled 'Object'.

**Correct Answer:**

The interface shows the correct solution. In the 'Objects' pane, the items `-f`, `AppPool1`, `https/contoso`, and `https/secure.contoso.com` have been removed. In the 'Answer Area', the three empty boxes have been replaced with the objects `*S`, `https/secure.contoso.com`, and `AppPool1`.

**Section: Configure and manage Active Directory**

**Explanation**

**Explanation/Reference:**

**Setspn** is a command-line tool that is built into Windows Server 2008. It is available if you have the Active Directory Domain Services (AD DS) server role installed. To use **setspn**, you must run the **setspn** command from an elevated command prompt.

## Syntax

```
setspn <Computer> [-l] [-r] [-d <SPN>] [-s <SPN>] [-?]
```

## Parameters

[-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
```

<https://technet.microsoft.com/en-us/library/cc731241>

## QUESTION 249

Your network contains an Active Directory forest named contoso.com. All domain controllers run Windows Server 2008 R2. The schema is upgraded to Windows Server 2012 R2. Contoso.com contains two servers. The servers are configured as shown in the following table.

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

Server1 and Server2 host a load-balanced application pool named AppPool1. You need to ensure that AppPool1 uses a group Managed Service Account as its identity.

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

**Select and Place:**

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

Correct Answer:

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

Section: Configure and manage Active Directory  
Explanation

Explanation/Reference:

#### Group Managed Service Accounts Requirements

- At least one Windows Server 2012 Domain Controller

- A Windows Server 2012 or Windows 8 machine with the ActiveDirectory PowerShell module, to create/manage the gMSA.
- A Windows Server 2012 or Windows 8 domain member to run/use the gMSA.

<http://blogs.technet.com/b/askpfeplat/archive/2012/12/17/windows-server-2012-group-managed-service-accounts.aspx>

The **New-ADServiceAccount** cmdlet creates a new Active Directory service account. You can set commonly used service account property values by using the cmdlet parameters. Property values that are not associated with cmdlet parameters can be set by using the OtherAttributes parameter.

<https://technet.microsoft.com/en-us/library/ee617211.aspx>

Service principal names are associated with the security principal (user or groups) in whose security context the service executes. SPNs are used to support mutual authentication between a client application and a service. An SPN is assembled from information that a client knows about a service. Or, it can obtain information from a trusted third party, such as Active Directory. A service principal name is associated with an account and an account can have many service principal names.

<https://technet.microsoft.com/en-us/library/cc961723.aspx>

The identity of an application pool is the name of the service account under which the application pool's worker process runs. By default, application pools operate under the Network Service user account, which has low-level user rights.

You can also configure a custom account to serve as an application pool's identity. Any custom account you choose should have only the minimum rights that your application requires. A custom account is useful in the following situations:

- When you want to improve security and make it easier to trace security events to the corresponding application.
- When you are hosting Web sites for multiple customers on a single Web server. If you use the same process account for multiple customers, source code from one customer's application may be able to access source code from another customer's application. In this case, you should also configure a custom account for the anonymous user account.
- When an application requires rights or permissions in addition to the default permissions for an application pool. In this case, you can create an application pool and assign a custom identity to the new application pool.

<https://technet.microsoft.com/en-us/library/cc771170>

## QUESTION 250

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

You need to create an Active Directory snapshot on DC1.

Which four commands should you run? To answer, move the four appropriate commands from the list of commands to the answer area and arrange them in the correct order.

**Select and Place:**

Commands	Answer Area
dsamain.exe	
snapshot	
create	
ntdsutil.exe	
activate instance ntds	
wbadmin.exe	

**Correct Answer:**

Commands	Answer Area
dsamain.exe	ntdsutil.exe
snapshot	snapshot
create	activate instance ntds
ntdsutil.exe	create
activate instance ntds	
wbadmin.exe	

## Section: Configure and manage Active Directory

### Explanation

#### Explanation/Reference:

#### To create an AD DS or AD LDS snapshot

1. Log on to a domain controller as a member of the Enterprise Admins groups or the Domain Admins group.
2. Click Start, right-click Command Prompt, and then click Run as administrator.
3. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.
4. At the elevated command prompt, type the following command, and then press ENTER:

**ntdsutil**

5. At the ntdsutil prompt, type the following command, and then press ENTER:

## **snapshot**

6. At the snapshot prompt, type the following command, and then press ENTER:

**activate instance ntds**

7. At the snapshot prompt, type the following command, and then press ENTER:

**create**

The command returns the following output:

```
Snapshot set {GUID} generated successfully.
```

Where *GUID* is the globally unique identifier (GUID) for the snapshot.

8. At the snapshot prompt, type the following command, and then press ENTER:

**mount {GUID}**

9. As an option, to see a list of all mounted snapshots, you can type the following command, and then press ENTER:

**list mounted**

The output lists each mounted snapshot and a corresponding index number. You can use the index number instead of the GUID to subsequently mount, unmount, or delete the snapshot.

<https://technet.microsoft.com/en-us/library/cc753609>

## **QUESTION 251**

Your network contains an Active Directory domain named contoso.com. You deploy a web-based application named App1 to a server named Server1. App1 uses an application pool named AppPool1. AppPool1 uses a domain user account named User1 as its identity.

You need to configure Kerberos constrained delegation for User1.

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

**Select and Place:**

Actions	Answer Area
Run <b>setspn.exe</b> and specify the <b>-l</b> parameter.	
From the properties of User1, open the <b>Delegation</b> tab, and add the <b>HOST</b> service.	
From the properties of User1, open the <b>Delegation</b> tab, and select "Trust this user for delegation to any service (Kerberos only)."	
From the properties of User1, open the <b>Delegation</b> tab, and select "Trust this user for delegation to specified services only."	
Run <b>setspn.exe</b> and specify the <b>-s</b> parameter.	

Correct Answer:

Actions	Answer Area
Run <b>setspn.exe</b> and specify the <b>-l</b> parameter.	From the properties of User1, open the <b>Delegation</b> tab, and select "Trust this user for delegation to specified services only."
From the properties of User1, open the <b>Delegation</b> tab, and select "Trust this user for delegation to any service (Kerberos only)."	From the properties of User1, open the <b>Delegation</b> tab, and add the <b>HOST</b> service.
	Run <b>setspn.exe</b> and specify the <b>-s</b> parameter.

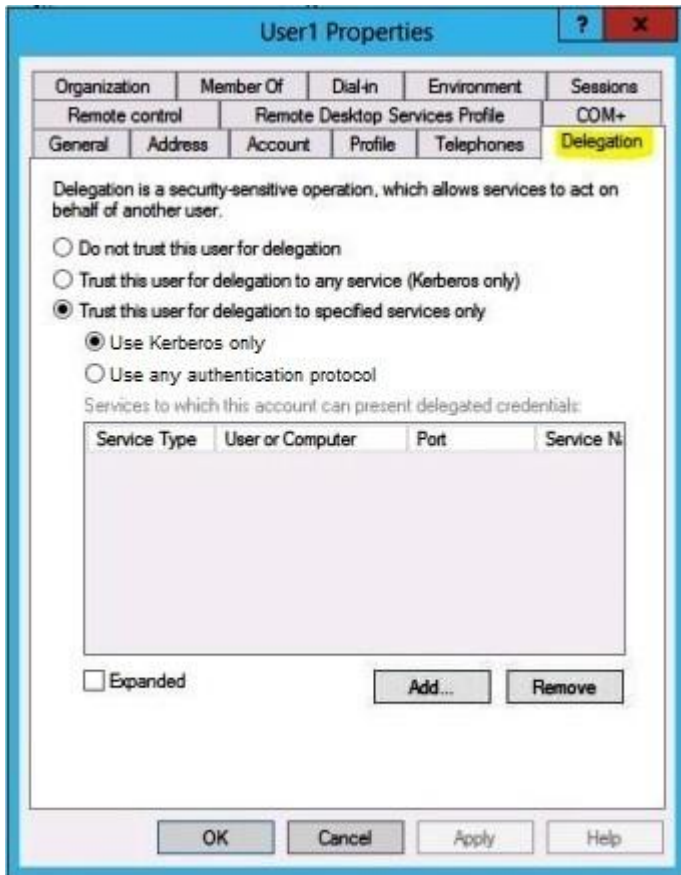


**Section: Configure and manage Active Directory**  
**Explanation**

**Explanation/Reference:**

**To allow a user to be trusted for delegation for specific services**

1. Open Active Directory Users and Computers.
2. In the console tree, click **Users**.
3. Right-click the user you want to be trusted for delegation, and click **Properties**.
4. *Click the **Delegation** tab and click **Trust this user for delegation to specified services only**.*
5. Select **Use Kerberos only** (default).
6. Click **Add** and, in **Add Services** click **Users and Computers**.
7. In **Select Users or Computers**, enter the name of the user or computer that the user will be trusted to delegate for.
8. *In **Add Services**, select the service or services that will be trusted for delegation and click **OK**. Repeat as necessary.*



If you cannot see the **Delegation** tab... 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.

<https://technet.microsoft.com/en-us/library/cc757194>

To add an SPN, use the **setspn -s service/hostname** 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.

Setspn also has an **-A** that you can use to add SPNs, but you should use **Setspn -S** instead because **-S** will verify that there are no duplicate SPNs. However, if you are using Windows Server 2003 or earlier, you will not be able to use the **-S** switch because it is not available for that platform. In the

case where you cannot use -S, then you should manually verify that there are no duplicate SPNs by first running Setspn -L.

<https://technet.microsoft.com/en-us/library/cc731241.aspx>

#### QUESTION 252

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

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

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

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

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

**Hot Area:**

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

**Correct Answer:**

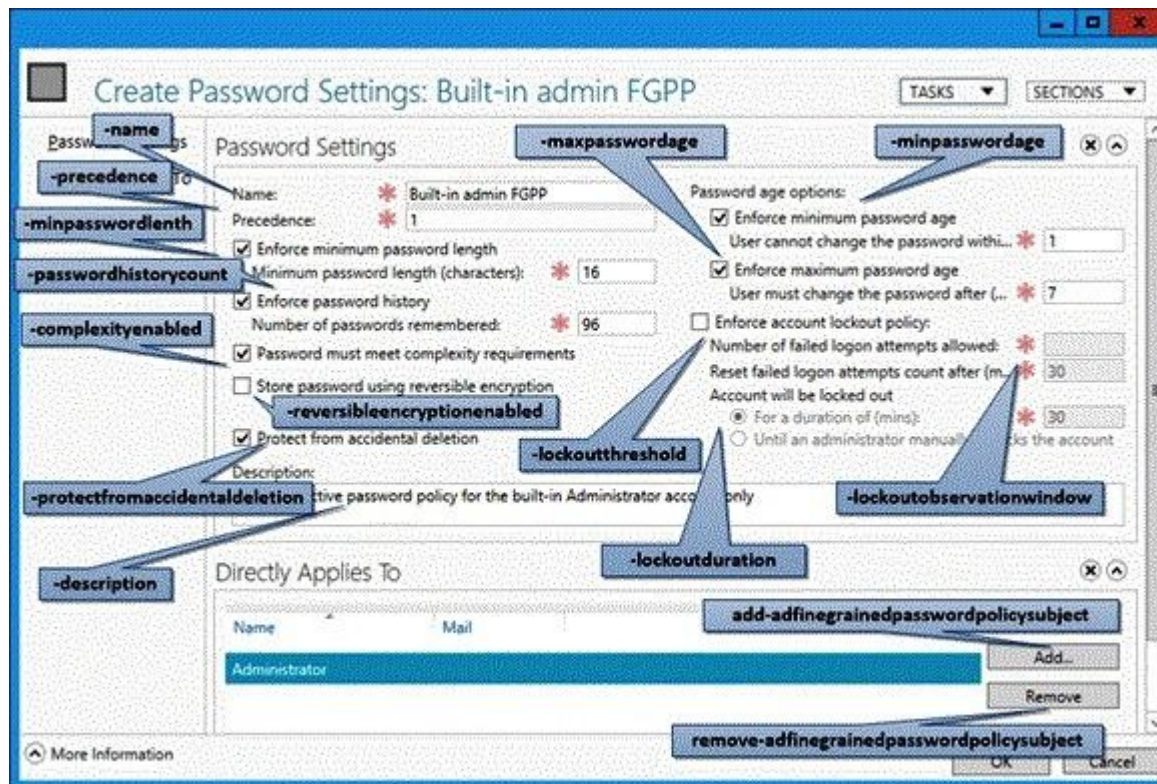
Security setting	Configured by using
Minimum password length	<div> <input type="text"/> </div> <div> PSO User account properties </div>
Account is sensitive and cannot be delegated	<div> <input type="text"/> </div> <div> PSO User account properties </div>
User cannot change password	<div> <input type="text"/>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

## Section: Configure and manage Active Directory

### Explanation

### Explanation/Reference:

Fine-Grained Password Policy cmdlet functionality did not change between the Windows Server 2008 R2 and Windows Server 2012. As a convenience, the following diagram illustrates the associated arguments for cmdlets:



<https://technet.microsoft.com/en-us/library/jj574144.aspx>

The following are the Active Directory user account options:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption
- Account is disabled
- Smart card is required for interactive logon
- Account is sensitive and cannot be delegated
- User Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption
- This account supports Kerberos AES 256 bit encryption
- Do not require Kerberos preauthentication

**User1 Properties**

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
			Organization	

User logon name:

User logon name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☒ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption
- ☐ Account is disabled
- ☐ Smart card is required for interactive logon
- ☒ Account is sensitive and cannot be delegated

Account expires:  
☒ Never  
☐ End of:

<https://technet.microsoft.com/en-us/library/dd145547.aspx>

### QUESTION 253

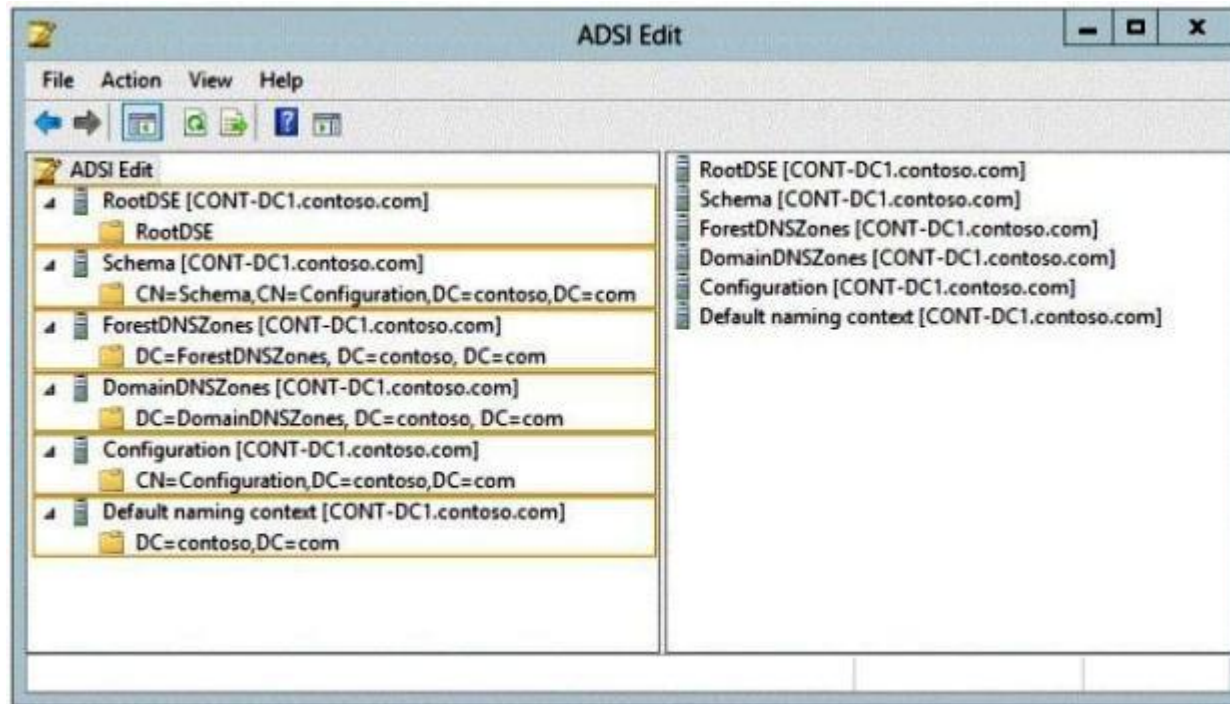
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012 R2 and are configured as DNS servers. All DNS zones are Active Directory-integrated. Active Directory Recycle Bin is enabled.

You need to modify the amount of time deleted objects are retained in the Active Directory Recycle Bin.



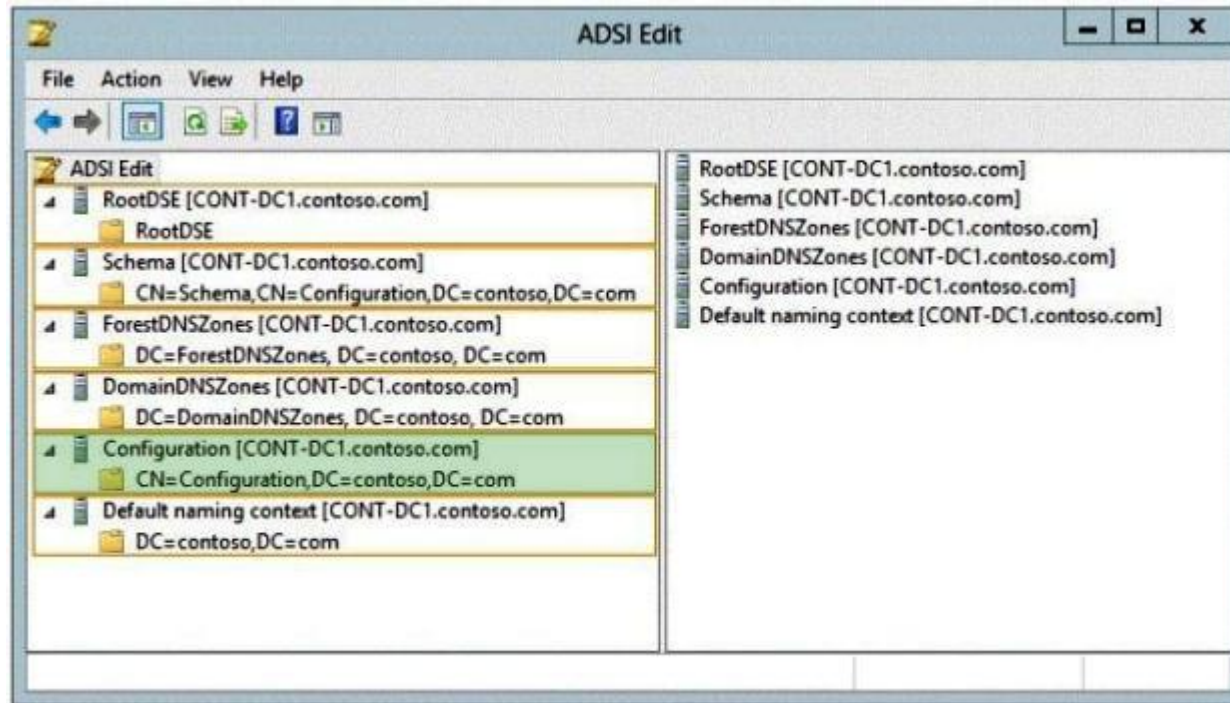
Which naming context should you use? To answer, select the appropriate naming context in the answer area.

**Hot Area:**



**Correct Answer:**





## Section: Configure and manage Active Directory

### Explanation

#### Explanation/Reference:

#### To modify the tombstone lifetime by using the Set-ADObject cmdlet

At the Active Directory module for Windows PowerShell command prompt, type the following command, and then press ENTER:

```
Set-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<mydomain>,DC=<com>"  
-Partition "CN=Configuration,DC=<mydomain>,DC=<com>" -Replace:@{ "tombstoneLifetime" = <value> }
```

Replace DC=<mydomain>,DC=<com> with the appropriate forest root domain name of your Active Directory environment, and replace <value> with the new value for the tombstone lifetime.

<https://technet.microsoft.com/en-us/library/dd392260>

**QUESTION 254**

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

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

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

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

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

**Hot Area:**

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

**Correct Answer:**

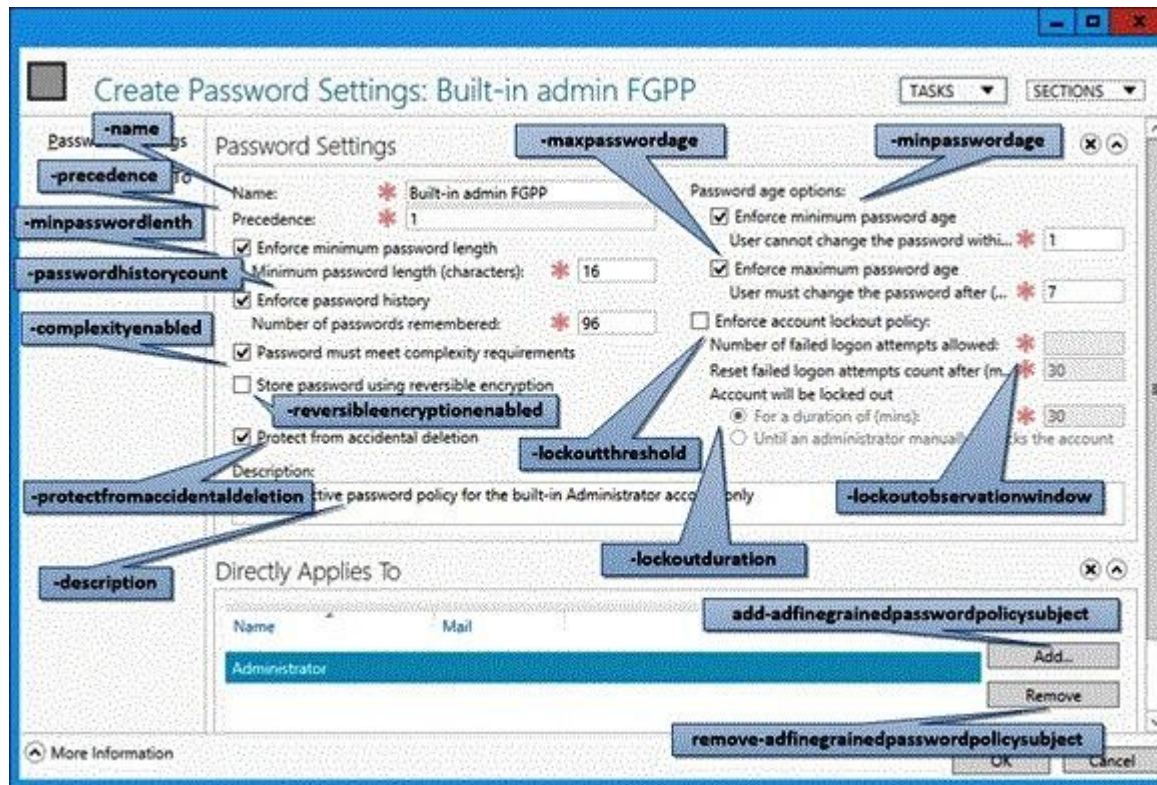
Security setting	Configured by using
Minimum password length	<div> <div></div> <div>PSO</div> <div>User account properties</div> </div>
Account is sensitive and cannot be delegated	<div> <div></div> <div>PSO</div> <div>User account properties</div> </div>
User cannot change password	<div> <div></div>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

### Section: Configure and manage Active Directory

#### Explanation

#### Explanation/Reference:

Fine-Grained Password Policy cmdlet functionality did not change between the Windows Server 2008 R2 and Windows Server 2012. As a convenience, the following diagram illustrates the associated arguments for cmdlets:



<https://technet.microsoft.com/en-us/library/jj574144.aspx>

The following are the Active Directory user account options:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption
- Account is disabled
- Smart card is required for interactive logon
- Account is sensitive and cannot be delegated
- User Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption
- This account supports Kerberos AES 256 bit encryption
- Do not require Kerberos preauthentication

**User1 Properties**

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
			Organization	

User logon name:  
 @contoso.com

User logon name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☒ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption
- ☐ Account is disabled
- ☐ Smart card is required for interactive logon
- ☒ Account is sensitive and cannot be delegated

Account expires:  
☒ Never  
☐ End of:

<https://technet.microsoft.com/en-us/library/dd145547.aspx>

### QUESTION 255

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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

You can create a central store that provides all administrators who edit domain-based Group Policy Objects (GPOs) access to the same set of Administrative Template files. The central store is an administrator-created folder on SYSVOL that provides a single centralized storage location for all Administrative Template files (ADMX and ADML) for the domain. Once you create the central store, the Group Policy tools use only the ADMX files in the central store and ignore ADMX versions stored locally. The central store is optional; if you do not create it, the Group Policy tools use the local ADMX files. The root folder for the central store must be named PolicyDefinitions (that is, %SystemRoot%\SYSVOL\domain\policies\PolicyDefinitions).

<https://technet.microsoft.com/en-us/library/gg699412.aspx>

In Group Policy for versions of Windows earlier than Windows Vista, if you change Administrative template policy settings on local computers, the Sysvol share on a domain controller within your domain is automatically updated with the new .ADM files. In turn, those changes are replicated to all other domain controllers in the domain. This might result in increased network load and storage requirements. 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.

<http://support.microsoft.com/kb/929841>

#### **QUESTION 256**

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

You implement a Group Policy central store. You have an application named App1. App1 requires that a custom registry setting be deployed to all of the computers. You need to deploy the custom registry setting. The solution must minimize administrator effort.

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

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

**Correct Answer:** D

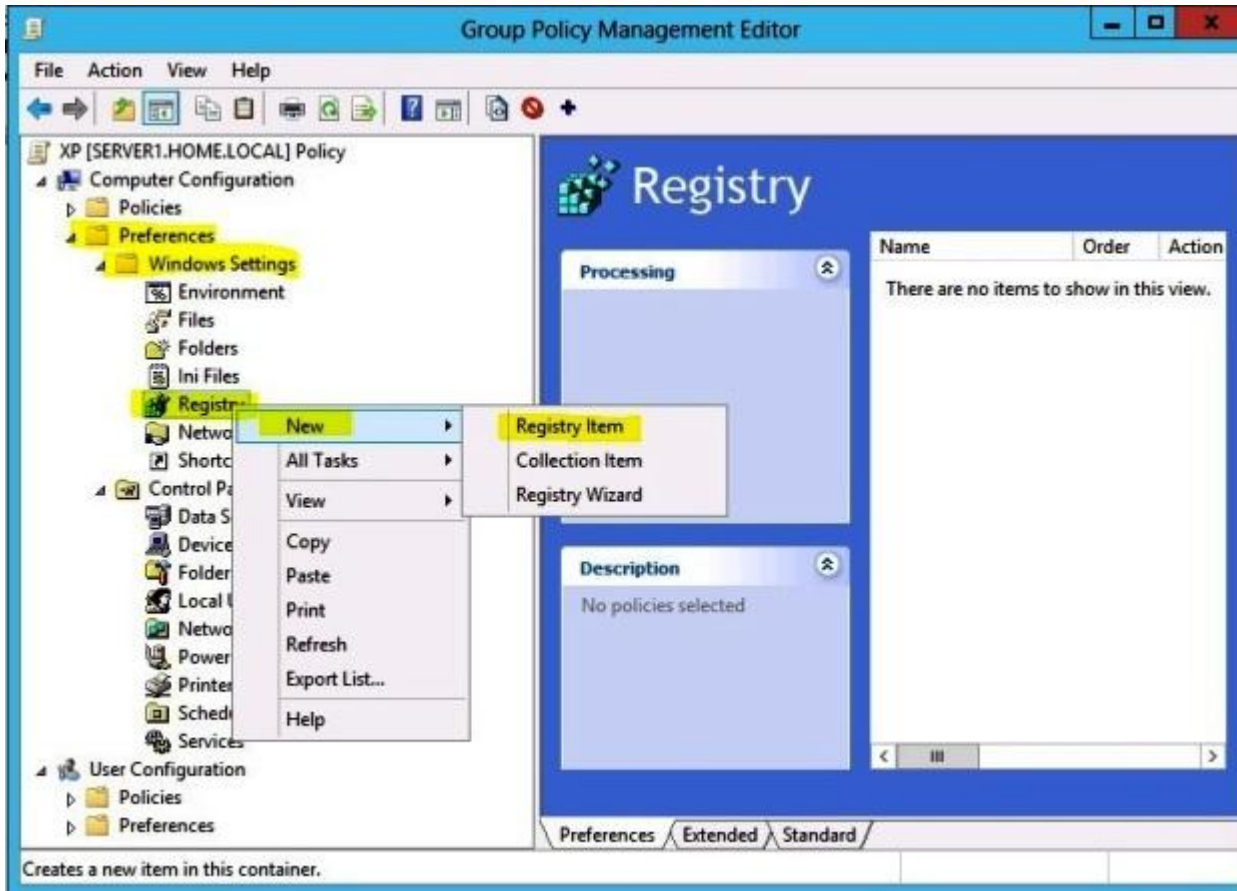
**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

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.





<https://technet.microsoft.com/en-us/library/gg699429.aspx>

#### QUESTION 257

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-NetGpo cmdlet.
- D. Run the Backup-Gpo cmdlet.

**Correct Answer:** A

**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

A copy operation allows you to transfer settings from an existing GPO in Active Directory directly into a new GPO. The new GPO created during the copy operation is given a new GUID and is unlinked. You can use a copy operation to transfer settings to a new GPO in the same domain, another domain in the same forest, or a domain in another forest. Because a copy operation uses an existing GPO in Active Directory as its source, trust is required between the source and destination domains. Copy operations are suited for moving Group Policy between production environments, and for migrating Group Policy that has been tested in a test domain or forest to a production environment, as long as there is trust between the source and destination domains.

<https://technet.microsoft.com/en-us/library/cc785343>

#### **QUESTION 258**

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:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

Group Policy Preferences are Group Policy client-side extensions. There are 20 extensions that makes up Group Policy Preferences. These extensions include:

Client Side Extension	Description
Environment	Create, modify, or delete environment variables.
Local Users and Groups	Create, modify, or delete local users and groups.
Device Settings	Enable or disable hardware devices or classes of devices.
Network Options	Create, modify, or delete virtual private networking (VPN) or dial-up networking (DUN) connections.
Drive Maps	Create, modify, or delete mapped drives, and configure the visibility of all drives.
Folders	Create, modify, or delete folders.
Network Shares	Create, modify, or delete network shares
Files	Copy, modify the attributes of, replace, or delete files.
Data Sources	Create, modify, or delete Open Database Connectivity (ODBC) data source names.
INI Files	Add, replace, or delete sections or properties in configuration settings (.ini) or setup information (.inf) files.
Folder Options	Create, modify, or delete folders.
Schedule Tasks	Create, modify, or delete scheduled or immediate tasks.
Registry	Copy registry settings and apply them to other computers. Create, replace, or delete registry settings.
Printers	Create, modify, or delete TCP/IP, shared, and local printer connections.
Shortcuts	Create, modify, or delete shortcuts.
Internet Settings	Modify user-configurable Internet settings
Start Menu Settings	Modify Start menu options. (Not applicable for Windows 8 and Windows Server 2012)
Regional Options	Modify regional options.
Power Options	Modify power options and create, modify, or delete power schemes.
Applications	Configure settings for applications.

<https://technet.microsoft.com/en-us/library/dn581922.aspx>

#### QUESTION 259

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: Configure and manage Group Policy**

**Explanation**

#### **Explanation/Reference:**

Shortcut preference items allow you to configure a shortcut to a file system object (such as a file, folder, drive, share, or computer), a shell object (such as a printer, desktop item, or control panel item), or a URL (such as a Web page or an FTP site). Before you create a Shortcut preference item, you should review the behavior of each type of action possible with this extension.

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.

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

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

#### QUESTION 260

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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

Group Policy scope is the list of all Group Policy objects that may be applicable to the user or computer because of their object's location within Active Directory. Security Filtering determines if the respective user or computer has the proper permissions to apply the Group Policy object. A user or

computer must have the **Read** and **Apply Group Policy** permissions for the Group Policy service to consider the Group Policy object applicable to the user.

The Group Policy services iterates through the entire list of Group Policy objects determining if the user or computer has the proper permissions to the GPO. If the user or computer has the permissions to apply the GPO, then the Group Policy service moves that GPO into a filtered list of GPOs. It continues to filter each Group Policy object based on permissions until it reaches the end of the list. The filtered list of Group Policy objects contains all GPOs within scope of the user or computer and are applicable to the user or computer based on permissions.

<https://technet.microsoft.com/en-us/library/dn581922.aspx>

#### **QUESTION 261**

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 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

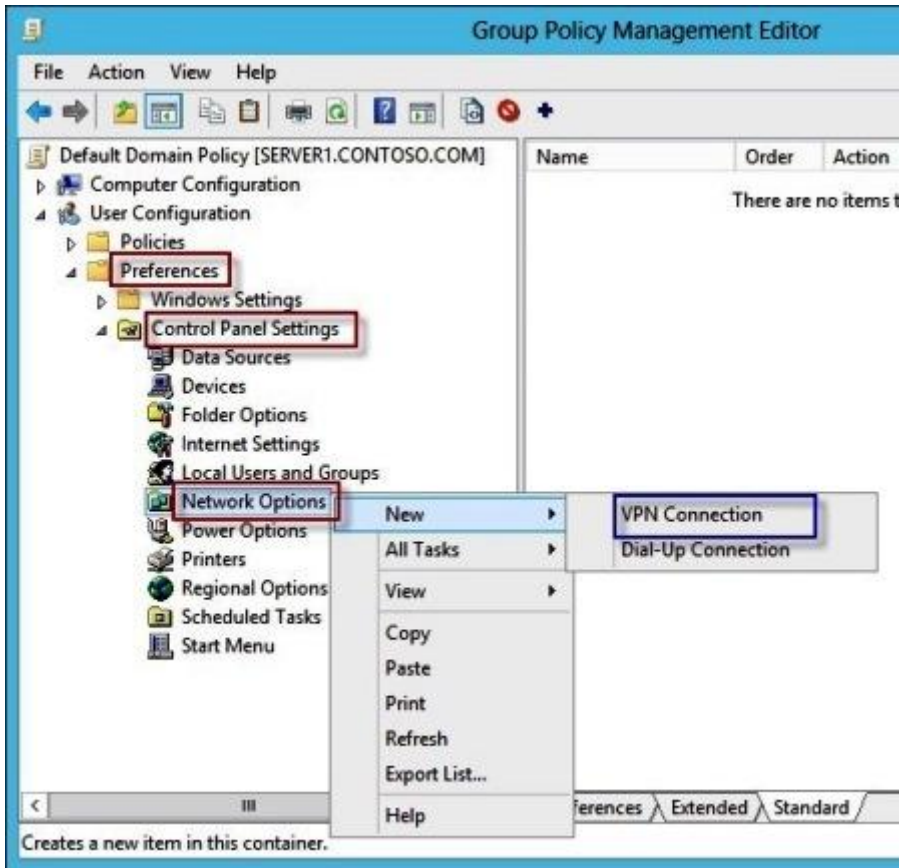
**Correct Answer: D**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

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.



<https://technet.microsoft.com/en-us/library/cc772449.aspx>

#### QUESTION 262

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:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

Group Policy Preferences are Group Policy client-side extensions. There are 20 extensions that makes up Group Policy Preferences. These extensions include:

Client Side Extension	Description
Environment	Create, modify, or delete environment variables.
Local Users and Groups	Create, modify, or delete local users and groups.
Device Settings	Enable or disable hardware devices or classes of devices.
Network Options	Create, modify, or delete virtual private networking (VPN) or dial-up networking (DUN) connections.
Drive Maps	Create, modify, or delete mapped drives, and configure the visibility of all drives.
Folders	Create, modify, or delete folders.
Network Shares	Create, modify, or delete network shares
<b>Files</b>	<b>Copy, modify the attributes of, replace, or delete files.</b>
Data Sources	Create, modify, or delete Open Database Connectivity (ODBC) data source names.
INI Files	Add, replace, or delete sections or properties in configuration settings (.ini) or setup information (.inf) files.
<b>Folder Options</b>	<b>Create, modify, or delete folders.</b>
Schedule Tasks	Create, modify, or delete scheduled or immediate tasks.
Registry	Copy registry settings and apply them to other computers. Create, replace, or delete registry settings.
Printers	Create, modify, or delete TCP/IP, shared, and local printer connections.
Shortcuts	Create, modify, or delete shortcuts.
Internet Settings	Modify user-configurable Internet settings
Start Menu Settings	Modify Start menu options. (Not applicable for Windows 8 and Windows Server 2012)
Regional Options	Modify regional options.
Power Options	Modify power options and create, modify, or delete power schemes.
Applications	Configure settings for applications.

<https://technet.microsoft.com/en-us/library/dn581922.aspx>

### QUESTION 263

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:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

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.

The Group Policy service does not govern unmanaged policy settings. These policy settings are persistent. The Group Policy service does not remove unmanaged policy settings, even if the policy setting is not within scope of the user or computer. Typically, you use these types of policy settings to set preferences for operating system components that are not policy enabled. You can also use unmanaged policy settings for application settings.

The Managed property filter has three states: **Any**, **Yes**, and **No**. Setting this property filter to **Any** causes the Group Policy Management Console to display all Administrative Template policy settings. Setting this property filter to **Yes** causes the editor to show only managed Administrative Template policy settings, hiding all unmanaged Administrative Template policy settings. Setting this property filter to **No** causes the editor to show only unmanaged Administrative Template policy settings, hiding all managed Administrative Template policy settings.

<https://technet.microsoft.com/en-us/library/cc731054.aspx>

The Event Viewer has a wealth of information regarding Group Policy. Unfortunately, it requires you to look at all of the different log files to find entries for Group Policy. There you'll find entries related to policy application, policy replication, and policy refresh, all of which can be useful when trying to track down a problem.

<https://technet.microsoft.com/en-us/magazine/2007.02.troubleshooting.aspx>

The Event Log service records events on the system by writing to one of three default logs that you can read in Event Viewer: the security, application, and system logs. The security log records audit events. You use the settings under Event Log to specify attributes of the security, application, and system logs, such as maximum log size, access rights for each log, and retention settings and methods.

Event Log policy settings can be configured in the following location in Group Policy Object Editor:

`GPO_name\Computer Configuration\Windows Settings\Security Settings\Event Log\`

<https://technet.microsoft.com/en-us/library/cc778402>

#### **QUESTION 264**

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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

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.

<https://technet.microsoft.com/en-us/library/gg699429.aspx>

#### **QUESTION 265**

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

200 Group Policy objects (GPOs).

An administrator named Admin1 must be able to add new WMI filters from the Group Policy Management Console (GPMC). You need to delegate the required permissions to Admin1. The solution must minimize the number of permissions assigned to Admin1.

What should you do?

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

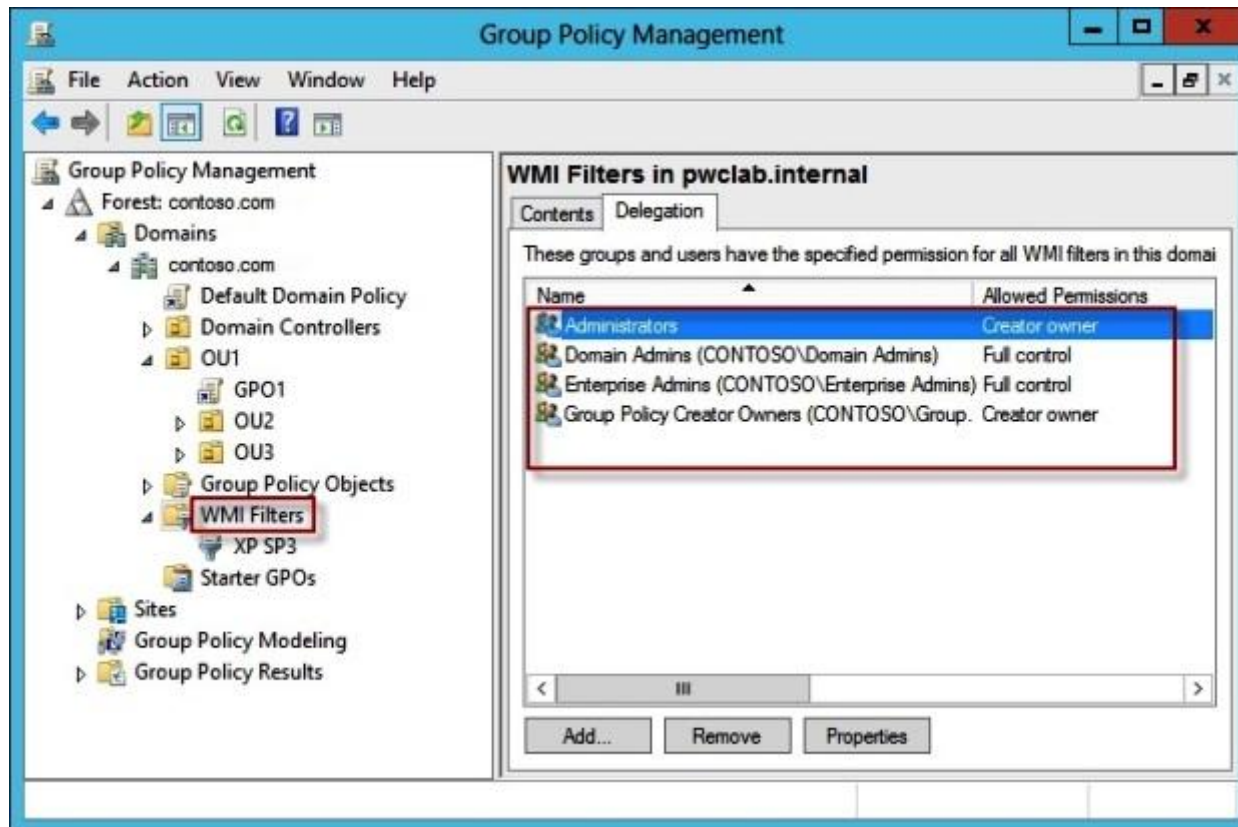
**Correct Answer: B**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

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.



<https://technet.microsoft.com/en-us/library/cc757429>

#### QUESTION 266

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

You have two GPOs linked to an organizational unit (OU) named OU1. You need to change the precedence order of the GPOs.

What should you use?

- A. Dcgpofix
- B. Get-GPReport
- 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: I**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

The **Set-GPLink** cmdlet sets the properties of a GPO link.

You can set the following properties:

- **Enabled.** If the GPO link is enabled, the settings of the GPO are applied when Group Policy is processed for the site, domain or OU.
- **Enforced.** If the GPO link is enforced, it cannot be blocked at a lower-level (in the Group Policy processing hierarchy) container.
- **Order.** The order specifies the precedence that the settings of the GPO take over conflicting settings in other GPOs that are linked (and enabled) to the same site, domain, or OU.

<https://technet.microsoft.com/en-us/library/ee461022.aspx>

#### **QUESTION 267**

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-GPInheritance
- I. Set-GPLink
- J. Set-GPPermission
- K. Gpupdate
- L. Add-ADGroupMember

**Correct Answer:** A

**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

**Dcgpofix** recreates the default Group Policy Objects (GPOs) for a domain.

When restoring the Default Domain Policy GPO to its original state, you will lose any changes that you have made to this GPO. As a best practice, you should configure the Default Domain Policy GPO only to manage the default Account Policies settings, Password Policy, Account Lockout Policy, and Kerberos Policy. In this example, you ignore the version of the Active Directory schema so that the **dcgpofix** command is not limited to same schema as the Windows version in which the command was shipped.

```
dcgpofix /ignore schema /target:Domain
```

Parameter	Description
<code>/ignore schema</code>	Ignores the version of the Active Directory® schema when you run this command. Otherwise, the command only works on the same schema version as the Windows version in which the command was shipped.
<code>/target {Domain   DC   Both}</code>	Specifies which GPO to restore. You can restore the Default Domain Policy GPO, the Default Domain Controllers GPO, or both.
<code>/?</code>	Displays Help at the command prompt.

<https://technet.microsoft.com/en-us/library/hh875588>



**QUESTION 268**

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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

**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. You can use the Name or the Guid parameter to set the permission level for the security principal on a single GPO, or you can use the All parameter to set the permission level for the security principal on all GPOs in the domain.

By default, if the security principal already has a higher permission level than the specified permission level, the change is not applied. You can specify the Replace parameter, to remove the existing permission level from the GPO before the new permission level is set. This ensures that the existing permission level is replaced by the new permission level.

<https://technet.microsoft.com/en-us/library/ee461038.aspx>

**QUESTION 269**

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-GPInheritance
- I. Set-GPLink
- J. Set-GPPermission
- K. Gpupdate
- L. Add-ADGroupMember

**Correct Answer: C**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

**Gpfixup** fixes domain name dependencies in Group Policy Objects and Group Policy links after a domain rename operation.

<https://technet.microsoft.com/en-us/library/hh852336>

**QUESTION 270**

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

You need to prevent all of the GPOs at the site level and at the domain level from being applied to users and computers in an organizational unit (OU) named OU1. 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-GPInheritance
- I. Set-GPLink
- J. Set-GPPermission
- K. Gpupdate
- L. Add-ADGroupMember

**Correct Answer:** H

**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

The **Set-GPInheritance** cmdlet blocks or unblocks inheritance for a specified domain or organizational unit (OU).

GPOs are applied according to the Group Policy hierarchy in the following order: local GPO, GPOs linked to the site, GPOs linked to the domain, GPOs linked to OUs. By default, an Active Directory container inherits settings from GPOs that are applied at the next higher level in the hierarchy. Blocking inheritance prevents the settings in GPOs that are linked to higher-level sites, domains, or organizational units from being automatically inherited by the specified domain or OU, unless the link (at the higher-level container) for a GPO is enforced.

<https://technet.microsoft.com/en-us/library/ee461032.aspx>

#### **QUESTION 271**

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

You need to provide an Administrator named Admin1 with the ability to create GPOs in the domain. The solution must not provide Admin1 with the ability to link GPOs.

What should you use?

- A. Dcgpofix
- B. Get-GPOReport
- C. Gpfixup
- D. Gpresult
- E. Gptedit.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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

**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. You can use the Name or the Guid parameter to set the permission level for the security principal on a single GPO, or you can use the All parameter to set the permission level for the security principal on all GPOs in the domain.

By default, if the security principal already has a higher permission level than the specified permission level, the change is not applied. You can specify the Replace parameter, to remove the existing permission level from the GPO before the new permission level is set. This ensures that the existing permission level is replaced by the new permission level.

<https://technet.microsoft.com/en-us/library/ee461038.aspx>

#### **QUESTION 272**

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 GPO named GPO1. GPO1 contains several Group Policy preferences.

You need to view all of the preferences configured in GPO1.

What should you use?

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

**Correct Answer:** B

**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

The **Get-GPOReport** cmdlet generates a report in either XML or HTML format that describes properties and policy settings for a specified GPO or for all GPOs in a domain. The information that is reported for each GPO includes: details, links, security filtering, WMI filtering, delegation, and computer and user configurations.

<https://technet.microsoft.com/en-us/library/hh967460.aspx>

### QUESTION 273

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. An organizational unit (OU) named OU1 contains 200 client computers that run Windows 8 Enterprise. A Group Policy object (GPO) named GPO1 is linked to OU1.

You make a change to GPO1. You need to force all of the computers in OU1 to refresh their Group Policy settings immediately. The solution must minimize administrative effort.

Which tool should you use?

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

D. Gpupdate command

**Correct Answer: B**

**Section: Configure and manage Group Policy**

**Explanation**

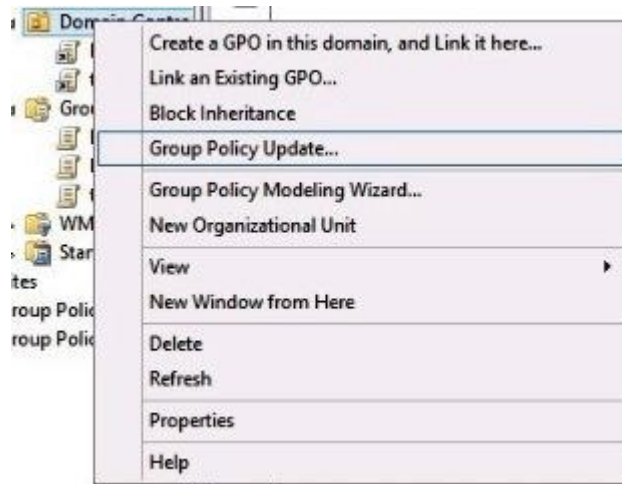
**Explanation/Reference:**

With Windows Server 2012 and Windows 8, you can remotely refresh Group Policy settings for all computers in an organizational unit (OU) from one central location by using the Group Policy Management Console (GPMC). Or you can use the **Invoke-GPUpdate** Windows PowerShell cmdlet to refresh Group Policy for a set of computers, including computers that are not within the OU structure—for example, if the computers are located in the default computers container.

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

### **Remote GP Update Wizard**

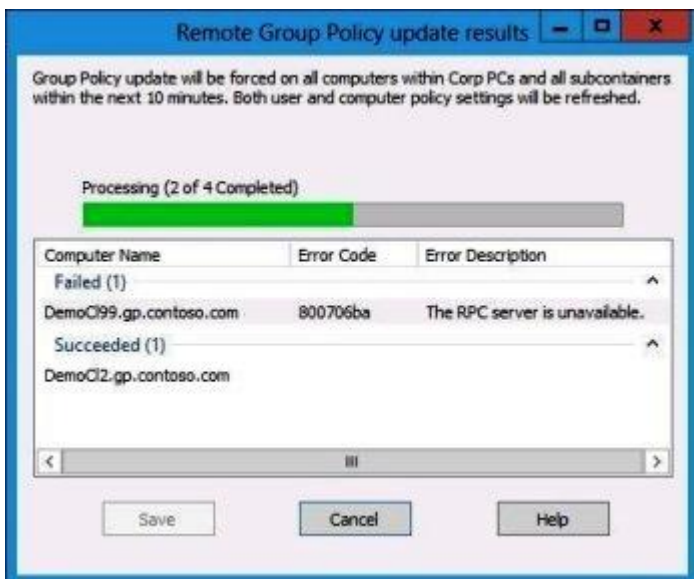
From the GPMC, right click on an OU that contains computer objects.



Click the “Group Policy Update” option.



This will run a `gpupdate /force` on all computers in the OU, and any subOUs. Computer policy will be refreshed for each computer, and user policy will be refreshed for any and all users currently logged into those computers.



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

## QUESTION 274

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

A domain controller named DC1 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**

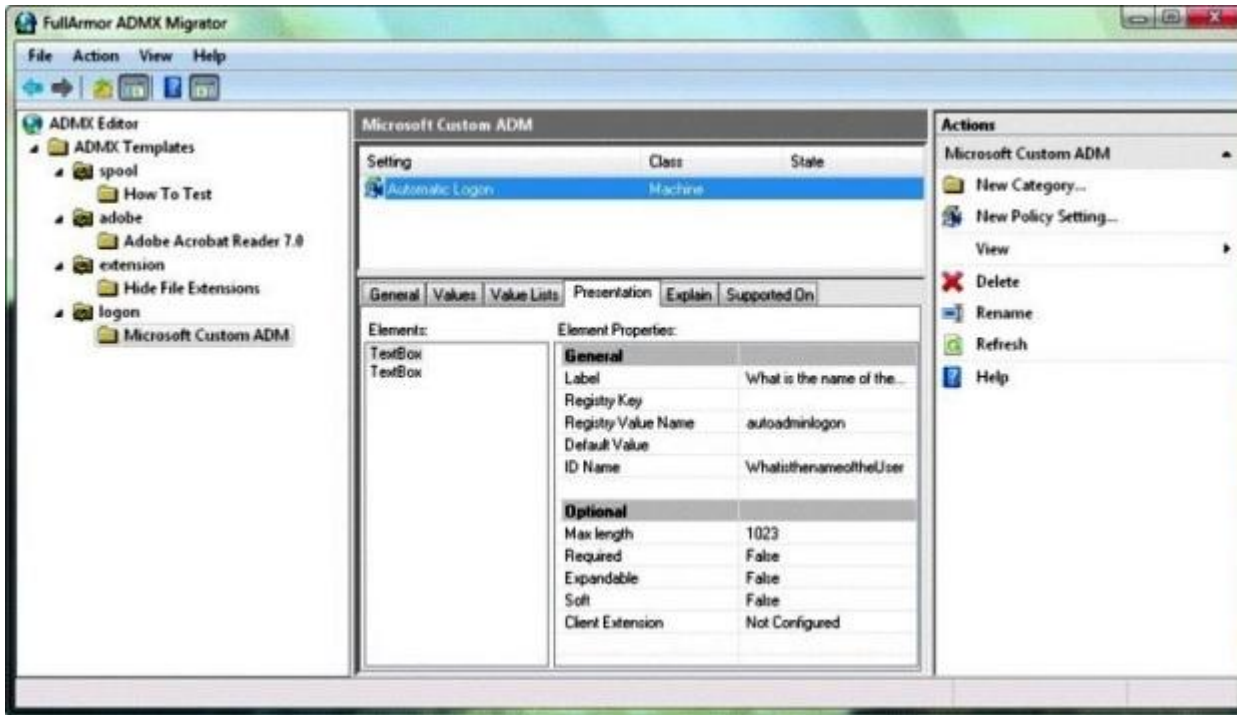
**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

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.





<https://technet.microsoft.com/en-us/magazine/2008.02.utilityspotlight.aspx>

### QUESTION 275

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

You create a central store for Group Policy. You receive a custom administrative template named Template1.admx. You need to ensure that the settings in Template1.admx appear in all new Group Policy objects (GPOs).

What should you do?

- A. From the Default Domain Controllers Policy, add Template1.admx to the Administrative Templates.
- B. From the Default Domain Policy, add Template1.admx to the Administrative Templates.
- C. Copy Template1.admx to \\Contoso.com\SYSVOL\Contoso.com\Policies\PolicyDefinitions\.
- D. Copy Template1.admx to \\Contoso.com\NETLOGON.

**Correct Answer: C**

## Section: Configure and manage Group Policy

### Explanation

#### Explanation/Reference:

You can create a central store that provides all administrators who edit domain-based Group Policy Objects (GPOs) access to the same set of Administrative Template files. The central store is an administrator-created folder on SYSVOL that provides a single centralized storage location for all Administrative Template files (ADMX and ADML) for the domain. Once you create the central store, the Group Policy tools use only the ADMX files in the central store and ignore ADMX versions stored locally. The central store is optional; if you do not create it, the Group Policy tools use the local ADMX files. The root folder for the central store must be named PolicyDefinitions (that is, %SystemRoot%\SYSVOL\domain\policies\PolicyDefinitions).

<https://technet.microsoft.com/en-us/library/gg699412.aspx>

In Group Policy for versions of Windows earlier than Windows Vista, if you change Administrative template policy settings on local computers, the Sysvol share on a domain controller within your domain is automatically updated with the new .ADM files. In turn, those changes are replicated to all other domain controllers in the domain. This might result in increased network load and storage requirements. 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.

<http://support.microsoft.com/kb/929841>

#### QUESTION 276

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: Configure and manage Group Policy

### Explanation

**Explanation/Reference:**

The **Minimum password length** policy setting determines the least number of characters that can make up a password for a user account. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.

Location:

*GPO\_name*\Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

<https://technet.microsoft.com/en-us/library/hh994560>

Fine-grained password policies apply only to user objects and global security groups. They cannot be applied to Computer objects.

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 fine-grained 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.

<https://technet.microsoft.com/en-us/library/cc770842>

**QUESTION 277**

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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

Group Policy Preferences are Group Policy client-side extensions. There are 20 extensions that makes up Group Policy Preferences. These extensions include:

Client Side Extension	Description
Environment	Create, modify, or delete environment variables.
Local Users and Groups	Create, modify, or delete local users and groups.
Device Settings	Enable or disable hardware devices or classes of devices.
Network Options	Create, modify, or delete virtual private networking (VPN) or dial-up networking (DUN) connections.
Drive Maps	Create, modify, or delete mapped drives, and configure the visibility of all drives.
Folders	Create, modify, or delete folders.
Network Shares	Create, modify, or delete network shares
Files	Copy, modify the attributes of, replace, or delete files.
Data Sources	Create, modify, or delete Open Database Connectivity (ODBC) data source names.
INI Files	Add, replace, or delete sections or properties in configuration settings (.ini) or setup information (.inf) files.
Folder Options	Create, modify, or delete folders.
Schedule Tasks	Create, modify, or delete scheduled or immediate tasks.
Registry	Copy registry settings and apply them to other computers. Create, replace, or delete registry settings.
Printers	Create, modify, or delete TCP/IP, shared, and local printer connections.
Shortcuts	Create, modify, or delete shortcuts.
Internet Settings	Modify user-configurable Internet settings
Start Menu Settings	Modify Start menu options. (Not applicable for Windows 8 and Windows Server 2012)
Regional Options	Modify regional options.
Power Options	Modify power options and create, modify, or delete power schemes.
Applications	Configure settings for applications.

<https://technet.microsoft.com/en-us/library/dn581922.aspx>

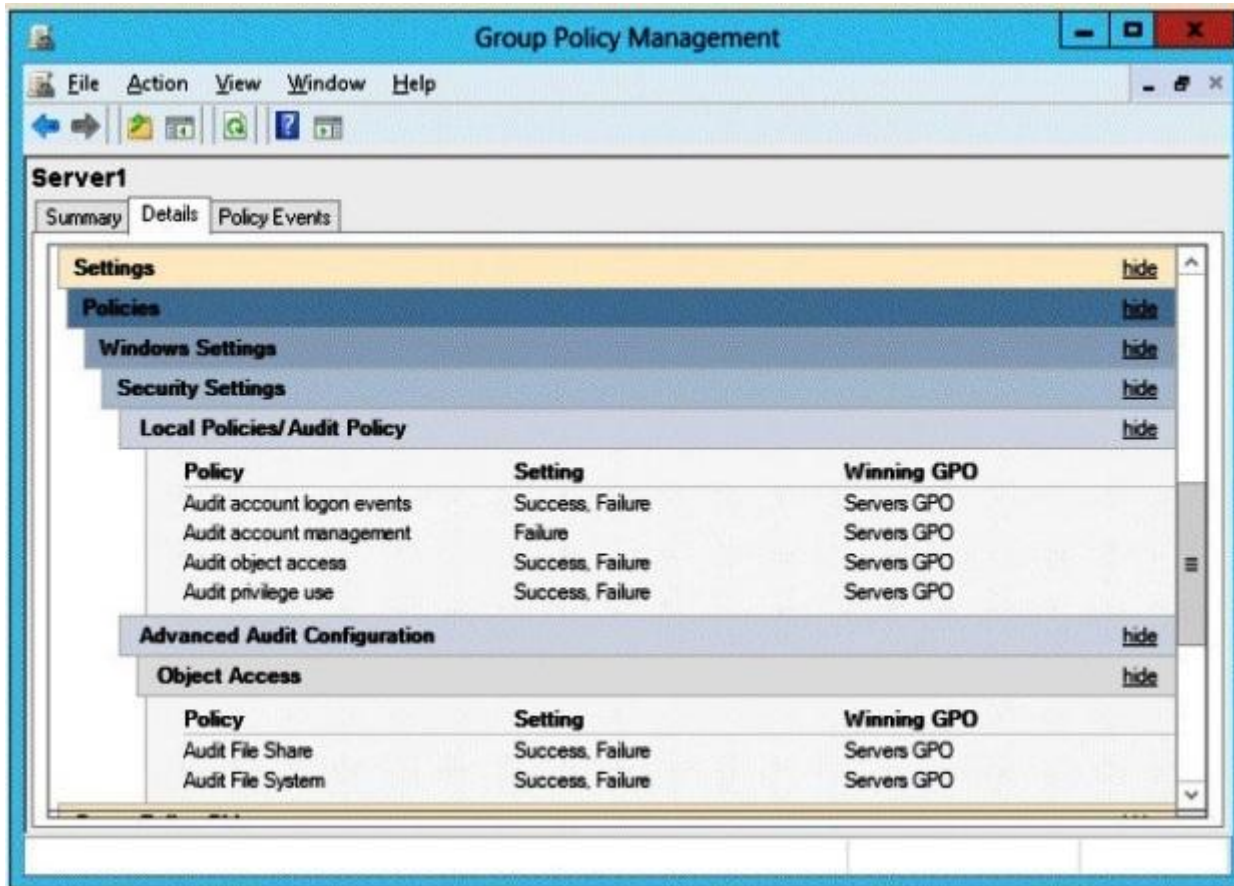
#### QUESTION 278

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

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

What should you do?

Exhibit:





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

**Correct Answer: C**

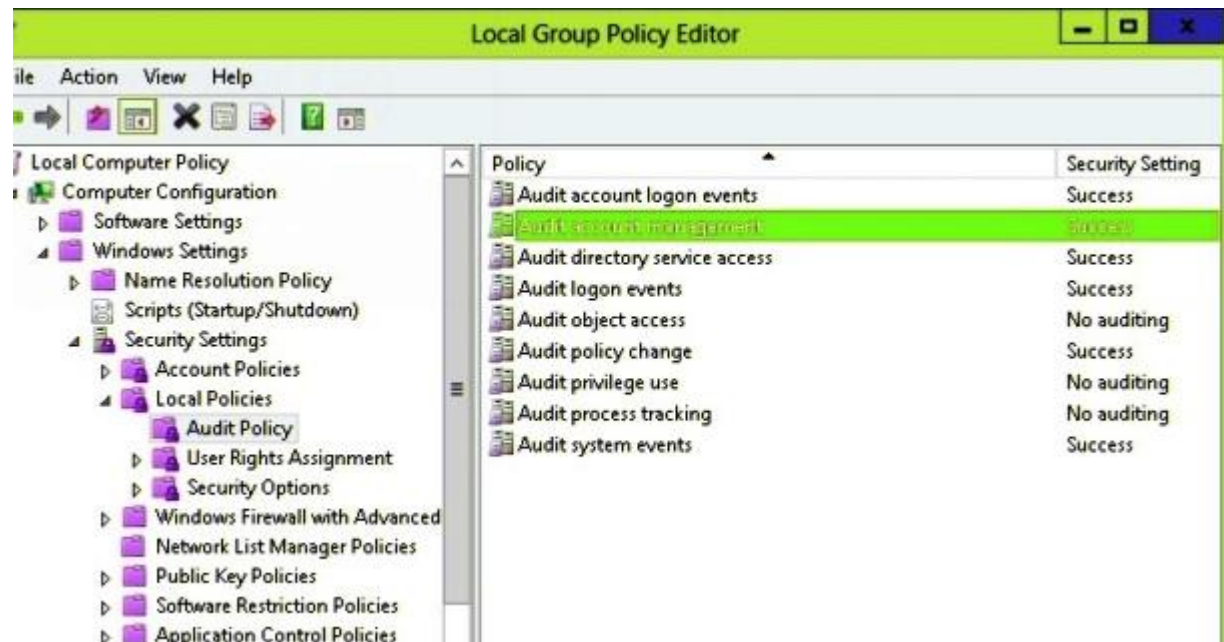
**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

### **Audit Account Management**

This audit setting determines whether to track management of users and groups. For example, users and groups should be tracked when a user or computer account, a security group, or a distribution group is created, changed, or deleted; when a user or computer account is renamed, disabled, or enabled; or when a user or computer password is changed. An event can be generated for users or groups that are added to or removed from other groups.



<https://technet.microsoft.com/en-us/library/dn487458.aspx>

**QUESTION 279**

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. All sales users have laptop computers that run Windows 8. The sales computers are joined to the domain. All user accounts for the sales department are in an organizational unit (OU) named Sales\_OU.

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

What should you configure from User Configuration in GPO1?

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

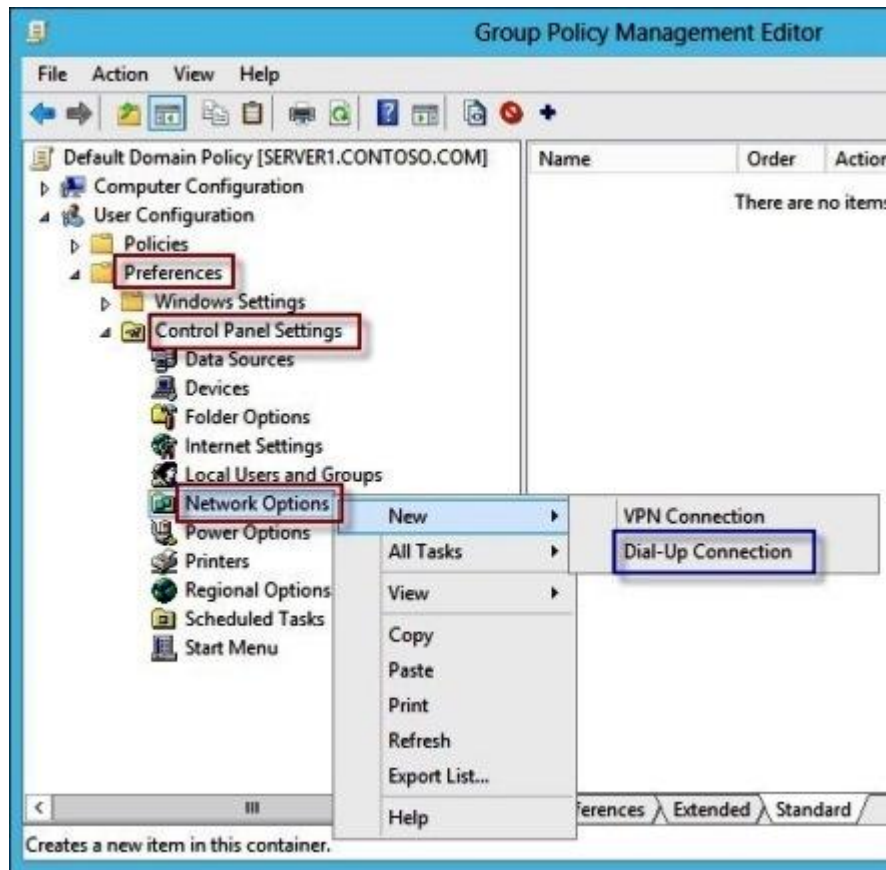
**Correct Answer: B**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

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.



<https://technet.microsoft.com/en-us/library/cc772449.aspx>

#### QUESTION 280

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?

**Exhibit:**





- 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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

You can create a central store that provides all administrators who edit domain-based Group Policy Objects (GPOs) access to the same set of Administrative Template files. The central store is an administrator-created folder on SYSVOL that provides a single centralized storage location for all Administrative Template files (ADMX and ADML) for the domain. Once you create the central store, the Group Policy tools use only the ADMX files in the central store and ignore ADMX versions stored locally. The central store is optional; if you do not create it, the Group Policy tools use the local ADMX files. The root folder for the central store must be named PolicyDefinitions (that is, %SystemRoot%\SYSVOL\domain\policies\PolicyDefinitions).

<https://technet.microsoft.com/en-us/library/gg699412.aspx>

In Group Policy for versions of Windows earlier than Windows Vista, if you change Administrative template policy settings on local computers, the Sysvol share on a domain controller within your domain is automatically updated with the new .ADM files. In turn, those changes are replicated to all other domain controllers in the domain. This might result in increased network load and storage requirements. 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.

<http://support.microsoft.com/kb/929841>

#### QUESTION 281

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. An organizational unit (OU) named OU1 contains 200 client computers that run Windows 8 Enterprise. A Group Policy object (GPO) named GPO1 is linked to OU1.

You make a change to GPO1. You need to force all of the computers in OU1 to refresh their Group Policy settings immediately. The solution must minimize administrative effort.

Which tool should you use?

- A. Group Policy Object Editor
- B. Set-AdComputer cmdlet
- C. Active Directory Users and Computers
- D. Invoke-GPUUpdate cmdlet

**Correct Answer: D**

**Section: Configure and manage Group Policy**

**Explanation**

#### **Explanation/Reference:**

With Windows Server 2012 and Windows 8, you can remotely refresh Group Policy settings for all computers in an organizational unit (OU) from one central location by using the Group Policy Management Console (GPMC). Or you can use the **Invoke-GPUUpdate** Windows PowerShell cmdlet to refresh Group Policy for a set of computers, including computers that are not within the OU structure—for example, if the computers are located in the default computers container.

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

#### QUESTION 282

Your network contains an Active Directory domain named contoso.com. The domain contains 30 organizational units (OUs).

You need to ensure that a user named User1 can link Group Policy Objects (GPOs) in the domain.

What should you do?

- A. From Active Directory Users and Computers, add User1 to the Network Configuration Operators group.
- B. From Group Policy Management, click the contoso.com node and modify the Delegation settings.
- C. From Group Policy Management, click the Group Policy Objects node and modify the Delegation settings.
- D. From Active Directory Users and Computers, add User1 to the Group Policy Creator Owners group.

**Correct Answer: B**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

**Link GPOs** permission is assigned to members of Domain Administrators and Enterprise Administrators by default. To assign **Link GPOs** permission to additional users or groups (such as accounts that have the roles of AGPM Administrator or Approver), click the node for the domain and then click the **Delegation** tab, select **Link GPOs**, click **Add**, and select users or groups to which you want to assign the permission.

<https://technet.microsoft.com/en-us/library/ee378482.aspx>

### **QUESTION 283**

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named dc1.contoso.com.

You discover that the Default Domain Policy Group Policy object (GPO) and the Default Domain Controllers Policy GPO were deleted. You need to recover the Default Domain Policy and the Default Domain Controllers Policy GPOs.

What should you run?

- A. dcgpofix.exe /target:domain
- B. gpfixup.exe /dc:dc1.contoso.com
- C. dcgpofix.exe /target:both
- D. gptfixup.exe /oldnb:contoso /newnb:dc1

**Correct Answer: C**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

**Dcgpofix** recreates the default Group Policy Objects (GPOs) for a domain.

When restoring the Default Domain Policy GPO or the Default Domain Controllers Policy GPO to their original states, you will lose any changes that you

have made to these GPOs. As a best practice, you should configure the Default Domain Policy GPO only to manage the default Account Policies settings, Password Policy, Account Lockout Policy, and Kerberos Policy. Also as a best practice, you should configure the Default Domain Controllers Policy GPO only to set user rights and audit policies. In this example, you ignore the version of the Active Directory schema so that the **dcgpofix** command is not limited to same schema as the Windows version in which the command was shipped.

```
dcgpofix /ignoreschema /target:Both
```

Parameter	Description
<code>/ignoreschema</code>	Ignores the version of the Active Directory® schema when you run this command. Otherwise, the command only works on the same schema version as the Windows version in which the command was shipped.
<code>/target {Domain   DC   Both}</code>	Specifies which GPO to restore. You can restore the Default Domain Policy GPO, the Default Domain Controllers GPO, or both.
<code>/?</code>	Displays Help at the command prompt.

<https://technet.microsoft.com/en-us/library/hh875588>

#### QUESTION 284

You are hired as a consultant to the ABC Company. The owner of the company complains that she continues to have Desktop wallpaper that she did not choose.

When you speak with the IT team, you find out that a former employee created 20 GPOs and they have not been able to figure out which GPO is changing the owner's Desktop wallpaper.

How can you resolve this issue?

- A. Run the RSoP utility against all forest computer accounts.
- B. Run the RSoP utility against the owner's computer account.
- C. Run the RSoP utility against the owner's user account.
- D. Run the RSoP utility against all domain computer accounts.

**Correct Answer: C**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

An administrator uses logging mode to report on the current state of Group Policy settings. The scope of reports can include Group Policy settings for

various targets, including a computer, a user, or both. The administrator selects combinations of targets in the Resultant Set of Policy Wizard.

In addition to using an empty MMC to access RSoP snap-in, there is another scenario an administrator is just as likely to use for troubleshooting Group Policy settings. An administrator can run RSOP.msc from the command prompt on a client computer to report on the current computer with the current user logged on. In this manner, the administrator avoids having to select targets in the Resultant Set of Policy Wizard.

<https://technet.microsoft.com/en-us/library/cc758010>

#### QUESTION 285

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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

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.

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

#### QUESTION 286

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 8.1 and 10 desktop computers that run Windows XP Service Pack 3 (SP3). All new desktop computers that are added to the domain run Windows 8.1.

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: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

To make sure that each GPO associated with a group can only be applied to computers running the correct version of Windows, use the Group Policy Management MMC snap-in to create and assign **WMI filters** to the GPO. Although you can create a separate membership group for each GPO, you would then have to manage the memberships of the different groups. Instead, use only a single membership group, and let WMI filters automatically ensure the correct GPO is applied to each computer.

<https://technet.microsoft.com/en-us/library/jj717288.aspx>

#### **QUESTION 287**

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. Administrators use client computers that run Windows 8 to perform all management tasks. A central store is configured on a domain controller named DC1. You have a custom administrative template file named App1.admx. App1.admx contains application settings for an application named App1.

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: Configure and manage Group Policy**

## Explanation

### Explanation/Reference:

You can create a central store that provides all administrators who edit domain-based Group Policy Objects (GPOs) access to the same set of Administrative Template files. The central store is an administrator-created folder on SYSVOL that provides a single centralized storage location for all Administrative Template files (ADMX and ADML) for the domain. Once you create the central store, the Group Policy tools use only the ADMX files in the central store and ignore ADMX versions stored locally. The central store is optional; if you do not create it, the Group Policy tools use the local ADMX files. The root folder for the central store must be named PolicyDefinitions (that is, %SystemRoot%\SYSVOL\domain\policies\PolicyDefinitions).

<https://technet.microsoft.com/en-us/library/gg699412.aspx>

In Group Policy for versions of Windows earlier than Windows Vista, if you change Administrative template policy settings on local computers, the Sysvol share on a domain controller within your domain is automatically updated with the new .ADM files. In turn, those changes are replicated to all other domain controllers in the domain. This might result in increased network load and storage requirements. 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.

<http://support.microsoft.com/kb/929841>

### QUESTION 288

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains two organizational units (OUs) named OU1 and OU2 in the root of the domain.

Two Group Policy objects (GPOs) named GPO1 and GPO2 are created. GPO1 is linked to OU1. GPO2 is linked to OU2. OU1 contains a client computer named Computer1. OU2 contains a user named User1.

You need to ensure that the GPOs applied to Computer1 are applied to User1 when User1 logs on.

What should you configure?

- A. The GPO Status
- B. GPO links
- C. The Enforced setting
- D. Security Filtering

**Correct Answer: D**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

GPOs cannot be linked directly to users, computers, or security groups. They can only be linked to sites, domains and organizational units. However, by using security filtering, you can narrow the scope of a GPO so that it applies only to a single group, user, or computer.

[https://technet.microsoft.com/en-us/library/Cc781988\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Cc781988(v=WS.10).aspx)

**QUESTION 289**

You administer a Microsoft Windows Server 2012 R2 domain named ABC.com. The ABC.com domain has several administrative templates that are applied via a Group Policy object (GPO).

You must provide a solution for reviewing active and inactive Group Policy settings containing comments.

You open the Group Policy settings. How would you apply the appropriate filters to accomplish this task? (Choose all that apply.)

- A. You should select the Enable Keyword Filters option.
- B. You should select the Enable Requirements Filters option.
- C. You should set the Managed Filter Options to Any.
- D. You should set the Configured Filter Options to Any.
- E. You should set the Commented Filter Options to Any.
- F. You should set the Managed Filter Options to Yes.
- G. You should set the Configured Filter Options to Yes.
- H. You should set the Commented Filter Options to Yes.
- I. You should set the Managed Filter Options to No.
- J. You should set the Configured Filter Options to No.
- K. You should set the Commented Filter Options to No.

**Correct Answer:** CDH

**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

The Local Group Policy Editor provides the option to filter Administrative Template policy settings based on:

- Managed, Configured, or Commented policy settings.
- Keywords within the title, Help text, or comment of policy settings.
- Platform or application requirements of policy settings.



<https://technet.microsoft.com/en-us/library/cc772295.aspx>

### Filter with Property Filters

There are three inclusive property filters that you can use to filter Administrative Templates. These property filters include:

- Managed
- Configured
- Commented

The **Managed** property filter has three states: **Any**, **Yes**, and **No**. Setting this property filter to **Any** causes the Local Group Policy Editor to display all Administrative Template policy settings. Setting this property filter to **Yes** causes the editor to show only managed Administrative Template policy settings, hiding all unmanaged Administrative Template policy settings. Setting this property filter to **No** causes the editor to show only unmanaged Administrative Template policy settings, hiding all managed Administrative Template policy settings.

The **Configured** property filter has three states: **Any**, **Yes**, and **No**. Setting this property filter to **Any** causes the Local Group Policy Editor to display all Administrative Template policy settings and is the default setting for this filter. Setting this property filter to **Yes** causes the editor to show only configured Administrative Template policy settings, hiding not configured policy settings. Setting this property filter to **No** causes the editor to show only not configured Administrative Template policy settings, hiding configured policy settings.

The **Commented** property filter has three states: **Any**, **Yes**, and **No**. Setting this property filter to **Any** causes the Local Group Policy Editor to display all Administrative Template policy settings and is the default setting for this filter. Setting this proper filter to **Yes** causes the editor to show only commented Administrative Template policy settings, hiding policy settings without comments. Setting this property filter to **No** causes the editor to show only Administrative Template policy settings without comments, hiding commented policy settings.

<https://technet.microsoft.com/en-us/library/dd759104.aspx>

### QUESTION 290

You administer a Microsoft Windows Server 2012 R2 domain named ABC.com. ABC.com makes use of Windows Power Shell scripts for configuring settings for network users. These settings are applied when the users log on to their client computers.

You notice users are able to use their client computers before the scripts have finished running. ABC.com wants you to make sure the scripts are finished running before the users can use their computers.

What action should you take?

- A. You should open Group Policy Management Editor and enable the Run logon scripts asynchronously policy.
- B. You should open Group Policy Management Editor and enable the Run logon scripts synchronously policy.
- C. You should open Group Policy Management Editor and enable the Run Windows PowerShell scripts first at user logon, logoff.
- D. You should open Group Policy Management Editor and enable the Run startup scripts asynchronously policy.
- E. You should open Group Policy Management Editor and configure the Specify maximum wait time for Group Policy scripts setting.

**Correct Answer:** B

**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

**Run logon scripts synchronously**

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

<https://technet.microsoft.com/en-us/library/Cc958585.aspx>

**QUESTION 291**

You work as a Network Administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain named ABC.com. All servers in the ABC.com domain have Microsoft Windows Server 2012 R2 installed.

A group policy object (GPO) is assigned to an organizational unit (OU) named Sales. The GPO assigns several settings to the computers in the Sales department.

You unlink the GPO from the Sales OU. You discover that some of the settings applied by the GPO are still in effect on the Sales computers while other settings applied by the GPO have been removed.

Which of the following statements is true?

- A. The Restricted Groups security settings still in effect.
- B. The unmanaged Administrative Template settings are still in effect.
- C. The managed Administrative Template settings are still in effect.
- D. The System Services security settings have been removed.

**Correct Answer:** B

**Section:** Configure and manage Group Policy

**Explanation**

**Explanation/Reference:**

The Group Policy Client service does not govern unmanaged policy settings. These policy settings are persistent. The Group Policy Client service does not remove unmanaged policy settings, even if the policy setting is not within scope of the user or computer. Typically, you use these types of policy settings to configure options for operating system components that are not policy enabled. You can also use unmanaged policy settings for application settings.

<https://technet.microsoft.com/en-us/library/dd759104.aspx>

#### **QUESTION 292**

You work as a Network Administrator at ABC.com. ABC.com has an Active Directory Domain Services (AD DS) domain named ABC.com. All servers in the ABC.com domain have Microsoft Windows Server 2012 R2 installed. All user and computer accounts for the company's Sales department are located in an organizational unit named Sales.

You must configure group policy object (GPO) for the Sales OU. You download updated administrative template files. You then configure a Central Store on a domain controller. However, when you open a new GPO for editing using the Group Policy Editor console, you discover that no administrative templates are listed under Computer Configuration \ Administrative Templates.

How can you view the administrative templates in the GPO?

- A. You should enable the Computer settings of the GPO.
- B. You should copy the .admx and .adml files from %Windir%\Policydefinitions to the central store.
- C. You should link the GPO to the Sales OU.
- D. You should modify the Security Filtering of the GPO.

**Correct Answer: B**

**Section: Configure and manage Group Policy**

**Explanation**

**Explanation/Reference:**

Administrative templates files in Windows Server 2008 and Windows Vista are divided into .ADMX (language-neutral) and .ADML (language-specific) files. These two file formats replace the .ADM file format used in earlier versions of Windows, which used a proprietary markup language. .ADML files are XML-based ADM Language files that are stored in a language-specific folder. For example, English (United States) .ADML files are stored in a folder that is named "en-US." By default, the %Systemroot%\PolicyDefinitions folder on a local computer stores all .ADMX files, and .ADML files for all languages that are enabled on the computer.

Two primary benefits are gained from creating and using an Administrative template central store. The first benefit is a replicated central storage location for domain Administrative templates. The GPMC included with Windows Server 2008 always uses an Administrative template central store over the local versions of the Administrative templates. This allows you to provide one set of approved Administrative templates for the entire domain.

[https://technet.microsoft.com/en-us/library/cc754948\(WS.10\).aspx](https://technet.microsoft.com/en-us/library/cc754948(WS.10).aspx)

#### **QUESTION 293**

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains an organizational unit (OU) named OU1. OU1 contains an OU named OU2. OU2 contains a user named User1. User1 is the member of a group named Group1. Group1 is in the Users container.

You create five Group Policy objects (GPO). The GPOs are configured as shown in the following table.

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

The Authenticated Users group is assigned the default permissions to all of the GPOs. There are no site-level GPOs.

You need to identify which three GPOs will be applied to User1 and in which order the GPOs will be applied to User1.

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

**Select and Place:**

The interface shows a list of GPOs on the left and an empty answer area on the right. The GPOs are: GPO5, GPO3, GPO2, GPO1, and GPO4.

**Correct Answer:**



## Section: Configure and manage Group Policy

### Explanation

#### Explanation/Reference:

Group Policy settings are processed in the following order:

1. **Local Group Policy object**—Each computer has exactly one Group Policy object that is stored locally. This processes for both computer and user Group Policy processing.
2. **Site**—Any GPOs that have been linked to the site that the computer belongs to are processed next. Processing is in the order that is specified by the administrator, on the **Linked Group Policy Objects** tab for the site in Group Policy Management Console (GPMC). The GPO with the lowest **link order** is processed last, and therefore has the highest precedence.
3. **Domain**—Processing of multiple domain-linked GPOs is in the order specified by the administrator, on the **Linked Group Policy Objects** tab for the domain in GPMC. The GPO with the lowest **link order** is processed last, and therefore has the highest precedence.
4. **Organizational units**—GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

The default order for processing settings is subject to the following exceptions:

- A GPO link may be **enforced**, or **disabled**, or both. By default, a GPO link is neither enforced nor disabled.
- A GPO may have its user settings disabled, its computer settings disabled, or all settings disabled. By default, neither user settings nor computer settings are disabled on a GPO.
- An organizational unit or a domain may have **Block Inheritance** set. By default, **Block Inheritance** is not set.

<https://technet.microsoft.com/en-us/library/cc785665>

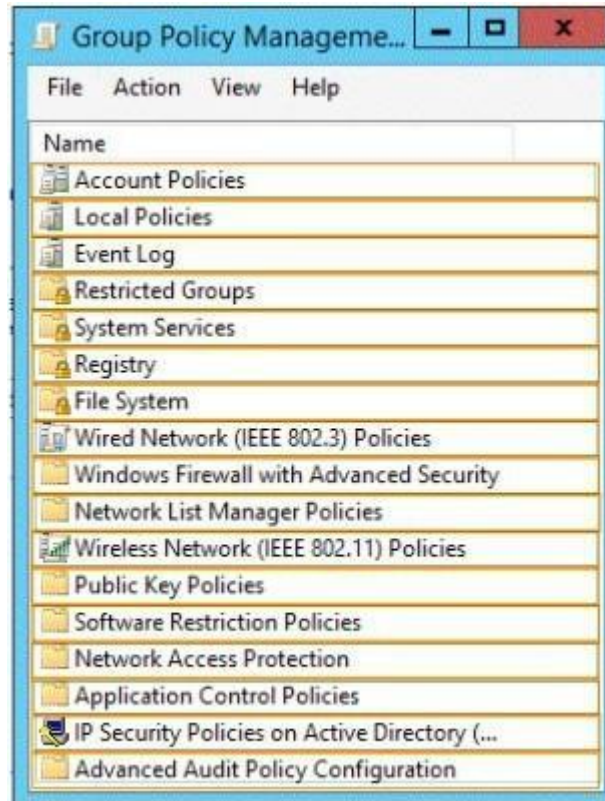
#### **QUESTION 294**

Your network contains an Active Directory domain named contoso.com. All client computers are configured as DHCP clients.

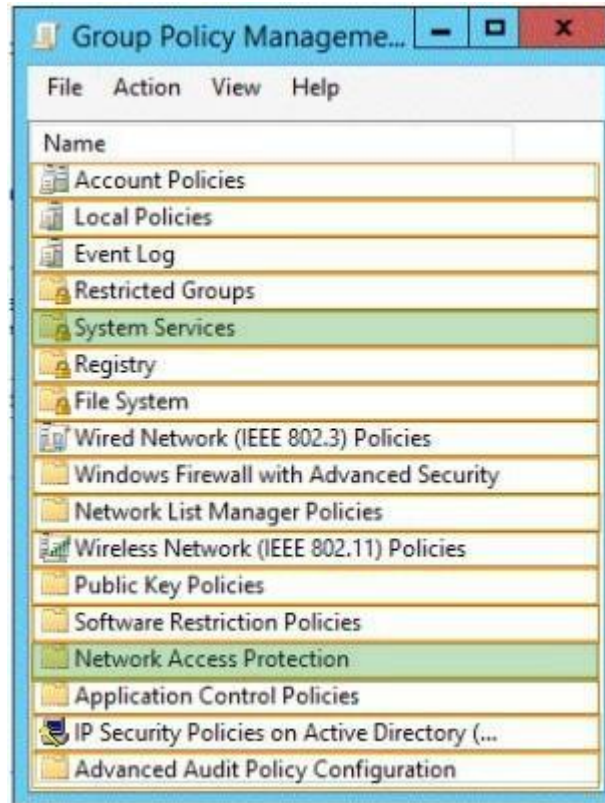
You link a Group Policy object (GPO) named GPO1 to an organizational unit (OU) that contains all of the client computer accounts. You need to ensure that Network Access Protection (NAP) compliance is evaluated on all of the client computers.

Which two settings should you configure in GPO1? To answer, select the appropriate two settings in the answer area.

**Hot Area:**



**Correct Answer:**



**Section: Configure and manage Group Policy**  
**Explanation**

**Explanation/Reference:**

To configure the NAP Agent service, in the Group Policy Management Editor tree, open Computer Configuration\Policies\Security Settings\ **System Services**. In the details pane, double-click **Network Access Protection Agent**.

<https://msdn.microsoft.com/en-us/library/dd314159>

**QUESTION 295**

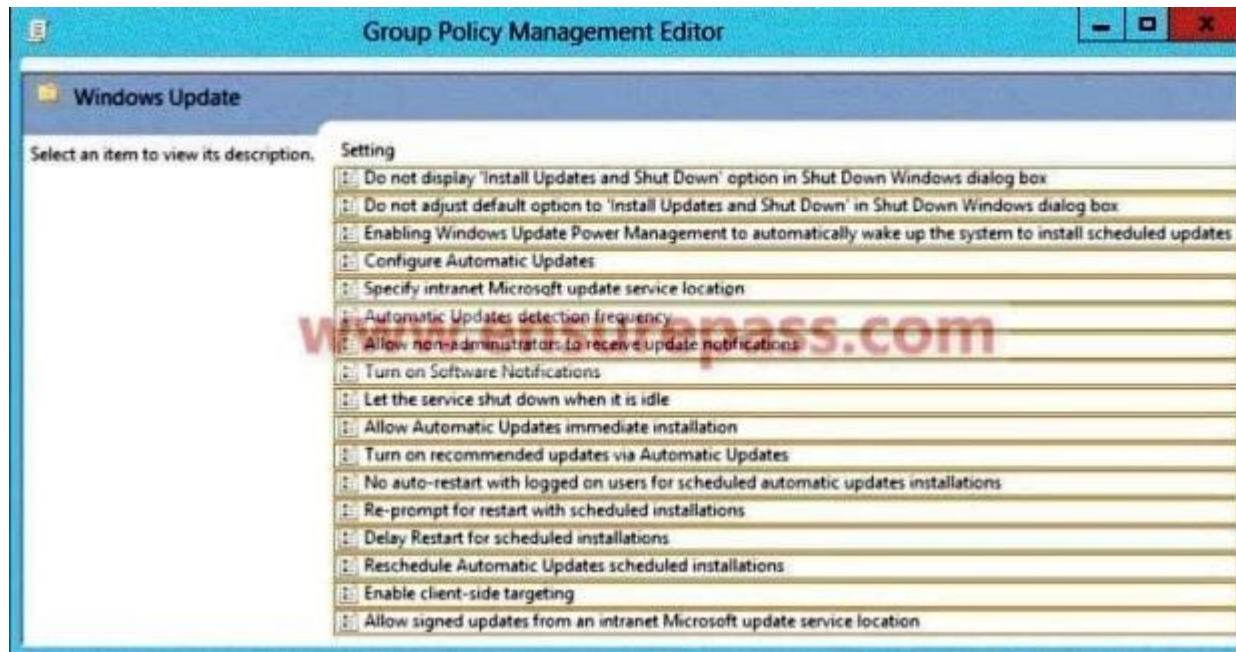
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Server Update Services server role installed.



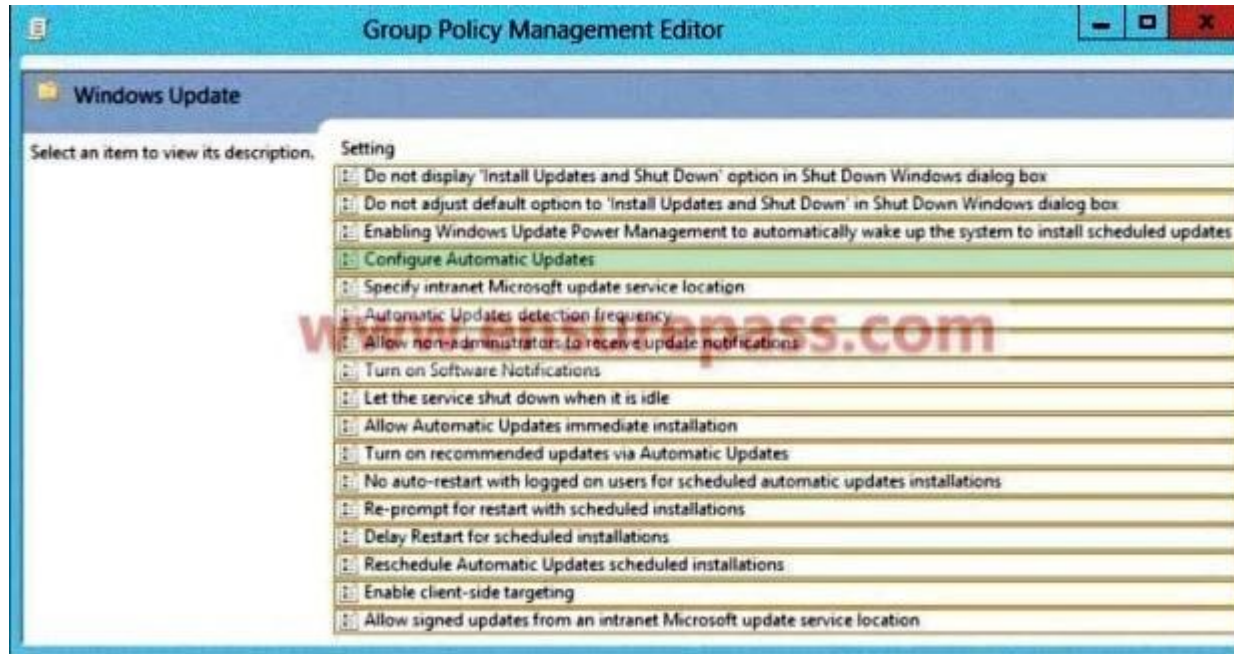
You have a Group Policy object (GPO) that configures the Windows Update settings. You need to modify the GPO to configure all client computers to install Windows updates every Wednesday at 01:00.

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

**Hot Area:**



**Correct Answer:**



## Section: Configure and manage Group Policy

### Explanation

#### Explanation/Reference:

#### Configure Automatic Updates

To use this setting, select **Enabled**, and then in **Options** under **Configure automatic updating**, select one of the options (2, 3, 4, or 5).

#### 4 – Auto download and schedule the install

You can specify the schedule by using the options in this Group Policy setting. If no schedule is specified, the default schedule for all installations will be every day at 3:00 A.M. If any updates require a restart to complete the installation, Windows will restart the computer automatically. (If a user is signed in to the computer when Windows is ready to restart, the user will be notified and given the option to delay the restart.)

<https://technet.microsoft.com/en-us/library/dn595129.aspx>

#### QUESTION 296

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 Windows Server Update Services server role installed.

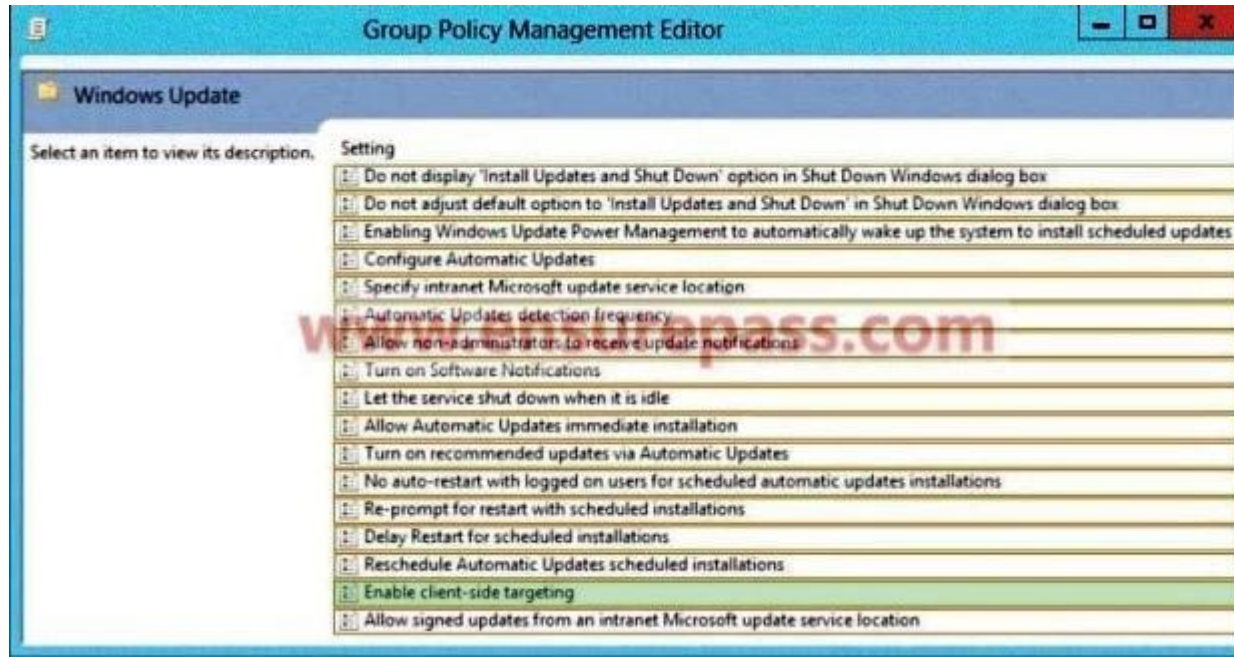
You need to use the Group Policy object (GPO) to assign members to a computer group.

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

**Hot Area:**



**Correct Answer:**



## Section: Configure and manage Group Policy

### Explanation

#### Explanation/Reference:

#### Enable client-side targeting

Specifies that the specified target group information is sent to WSUS, which uses it to determine which updates should be deployed to this computer. If WSUS supports multiple target groups, you can use this policy to specify multiple group names, separated by semicolons, if you have added the target group names in the Computer group list in WSUS. Otherwise, a single group must be specified.

<https://technet.microsoft.com/en-us/library/dn595129.aspx>

### QUESTION 297

Your network contains an Active Directory domain named contoso.com. You have several Windows PowerShell scripts that execute when client computers start.

When a client computer starts, you discover that it takes a long time before users are prompted to log on. You need to reduce the amount of time it takes for the client computers to start. The solution must not prevent scripts from completing successfully.



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

**Hot Area:**



**Correct Answer:**



## Section: Configure and manage Group Policy

### Explanation

#### Explanation/Reference:

#### Run startup scripts asynchronously

Lets the system run startup scripts simultaneously.

*Startup scripts* are batch files that run before the user is invited to log on. By default, the system waits for each startup script to complete before it runs the next startup script.

If you enable this policy, the system does not coordinate the running of startup scripts. As a result, startup scripts can run simultaneously.

If you disable this policy or do not configure it, a startup script cannot run until the previous script is complete.

<https://technet.microsoft.com/en-us/library/cc939423.aspx>

#### Run startup scripts synchronously

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

If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing

is complete before the user starts working, but **it can delay the appearance of the desktop**.

<https://technet.microsoft.com/en-us/library/cc958585.aspx>

#### QUESTION 298

Your network contains an Active Directory domain named contoso.com. You have several Windows PowerShell scripts that execute when users log on to their client computer.

You need to ensure that all of the scripts execute completely before the users can access their desktop.

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

**Hot Area:**



**Correct Answer:**



## Section: Configure and manage Group Policy

### Explanation

#### Explanation/Reference:

#### Run startup scripts synchronously

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

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

<https://technet.microsoft.com/en-us/library/cc958585.aspx>

#### Run startup scripts asynchronously

Lets the system run startup scripts simultaneously.

*Startup scripts* are batch files that run before the user is invited to log on. By default, the system waits for each startup script to complete before it runs the next startup script.

If you enable this policy, the system does not coordinate the running of startup scripts. As a result, startup scripts can run simultaneously.



If you disable this policy or do not configure it, a startup script cannot run until the previous script is complete.

<https://technet.microsoft.com/en-us/library/cc939423.aspx>

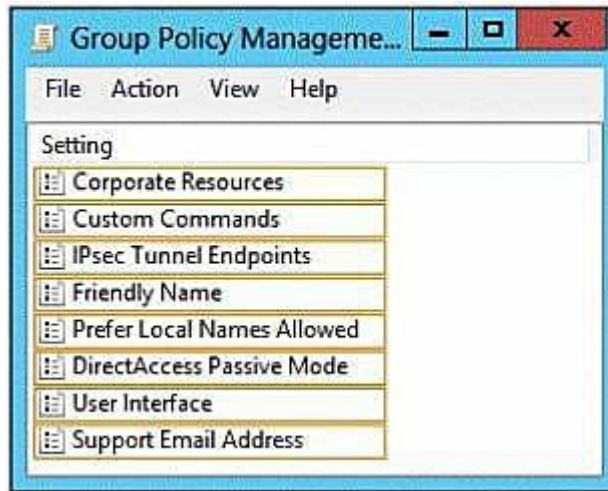
#### QUESTION 299

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1. Your company implements DirectAccess.

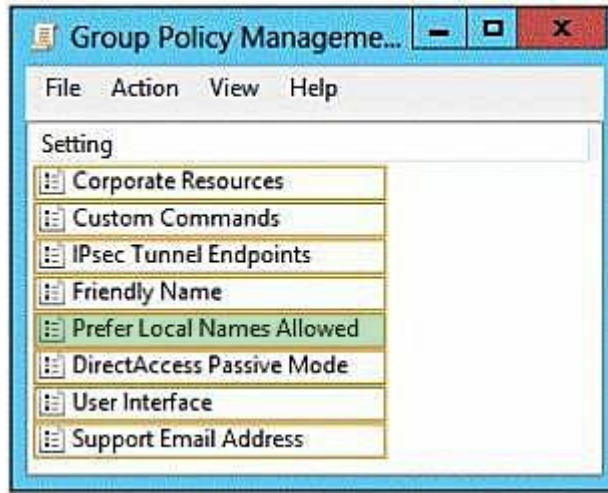
A user named User1 works at a customer's office. The customer's office contains a server named Server1. When User1 attempts to connect to Server1, User1 connects to Server1 in adatum.com. You need to provide User1 with the ability to connect to Server1 in the customer's office.

Which Group Policy option should you configure? To answer, select the appropriate option in the answer area.

**Hot Area:**



**Correct Answer:**



## Section: Configure and manage Group Policy

### Explanation

#### Explanation/Reference:

#### Configuring the DirectAccess Connectivity Assistant (DCA)

To allow users to resolve single label names on the local subnet, rather than resolving them on the intranet select **Allow users to use local name resolution**. When selected, the DirectAccess client has an option to **Prefer Local Names** in the client-side DCA.

<https://technet.microsoft.com/en-us/library/gg274289.aspx>

### QUESTION 300

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 three settings in the answer area.

#### Hot Area:

**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
Any	Any	Any
Yes	Yes	Yes
No	No	No

☐ 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

Correct Answer:

**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
Yes	Yes	Yes
No	No	No

☐ 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

**Section: Configure and manage Group Policy**  
**Explanation**

## Explanation/Reference:

The Local Group Policy Editor provides the option to filter Administrative Template policy settings based on:

- Managed, Configured, or Commented policy settings.
- Keywords within the title, Help text, or comment of policy settings.
- Platform or application requirements of policy settings.

<https://technet.microsoft.com/en-us/library/cc772295.aspx>

## Filter with Property Filters

There are three inclusive property filters that you can use to filter Administrative Templates. These property filters include:

- Managed
- Configured
- Commented

The **Managed** property filter has three states: **Any**, **Yes**, and **No**. Setting this property filter to **Any** causes the Local Group Policy Editor to display all Administrative Template policy settings. Setting this property filter to **Yes** causes the editor to show only managed Administrative Template policy settings, hiding all unmanaged Administrative Template policy settings. Setting this property filter to **No** causes the editor to show only unmanaged Administrative Template policy settings, hiding all managed Administrative Template policy settings.

The **Configured** property filter has three states: **Any**, **Yes**, and **No**. Setting this property filter to **Any** causes the Local Group Policy Editor to display all Administrative Template policy settings and is the default setting for this filter. Setting this property filter to **Yes** causes the editor to show only configured Administrative Template policy settings, hiding not configured policy settings. Setting this property filter to **No** causes the editor to show only not configured Administrative Template policy settings, hiding configured policy settings.

The **Commented** property filter has three states: **Any**, **Yes**, and **No**. Setting this property filter to **Any** causes the Local Group Policy Editor to display all Administrative Template policy settings and is the default setting for this filter. Setting this proper filter to **Yes** causes the editor to show only commented Administrative Template policy settings, hiding policy settings without comments. Setting this property filter to **No** causes the editor to show only Administrative Template policy settings without comments, hiding commented policy settings.

<https://technet.microsoft.com/en-us/library/dd759104.aspx>