



# Microsoft

## Exam Questions 70-411

Administering Windows Server 2012

### NEW QUESTION 1

- (Topic 1)

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

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

Server1 provides VPN access to external users.

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

What should you run?

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

**Answer: C**

#### Explanation:

Add-RemoteAccessRadius

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

AccountingOnOffMsg<String>

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

? Enabled.

? Disabled. This is the default value.

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

### NEW QUESTION 2

- (Topic 1)

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

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

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

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

**Answer: C**

#### Explanation:

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

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

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

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

auditpol /resourceSACL

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

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

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

References:

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

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

### NEW QUESTION 3

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 P.2.

Server1 has the Network Policy and Access Services server role installed.

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

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

Which authentication method should you identify?

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

**Answer: C**

#### Explanation:

802.1X uses EAP, EAP-TLS, EAP-MS-CHAP v2, and PEAP authentication methods:

? EAP (Extensible Authentication Protocol) uses an arbitrary authentication method, such as certificates, smart cards, or credentials.

? EAP-TLS (EAP-Transport Layer Security) is an EAP type that is used in certificate-based security environments, and it provides the strongest authentication and key determination method.

? EAP-MS-CHAP v2 (EAP-Microsoft Challenge Handshake Authentication Protocol

version 2) is a mutual authentication method that supports password-based user or computer authentication.

? PEAP (Protected EAP) is an authentication method that uses TLS to enhance the security of other EAP authentication protocols.

#### NEW QUESTION 4

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a read-only domain controller (RODC) named R0DC1. You create a global group named RODC\_Admins. You need to provide the members of RODC\_Admins with the ability to manage the hardware and the software on R0DC1. The solution must not provide RODC\_Admins with the ability to manage Active Directory objects. What should you do?

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

**Answer: D**

#### Explanation:

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

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

#### NEW QUESTION 5

- (Topic 1)

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

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

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

- A. Rid master
- B. Domain naming master
- C. PDC emulator
- D. Infrastructure master

**Answer: C**

#### Explanation:

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

Reference:

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

#### NEW QUESTION 6

- (Topic 1)

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

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

You need to ensure that end-to-end encryption is used between clients and Server2 when the clients connect to the network by using DirectAccess. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Answer:** BE

**Explanation:**

Unsure about these answers:

? A public key infrastructure must be deployed.

? Windows Firewall must be enabled on all profiles.

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

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

Windows Server® 2012 R2

Windows 8.1 Enterprise

Windows Server® 2012

Windows 8 Enterprise Windows Server® 2008 R2 Windows 7 Ultimate

Windows 7 Enterprise

? Force tunnel configuration is not supported with KerbProxy authentication.

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

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

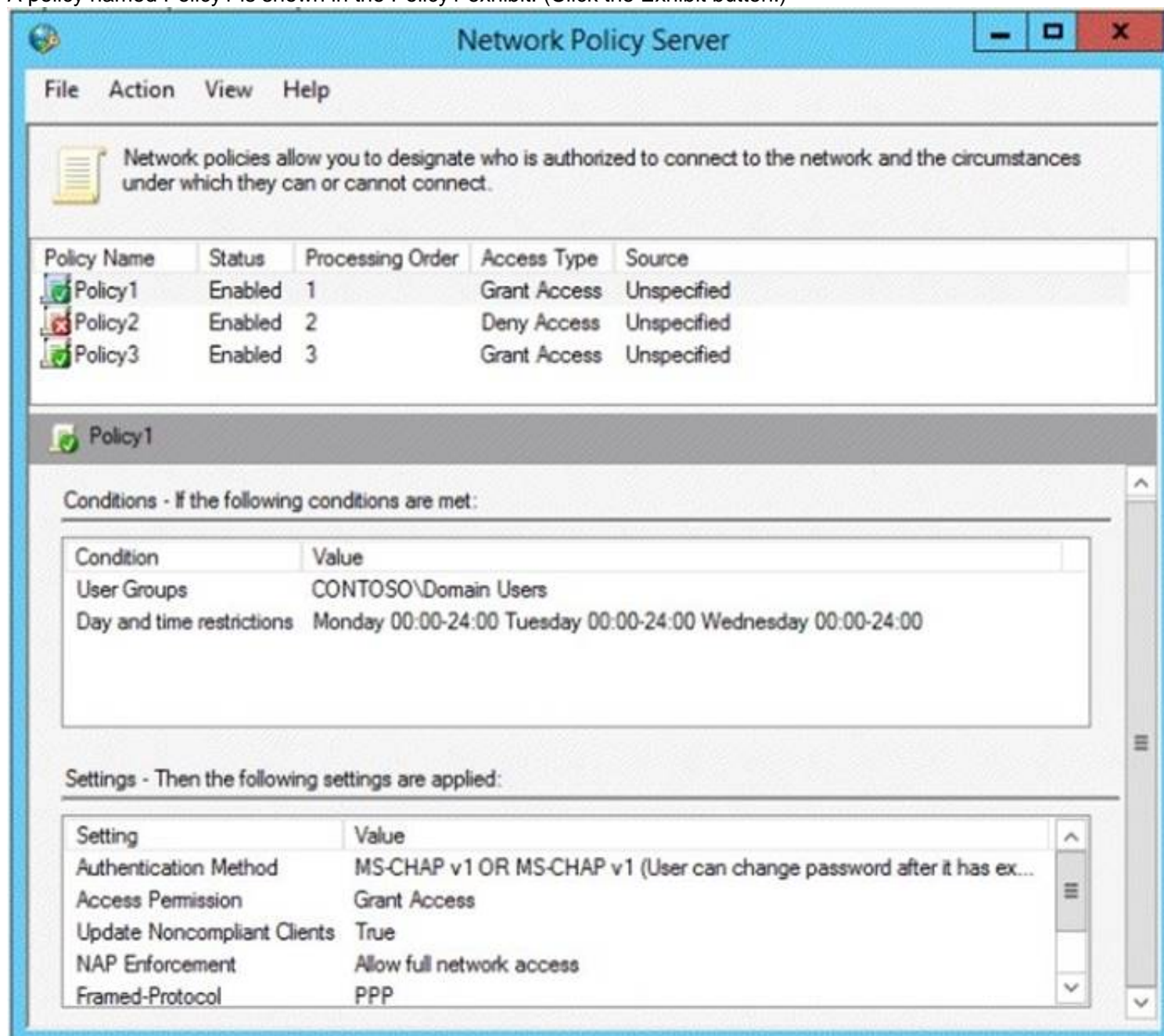
**NEW QUESTION 7**

HOTSPOT - (Topic 1)

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

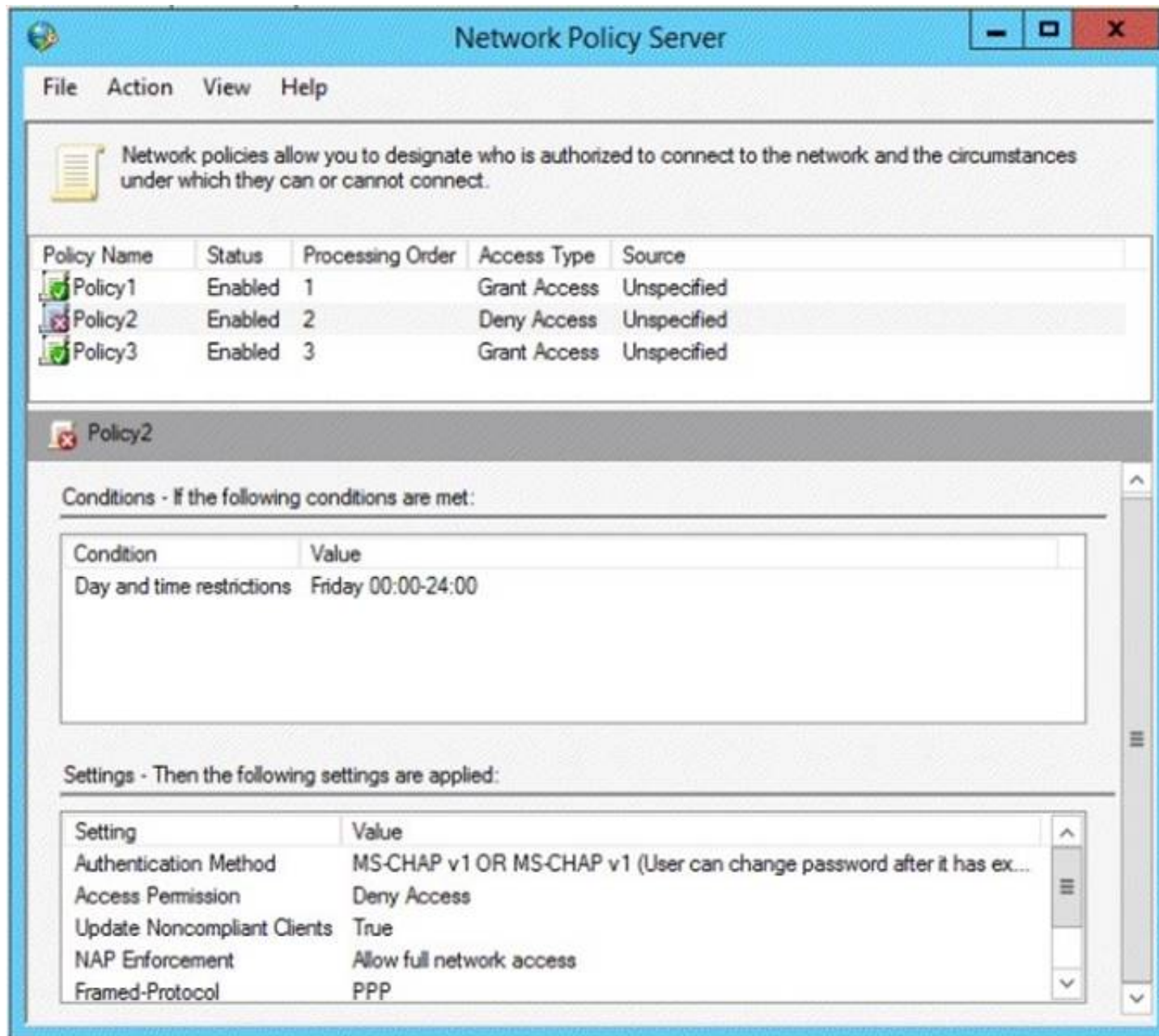
The Network Access Permission for User1 is set to Control access through NPS Network Policy. The Network Access Permission for User2 is set to Allow access.

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

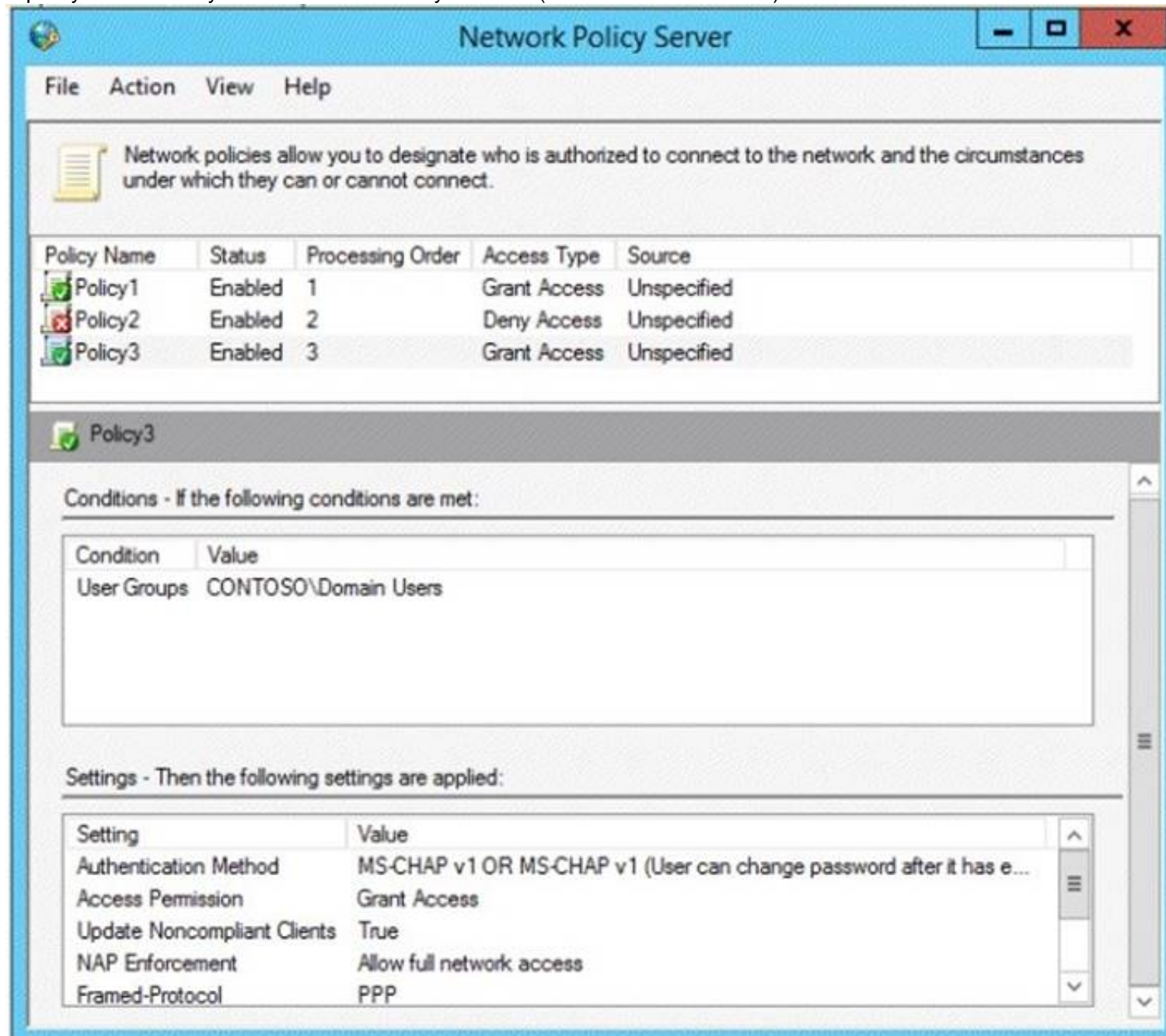


A policy named Policy2 is shown in the Policy2 exhibit. (Click the Exhibit button.)





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



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

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

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

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

### NEW QUESTION 8

HOTSPOT - (Topic 1)

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

User name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

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

Answer Area

User1:

User2:

User3:

#### Answer Area

User1:   
Policy1  
Policy2  
Policy3

User2:   
Policy1  
Policy2  
Policy3

User3:   
Policy1  
Policy2  
Policy3

- A. Mastered  
B. Not Mastered

**Answer:** A

#### Explanation:

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

Policies are processed in this order:

-Policy2 (applies only to members of Group1)

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

-Policy3 (applies only to members of Group2)

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

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

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

#### NEW QUESTION 9

- (Topic 1)

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

You deploy a new domain controller named DC1 that runs Windows Server 2012 R2. You log on to DC1 by using an account that is a member of the Domain Admins group. You discover that you cannot create Password Settings objects (PSOs) by using Active

Directory Administrative Center.

You need to ensure that you can create PSOs from Active Directory Administrative Center. What should you do?

- A. Modify the membership of the Group Policy Creator Owners group.  
B. Transfer the PDC emulator operations master role to DC1.  
C. Upgrade all of the domain controllers that run Window Server 2008.  
D. Raise the functional level of the domain.

**Answer:** D

#### Explanation:

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

Step 1: Create a PSO

Applies To: Windows Server 2008, Windows Server 2008 R2

ce:

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

#### NEW QUESTION 10

DRAG DROP - (Topic 1)

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

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

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



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

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

References:

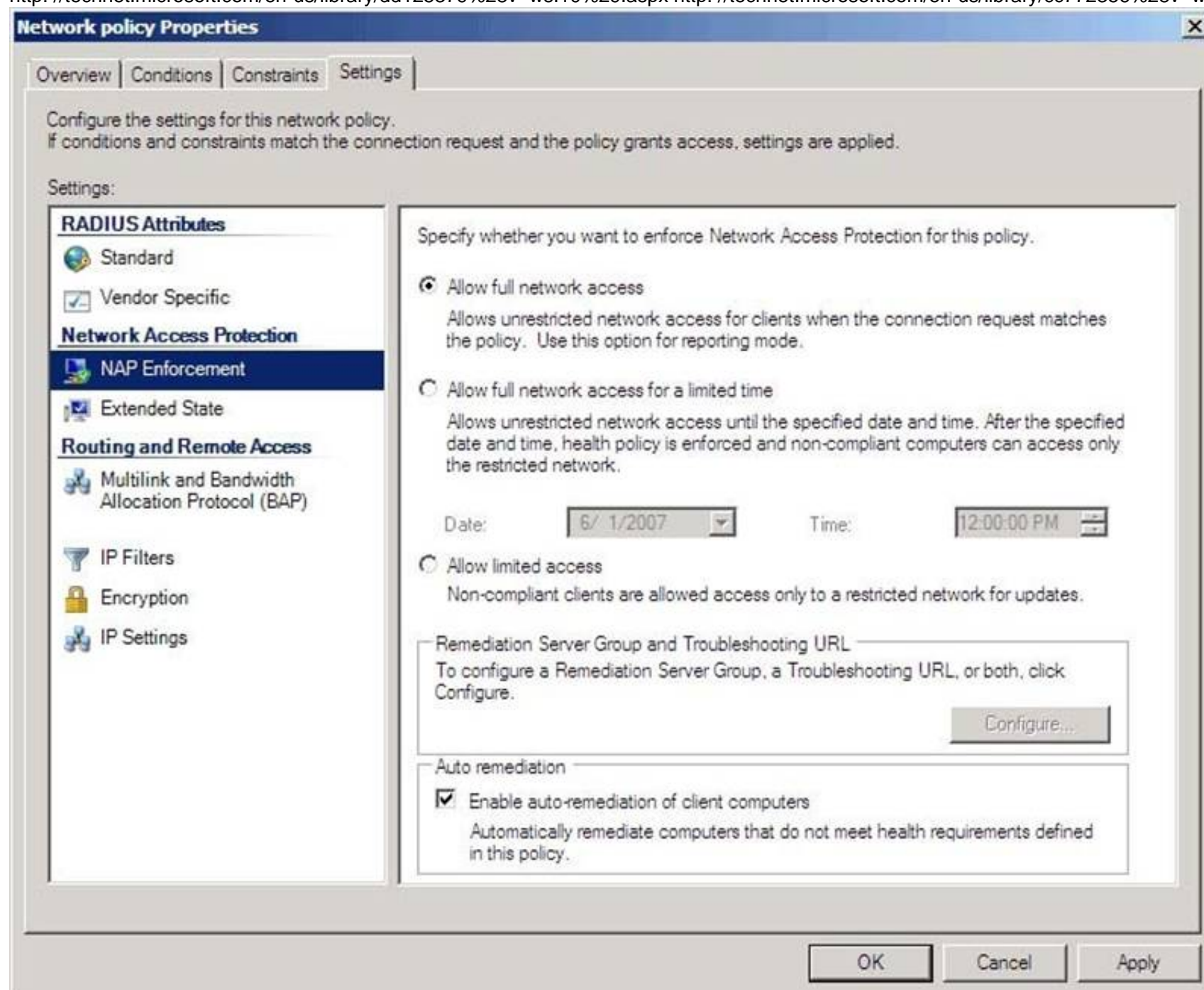
<http://technet.microsoft.com/es-es/library/dd314198%28v=ws.10%29.aspx>

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

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

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

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



**Network policy Properties**

Overview | Conditions | Constraints | Settings

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

Settings:

**RADIUS Attributes**

- Standard
- ☒ Vendor Specific

**Network Access Protection**

- NAP Enforcement**
  - ☒ Extended State

**Routing and Remote Access**

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

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

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

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

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

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

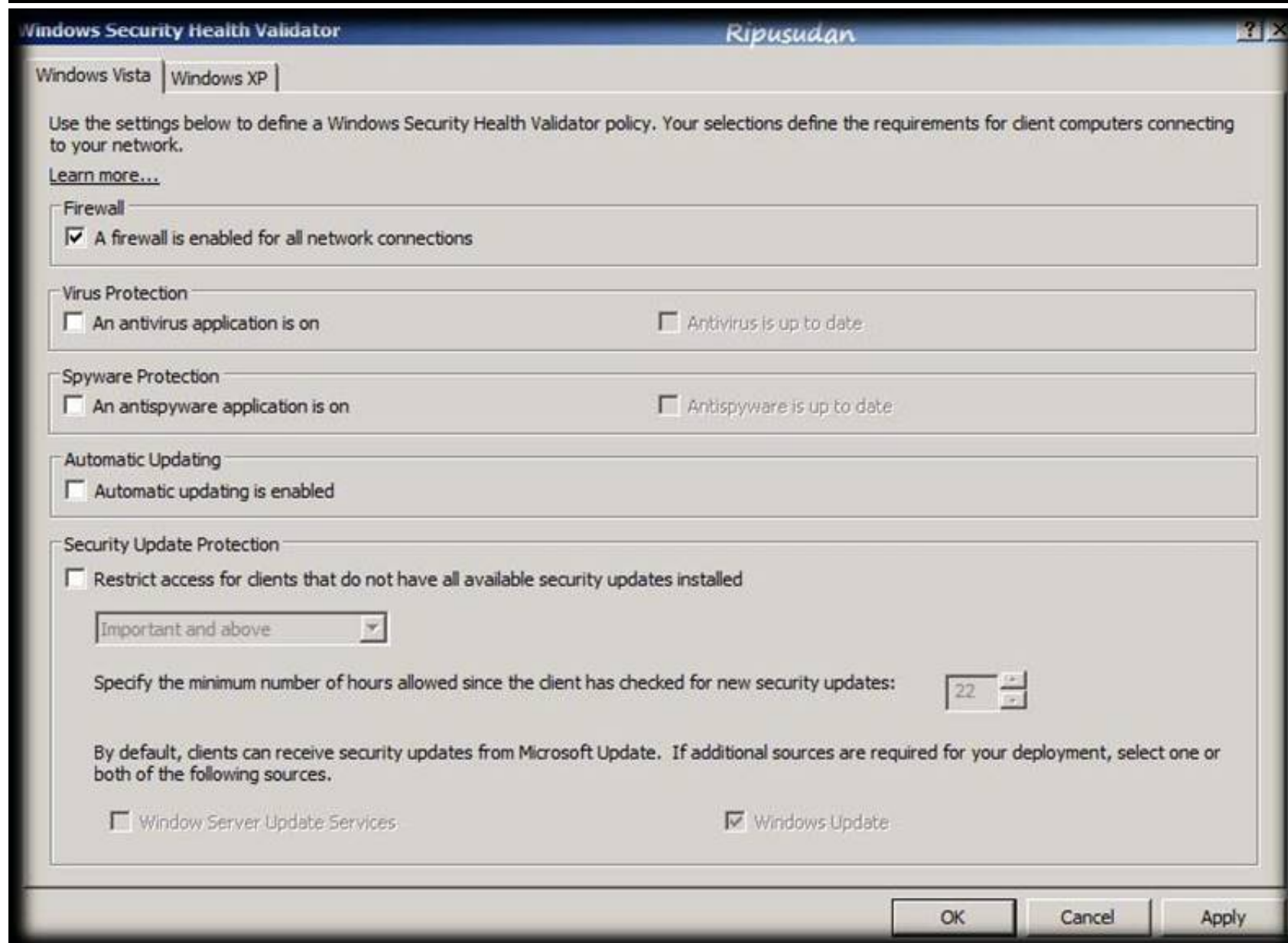
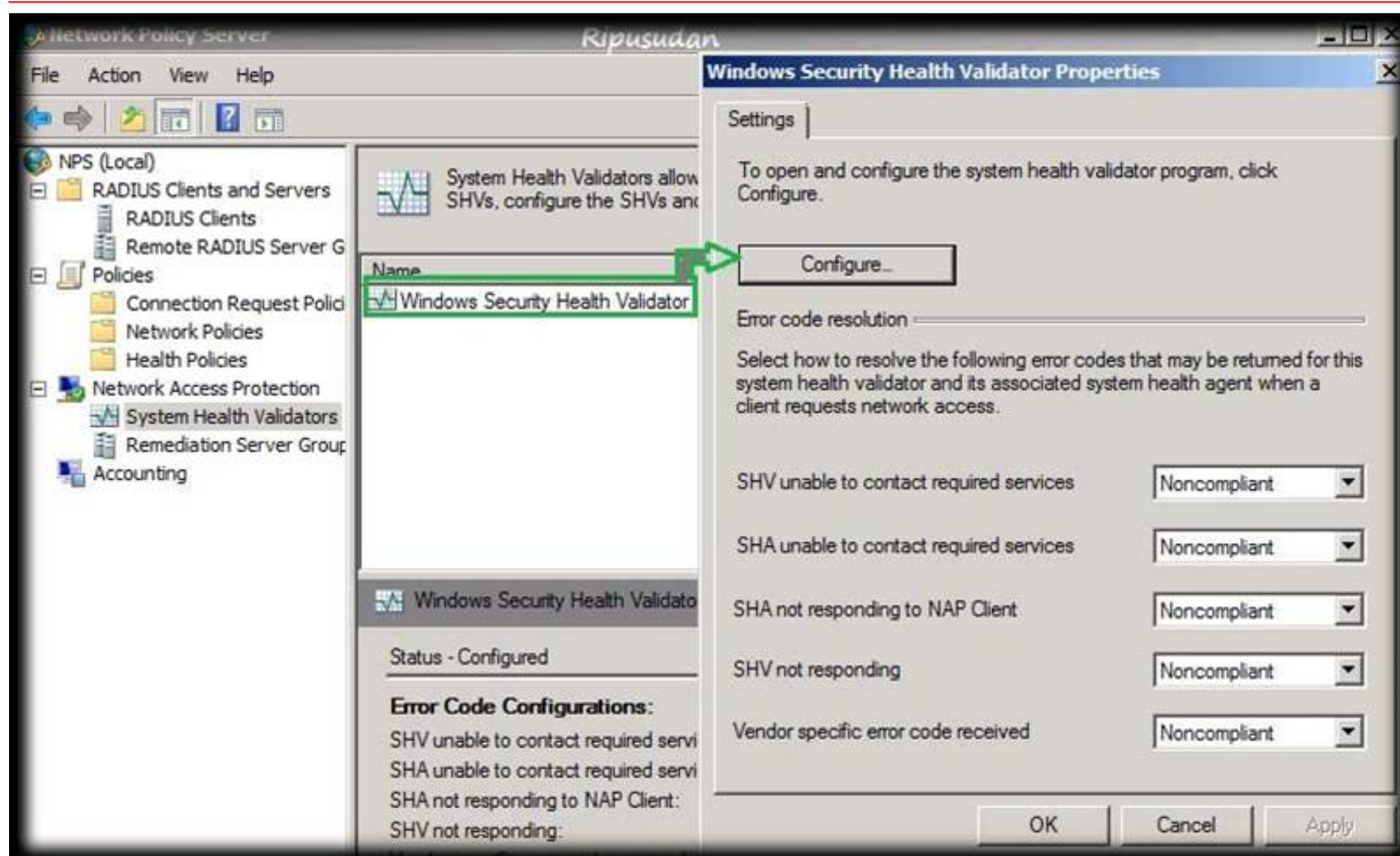
Remediation Server Group and Troubleshooting URL  
 To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

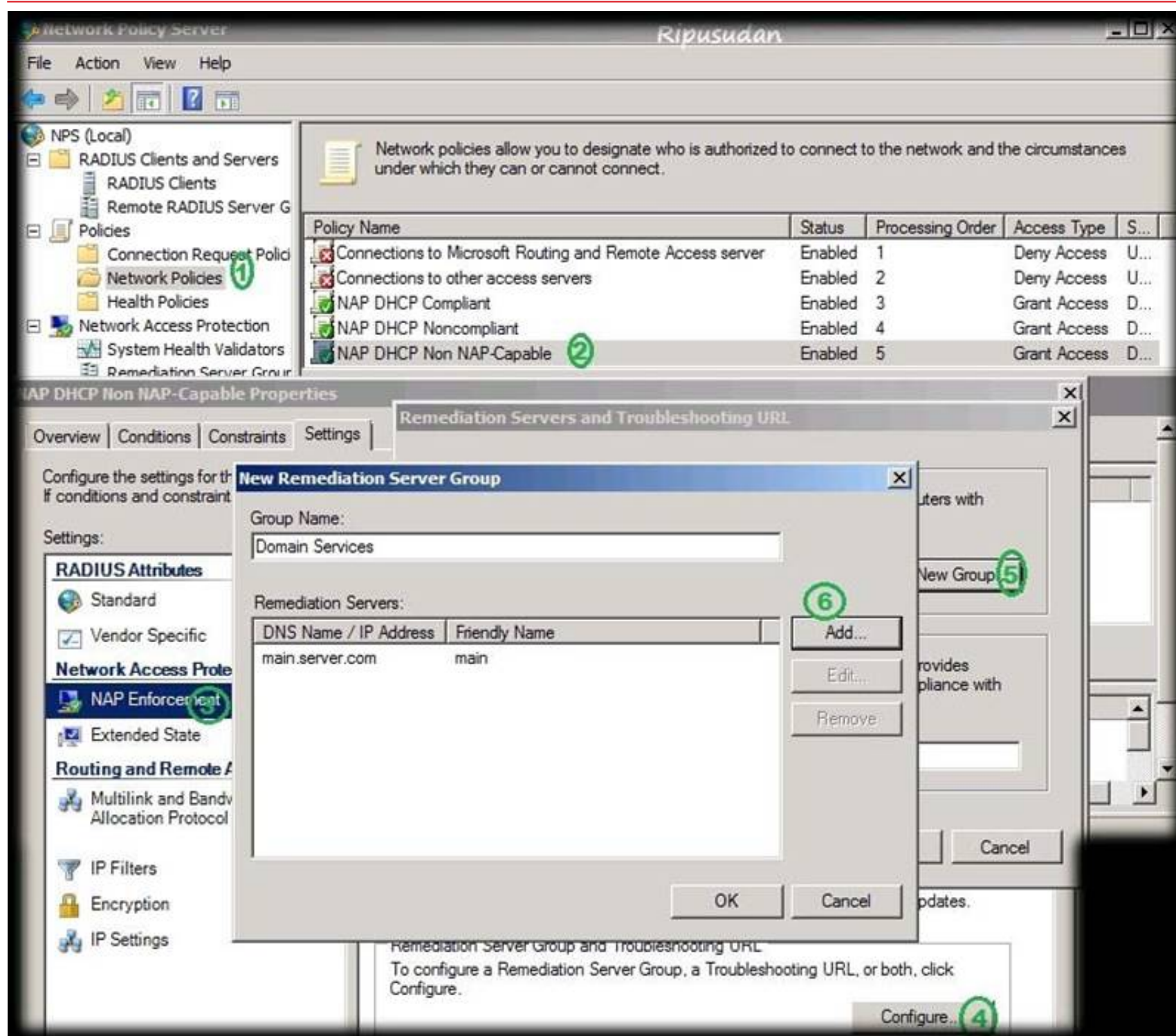
Auto remediation

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

OK Cancel Apply







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

\* Example measurements of health include:

The operational status of Windows Firewall. Is the firewall enabled or disabled?

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

#### NEW QUESTION 10

- (Topic 1)

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

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

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

What should you configure?

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

**Answer: B**

#### Explanation:

To configure data management for a Data Collector Set

1. In Windows Performance Monitor, expand Data Collector Sets and click User Defined.
2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click Data Manager.
3. On the Data Manager tab, you can accept the default values or make changes according to your data retention policy. See the table below for details on each option.

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

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

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

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

#### NEW QUESTION 14

- (Topic 1)

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



The domain 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. Gpedi
- F. msc
- G. Import-GPO
- H. Restore-GPO
- I. Set-GPInheritance
- J. Set-GPLink
- K. Set-GPPermission
- L. Gpupdate
- M. Add-ADGroupMember

**Answer:** J

**Explanation:**

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

-Replace <SwitchParameter>

Specifies that the existing permission level for the group or user is removed before the new permission level is set. If a security principal is already granted a permission level that is higher than the specified permission level and you do not use the Replace parameter, no change is made.

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

**NEW QUESTION 18**

- (Topic 1)

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

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

Which tool should you use?

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

**Answer:** C

**NEW QUESTION 19**

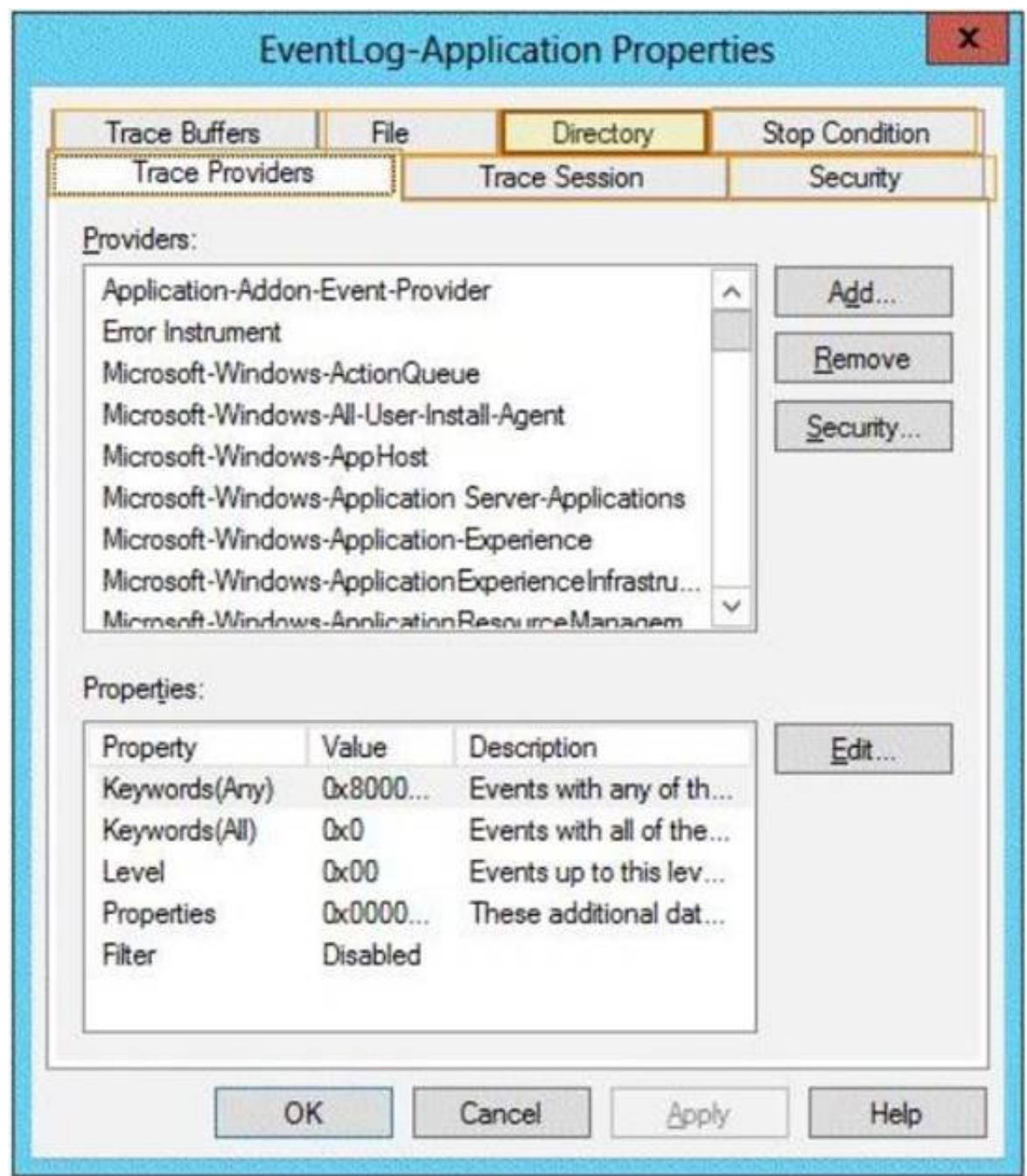
HOTSPOT - (Topic 1)

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

You enable the EventLog-Application event trace session.

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





- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 20

DRAG DROP - (Topic 1)

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

	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.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Note:

\* At a command prompt, specify the package identity to remove it from the image. You can remove multiple packages on one command line.

DISM /Image: C:\test\offline /Remove-Package /PackageName: Microsoft.Windows.Calc. Demo~6595b6144ccf1df~x86~en~1.0.0.0 /PackageName: Micro  
 /Cleanup-Image

Performs cleanup or recovery operations on the image.

**NEW QUESTION 23**

- (Topic 1)

You are a network administrator of an Active Directory domain named contoso.com.

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

You enable Network Access Protection (NAP) on all of the DHCP scopes on Server1. You need to create a DHCP policy that will apply to all of the NAP non-compliant DHCP

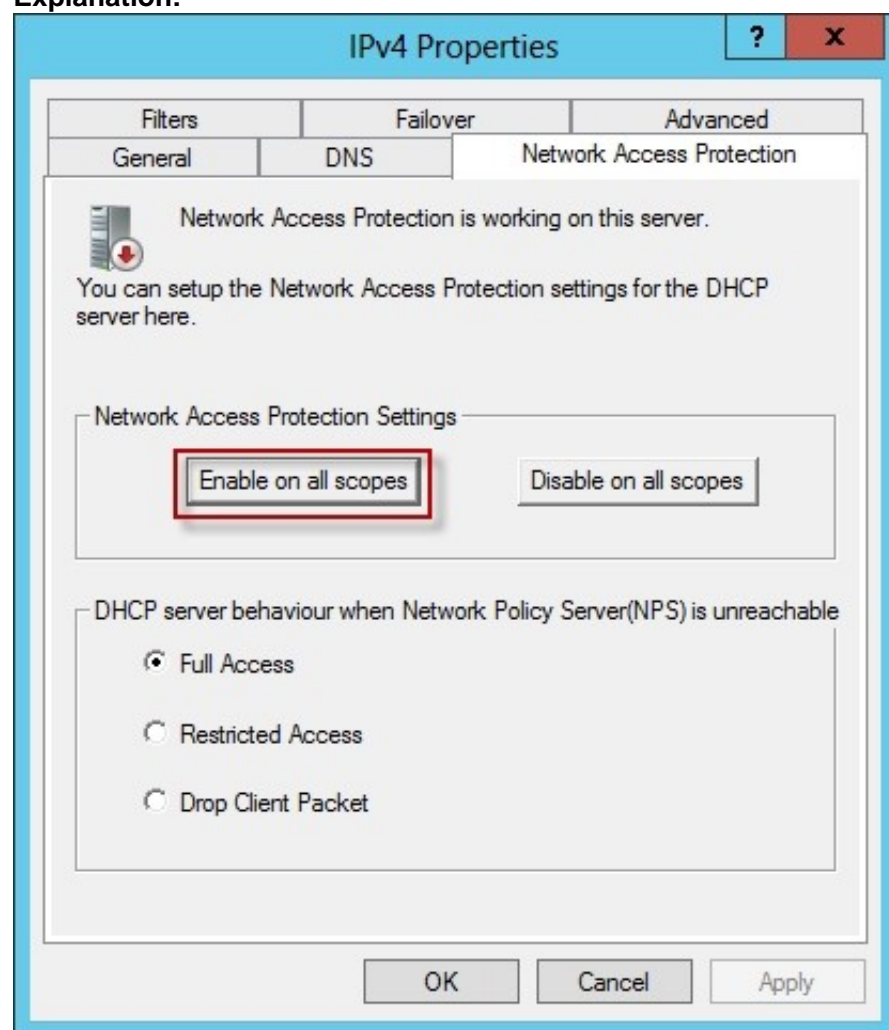
clients.

Which criteria should you specify when you create the DHCP policy?

- A. The client identifier
- B. The user class
- C. The vendor class
- D. The relay agent information

**Answer:** B

**Explanation:**



To configure a NAP-enabled DHCP server

? On the DHCP server, click Start, click Run, in Open, type dhcpgmt. smc, and then press ENTER.

? In the DHCP console, open <servername>\IPv4.

? Right-click the name of the DHCP scope that you will use for NAP client computers, and then click Properties.

? On the Network Access Protection tab, under Network Access Protection Settings, choose Enable for this scope, verify that Use default Network Access Protection profile is selected, and then click OK.

? In the DHCP console tree, under the DHCP scope that you have selected, right- click Scope Options, and then click Configure Options.

? On the Advanced tab, verify that Default User Class is selected next to User class.

? Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by compliant NAP client computers, and then click Add.

? Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each router to be used by compliant NAP client computers, and then click Add.

? Select the 015 DNS Domain Name check box, and in String value, under Data entry, type your organization's domain name (for example, woodgrovebank. local), and then click Apply. This domain is a full-access network assigned to compliant NAP clients.

? On the Advanced tab, next to User class, choose Default Network Access Protection Class.

? Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by noncompliant NAP client computers, and then click Add. This can be the same default gateway that is used by compliant NAP clients.

? Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each DNS server to be used by noncompliant NAP client computers, and then click Add. These can be the same DNS servers used by compliant NAP clients.

? Select the 015 DNS Domain Name check box, and in String value, under Data entry, type a name to identify the restricted domain (for example, restricted. Woodgrovebank. local), and then click OK. This domain is a restricted-access network assigned to noncompliant NAP clients.

? Click OK to close the Scope Options dialog box.

? Close the DHCP console.

Reference: <http://technet.microsoft.com/en-us/library/dd296905%28v=ws.10%29.aspx>

### NEW QUESTION 26

- (Topic 1)

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

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

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

What should you do?

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

**Answer: A**

#### Explanation:

WSUS Reporting Rollup Sample Tool

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

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

### NEW QUESTION 31

- (Topic 1)

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

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

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

What should you do?

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

**Answer: A**

#### Explanation:

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

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

2. Start group policy by running the following command:

`%SYSTEMROOT%\System32\gpedit.msc`.

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

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

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

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

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

### NEW QUESTION 32

- (Topic 1)

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.

**Answer: D**

#### Explanation:

To configure an existing RRAS server to support both VPN remote access and NAT routing:

1. Open Server Manager.
2. Expand Roles, and then expand Network Policy and Access Services.
3. Right-click Routing and Remote Access, and then click Properties.



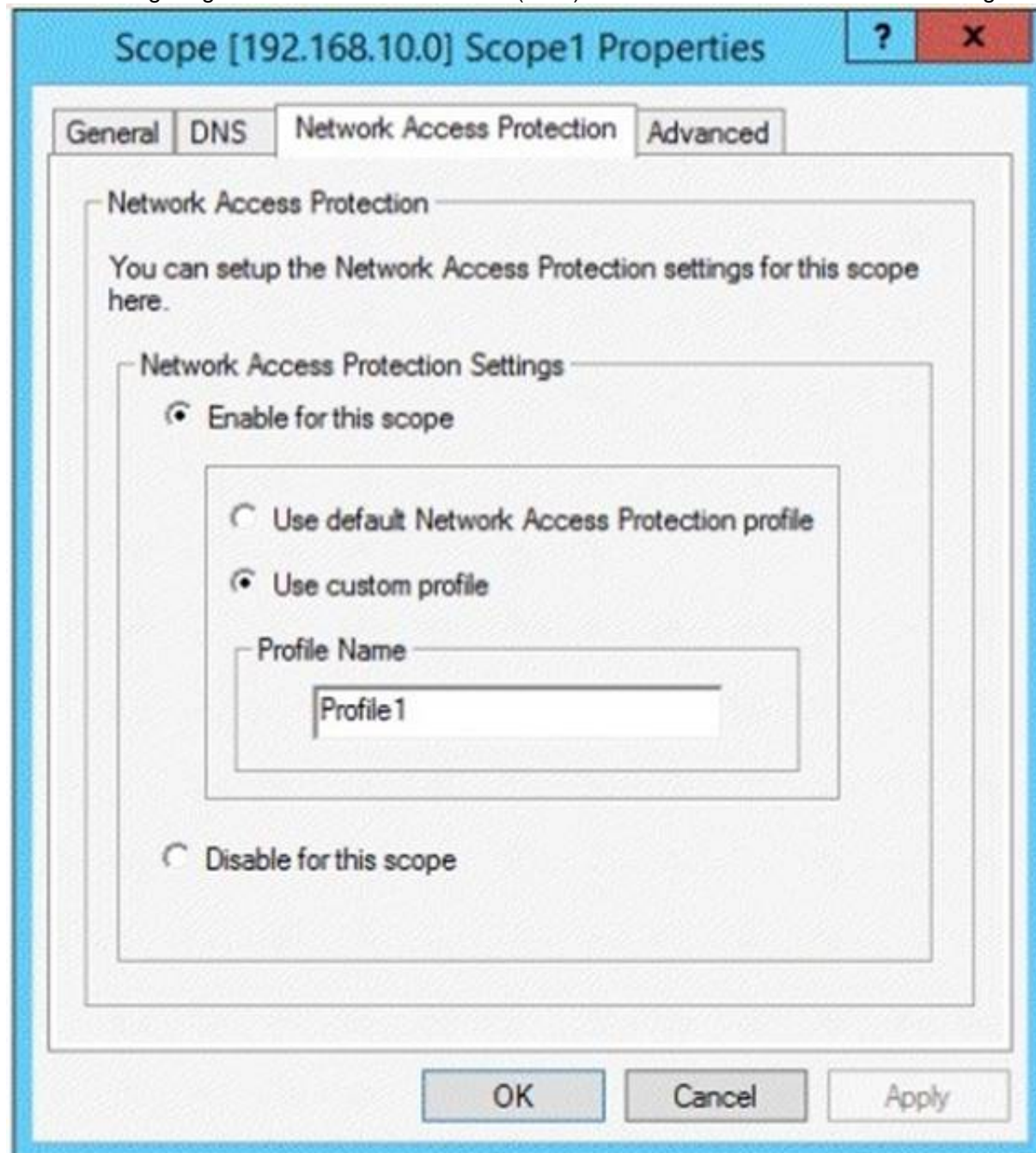
4. Select IPv4 Remote access Server or IPv6 Remote access server, or both.

**NEW QUESTION 33**

HOTSPOT - (Topic 1)

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.

**Answer Area**

Server1:

Server2:

**Answer Area**

Server1:   
Health Policies  
Identity-Type  
MS-Service Class  
Service-Type

Server2:   
filters  
a policy  
scope options  
server options  
a User class  
a Vendor class

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

Health Policies Server Options

\* Health policy on the NAP server.

\* The DHCP server must be NAP enabled.

Note: With DHCP enforcement, a computer must be compliant to obtain an unlimited access IP address configuration from a DHCP server. For noncompliant computers, network access is limited by an IP address configuration that allows access only to the restricted network. DHCP enforcement enforces health policy requirements every time a DHCP client attempts to lease or renew an IP address configuration. DHCP enforcement also actively monitors the health status of the NAP client and renews the IPv4 address configuration for access only to the restricted network if the client becomes noncompliant.

**NEW QUESTION 35**

- (Topic 2)

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

Server1 stores update files locally in C:\Updates.

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

A. From the Update Services console, run the Windows Server Update Services Configuration Wizard.

B. From a command prompt, run wsusutil.exe and specify the movecontent parameter.

C. From the Update Services console, configure the Update Files and Languages option.

D. From a command prompt, run wsusutil.exe and specify the export parameter.

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 38**

- (Topic 2)

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

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

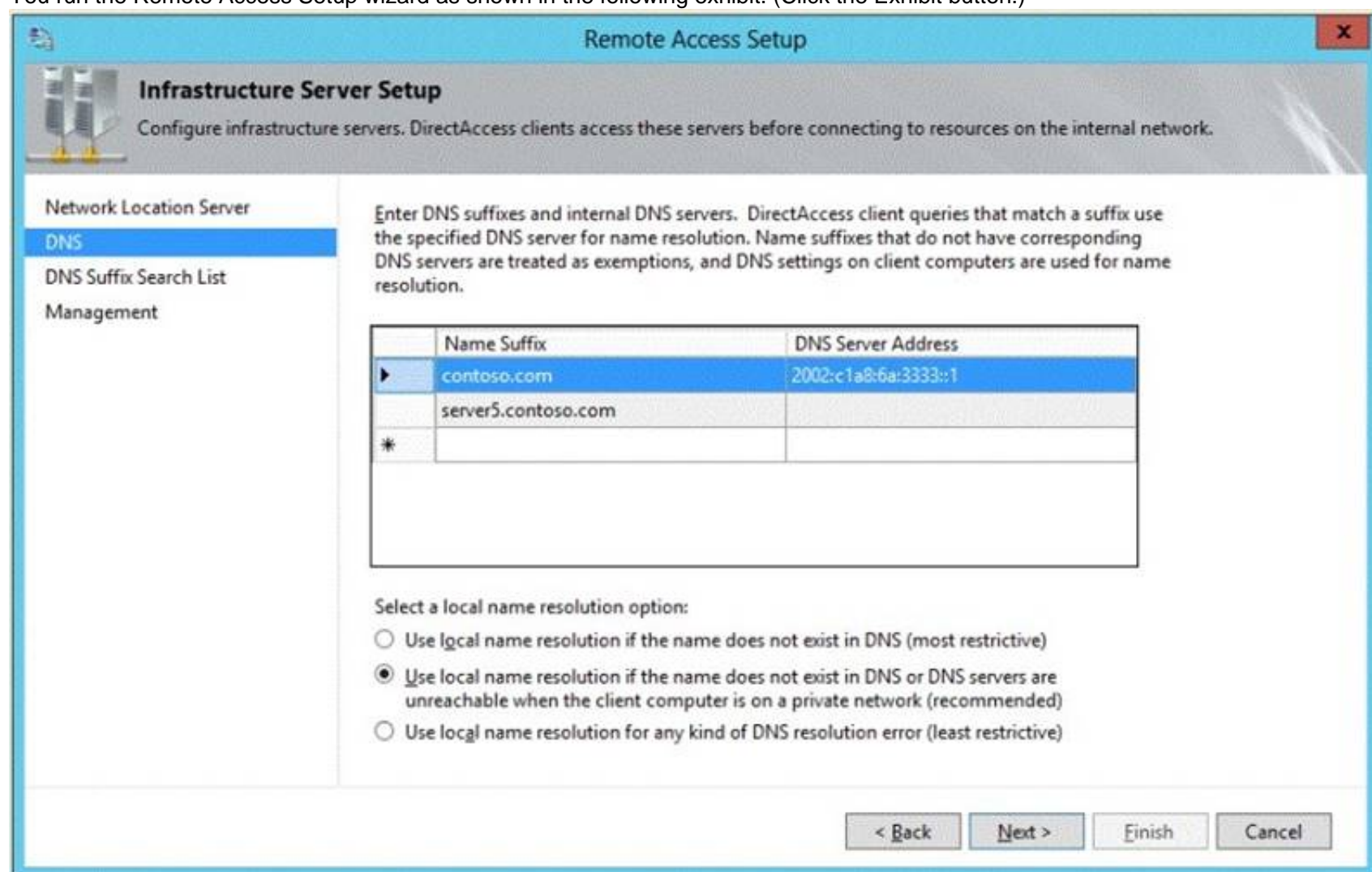
Internal DNS name: server1.contoso.com

External DNS name: da1.contoso.com

Internal IPv6 address: 2002:c1a8:6a:3333::1

External IPv4 address: 65.55.37.62

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



**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

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

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

A. A Name Suffix value of da1.contoso.com and a blank DNS Server Address value

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

**Answer:** A

**Explanation:**

Split-brain DNS is the use of the same DNS domain for both Internet and intranet resources. For example, the Contoso Corporation is using split brain DNS; contoso.com is the domain name for intranet resources and Internet resources. Internet users use http:

http://www.contoso.com to access Contoso's public Web site and Contoso employees on the Contoso intranet use http://www.contoso.com to access Contoso's intranet Web site. A Contoso employee with their laptop that is not a DirectAccess client on the intranet that accesses http://www.contoso.com sees the intranet Contoso Web site. When they take their laptop to the local coffee shop and access that same URL, they will see the public Contoso Web site.

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

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

References:

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

**NEW QUESTION 42**

DRAG DROP - (Topic 2)

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

You need to create an Active Directory snapshot on DC1. Which four commands should you run?

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

Commands	Answer Area
dsamain.exe	1
snapshot	
create	
ntdsutil.exe	
activate instance ntds	
wbadmin.exe	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: ntdsutil

Box 2: snapshot

Box 3: activate instance ntds Box 4: create

Note:

Create a snapshot of AD DS in Windows Server 2012 R2 by using NTDSUTIL

1 – On the domain server, open command prompt and type ntdsutil and press Enter. 2- Next, type snapshot and press Enter.

3 – Next, type activate instance ntds and press Enter.

4 – Next, type create (this create command is to generate a snapshot of my AD) and press Enter.

**NEW QUESTION 45**

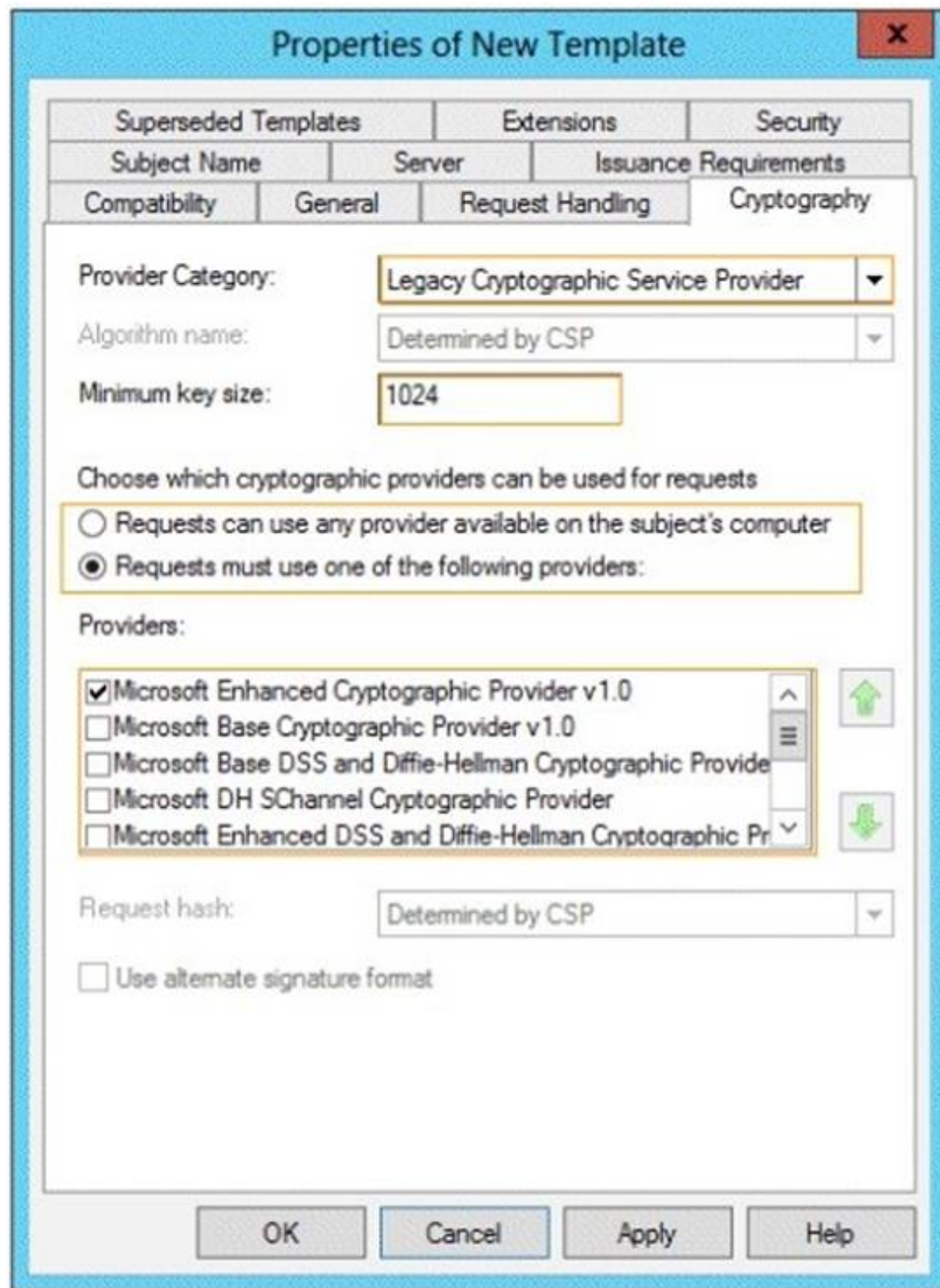
HOTSPOT - (Topic 2)

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.





- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 50**

- (Topic 2)

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

**Answer:** BC

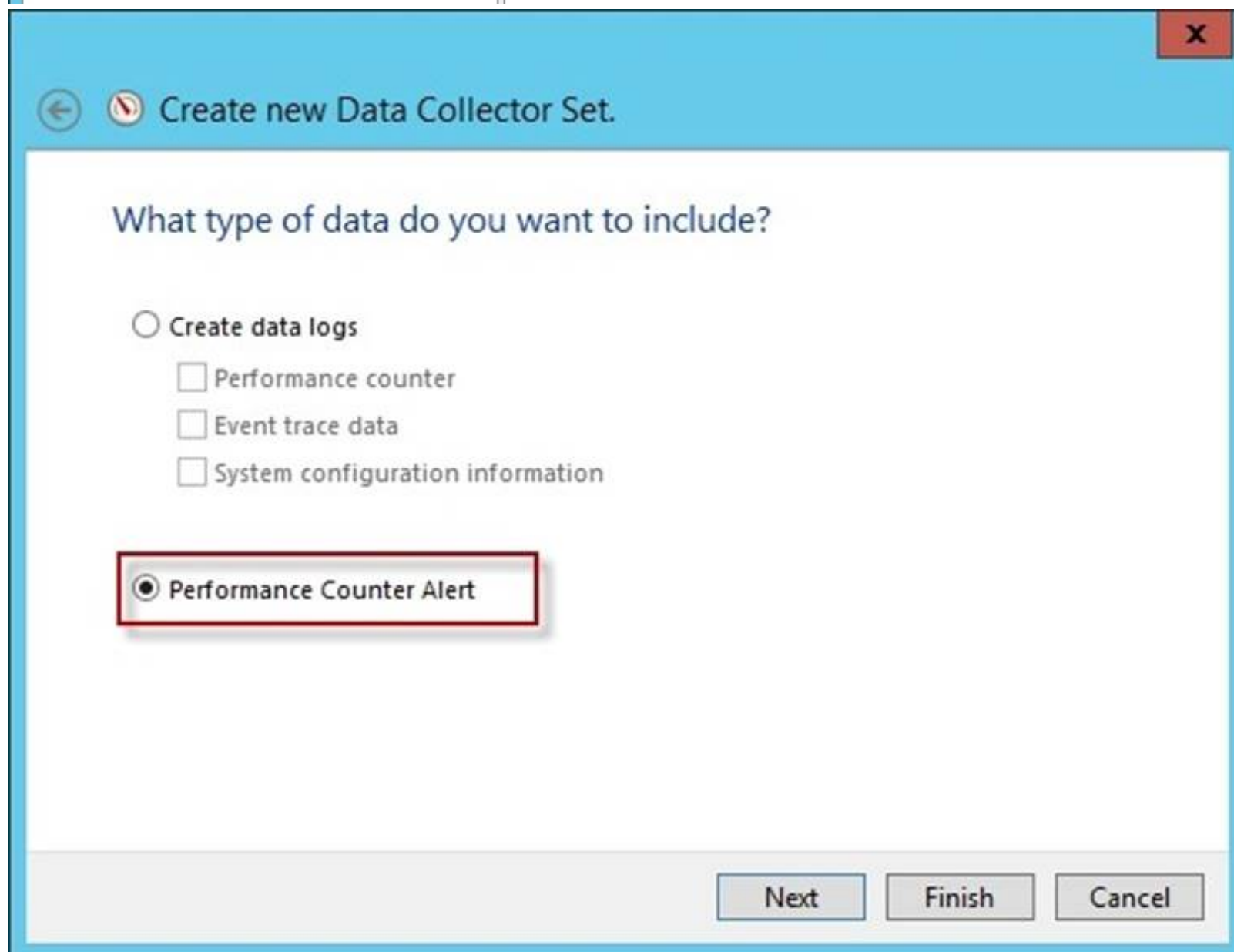
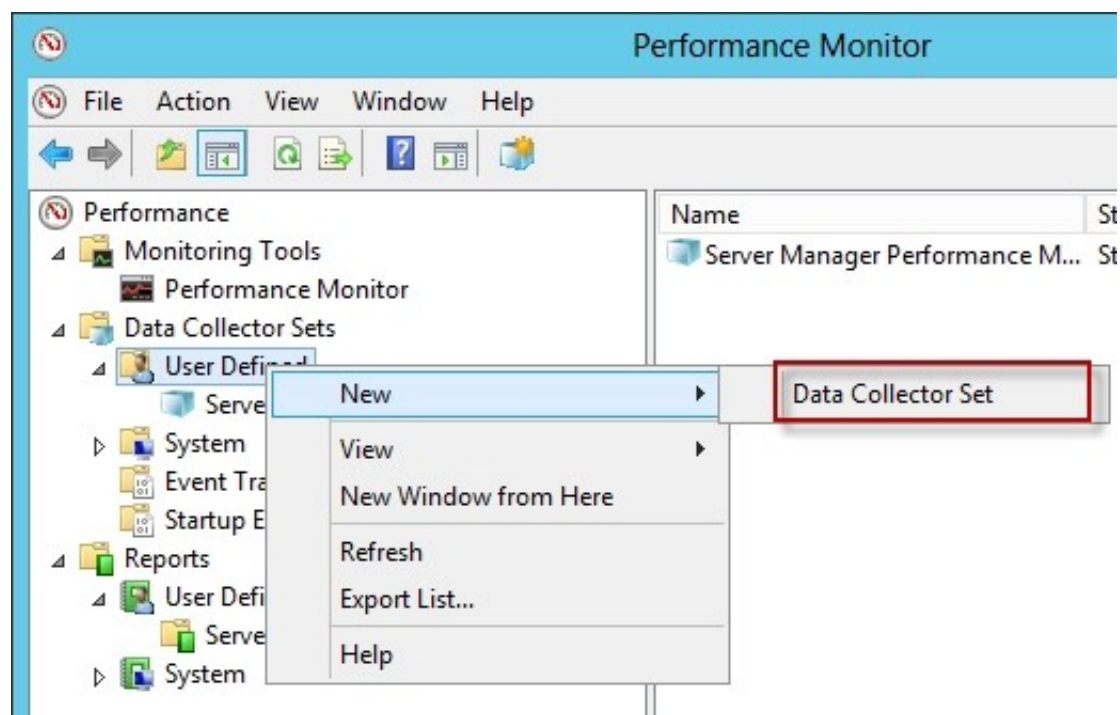
**Explanation:**

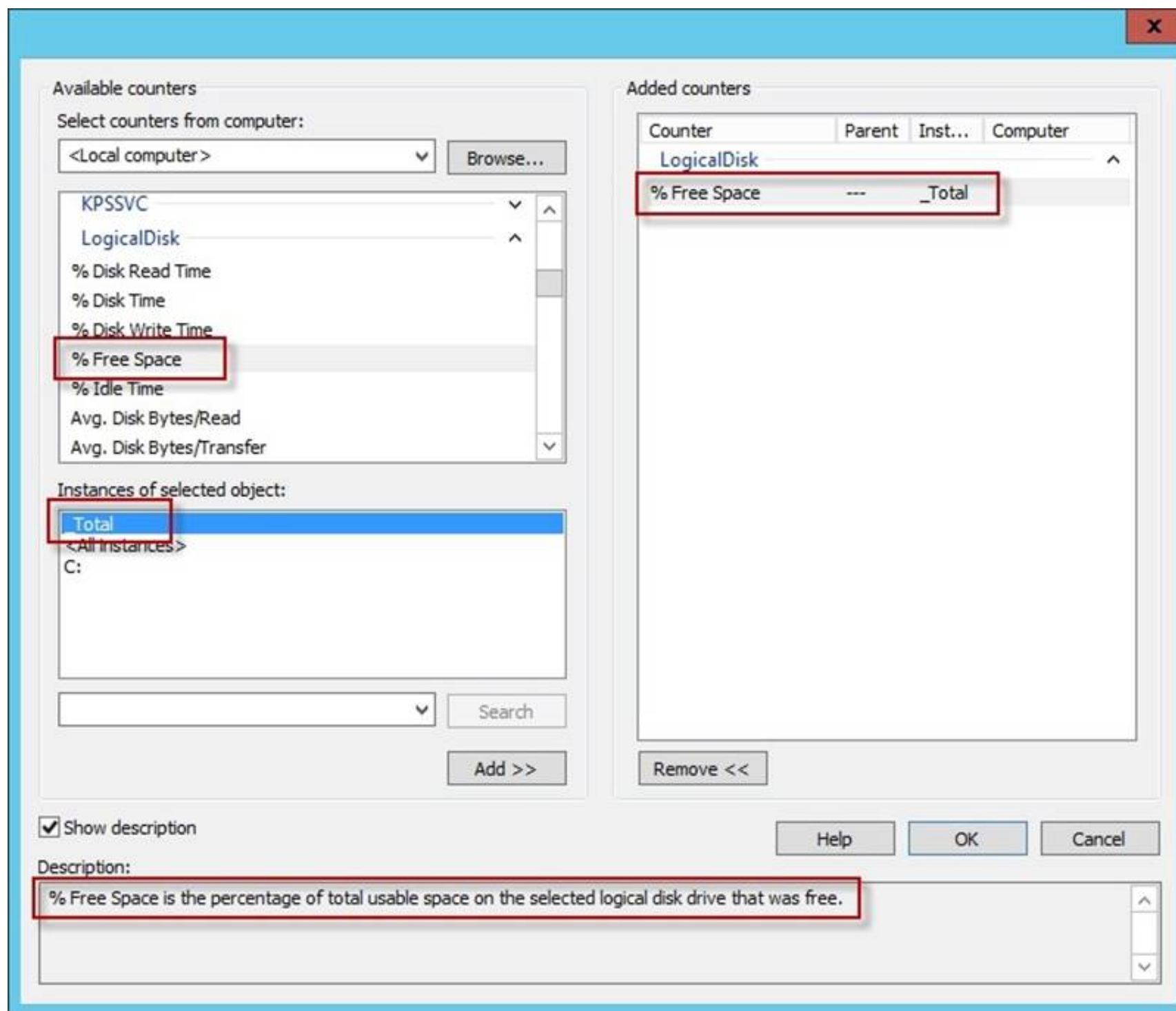
Automatically run a program when the amount of total free disk space on Server1 drops below 10 percent of capacity.

You can also configure alerts to start applications and performance logs Log the current values of several registry settings.

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

Total free disk space





Available counters

Select counters from computer:

<Local computer> Browse...

Available counters list:

- KPSSVC
- LogicalDisk
- % Disk Read Time
- % Disk Time
- % Disk Write Time
- % Free Space**
- % Idle Time
- Avg. Disk Bytes/Read
- Avg. Disk Bytes/Transfer

Instances of selected object:

**Total**

<All instances>

C:

Search

Add >>

Added counters

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

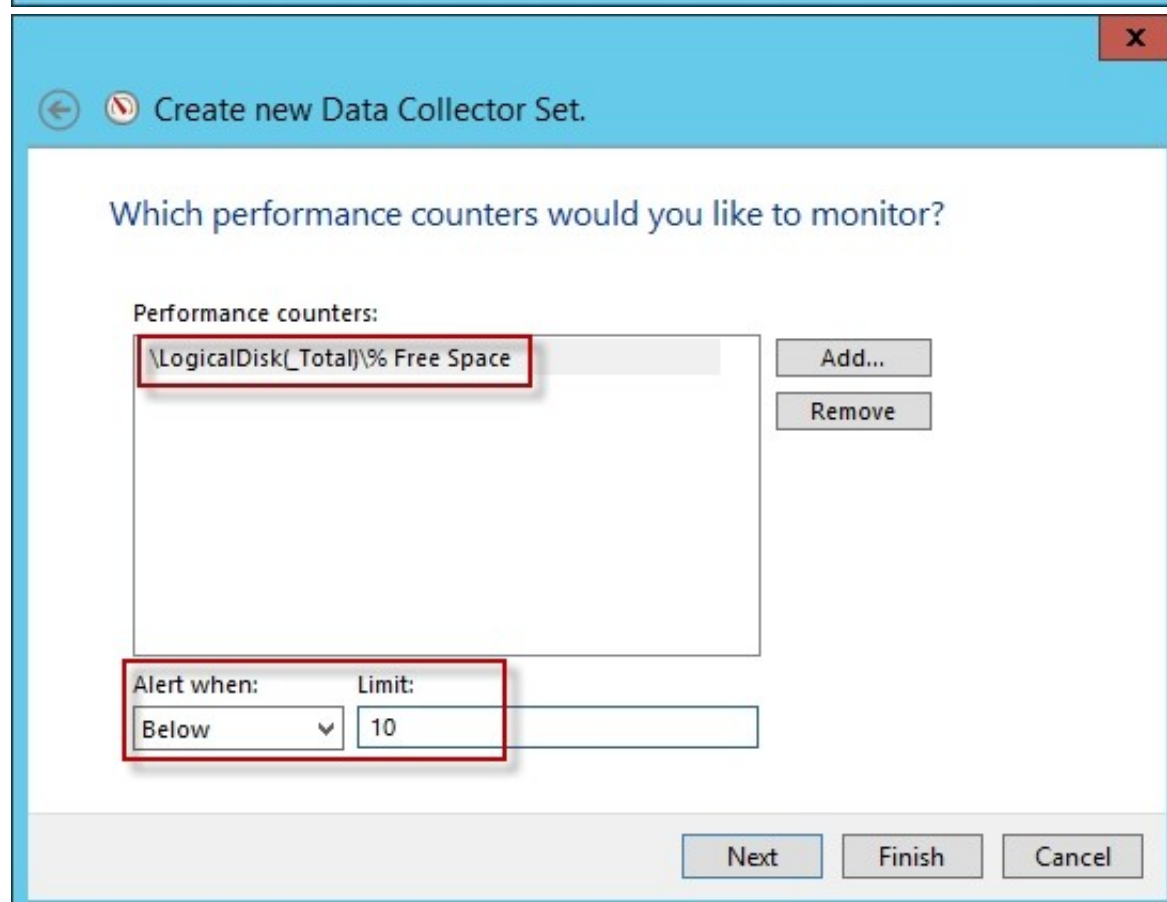
Remove <<

☒ Show description

Help OK Cancel

Description:

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



Create new Data Collector Set.

Which performance counters would you like to monitor?

Performance counters:

**\LogicalDisk(\_Total)\% Free Space**

Add... Remove

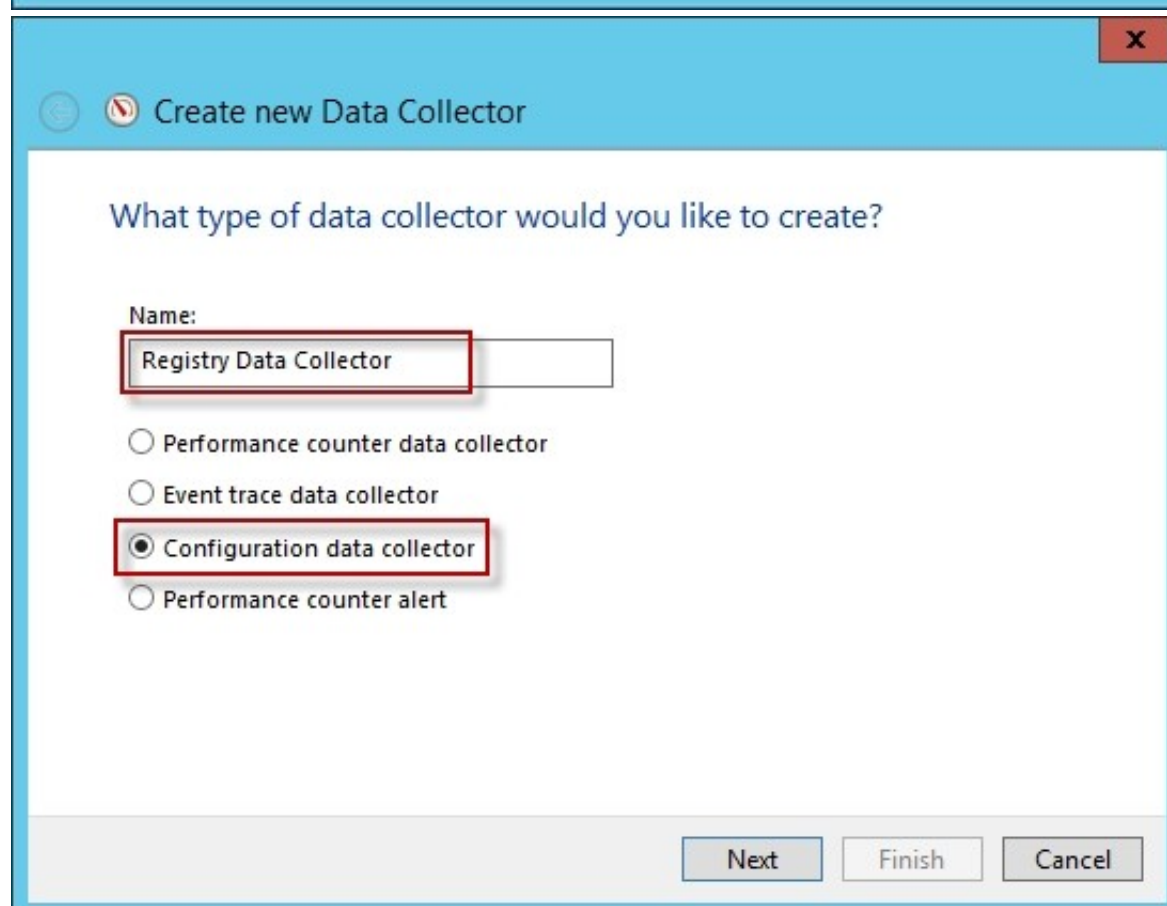
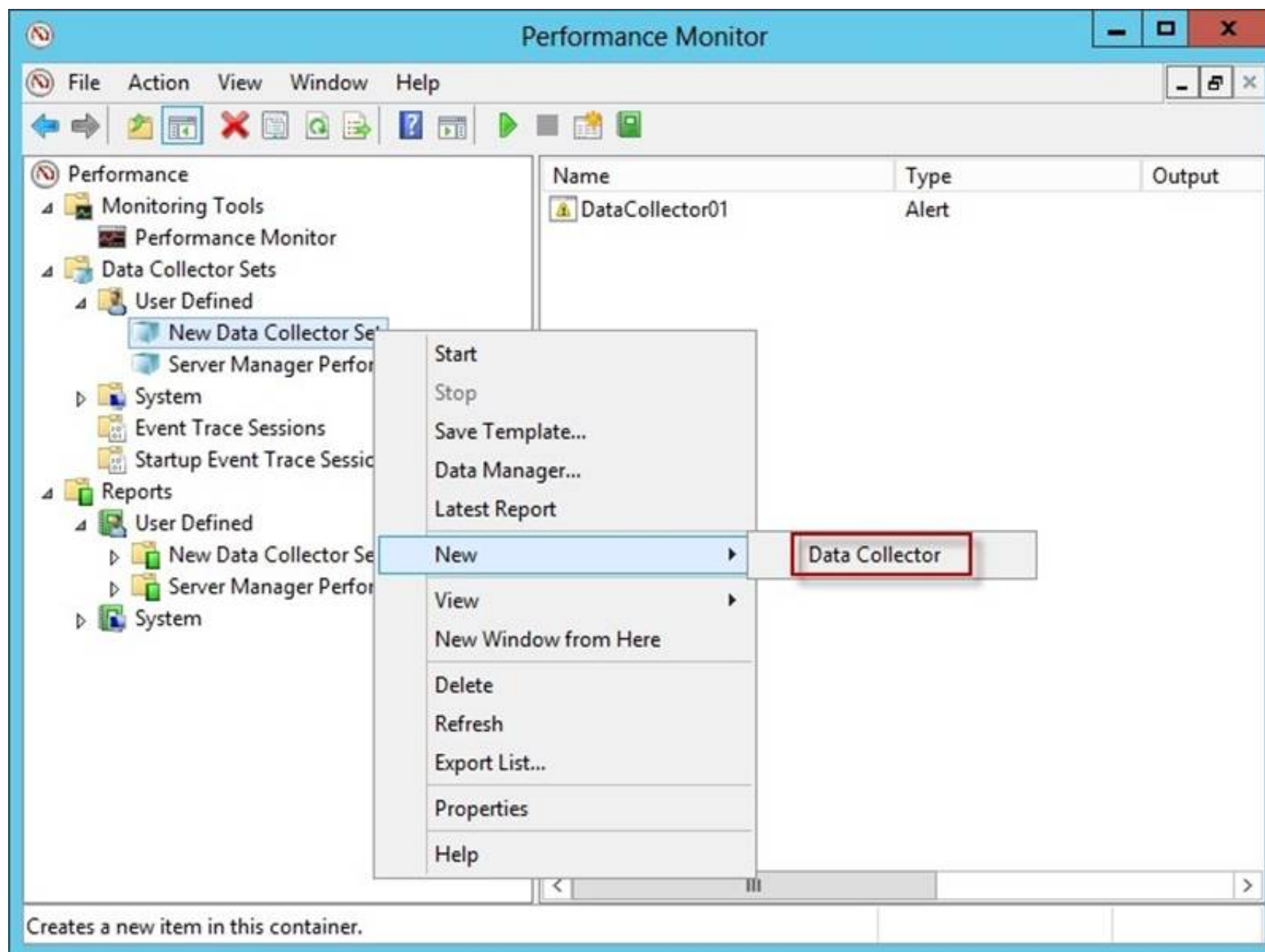
Alert when: Limit:

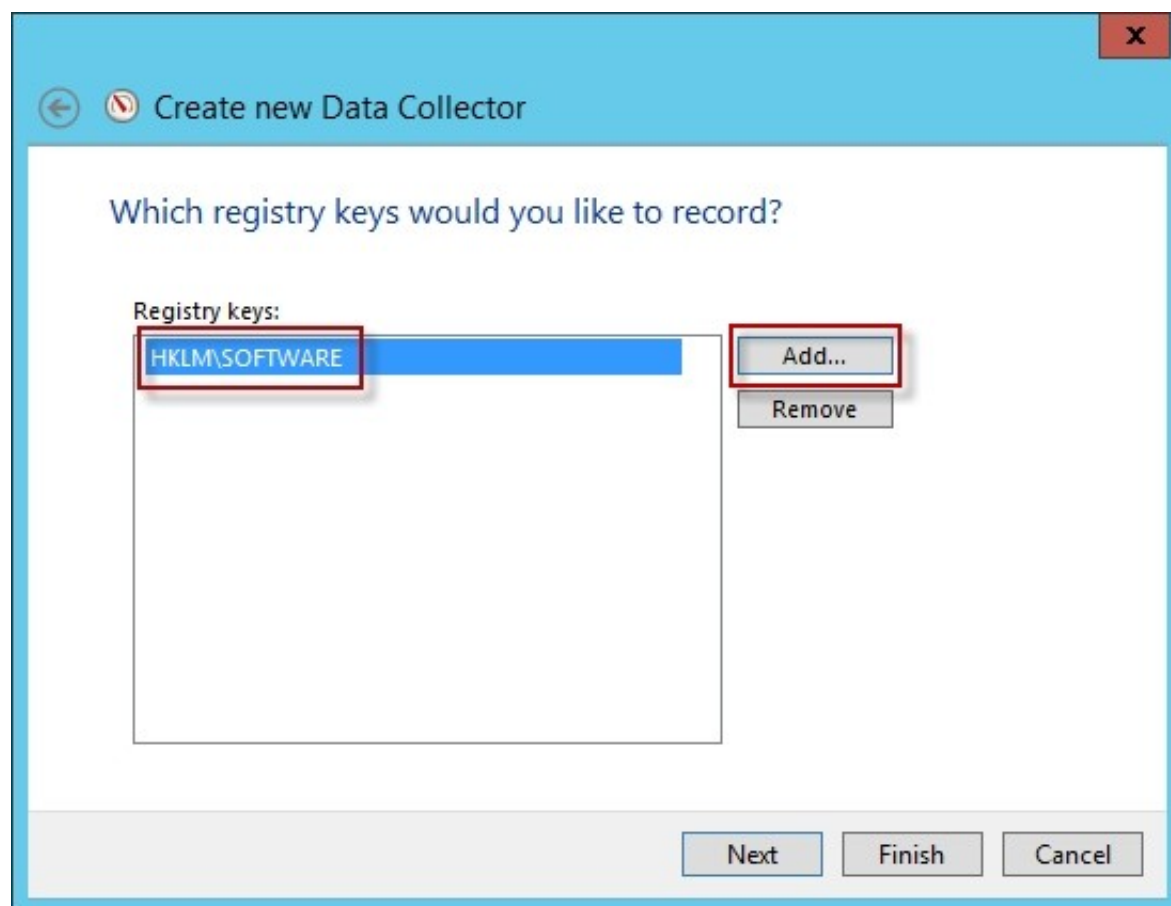
Below 10

Next Finish Cancel

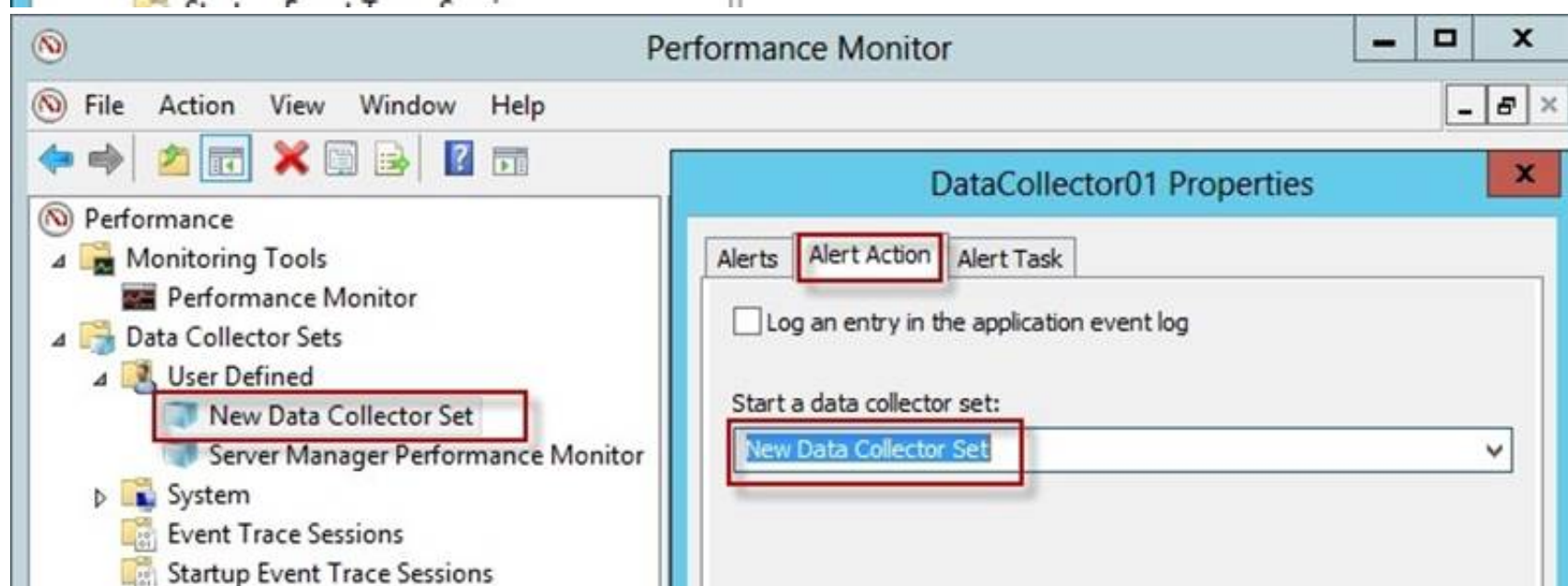
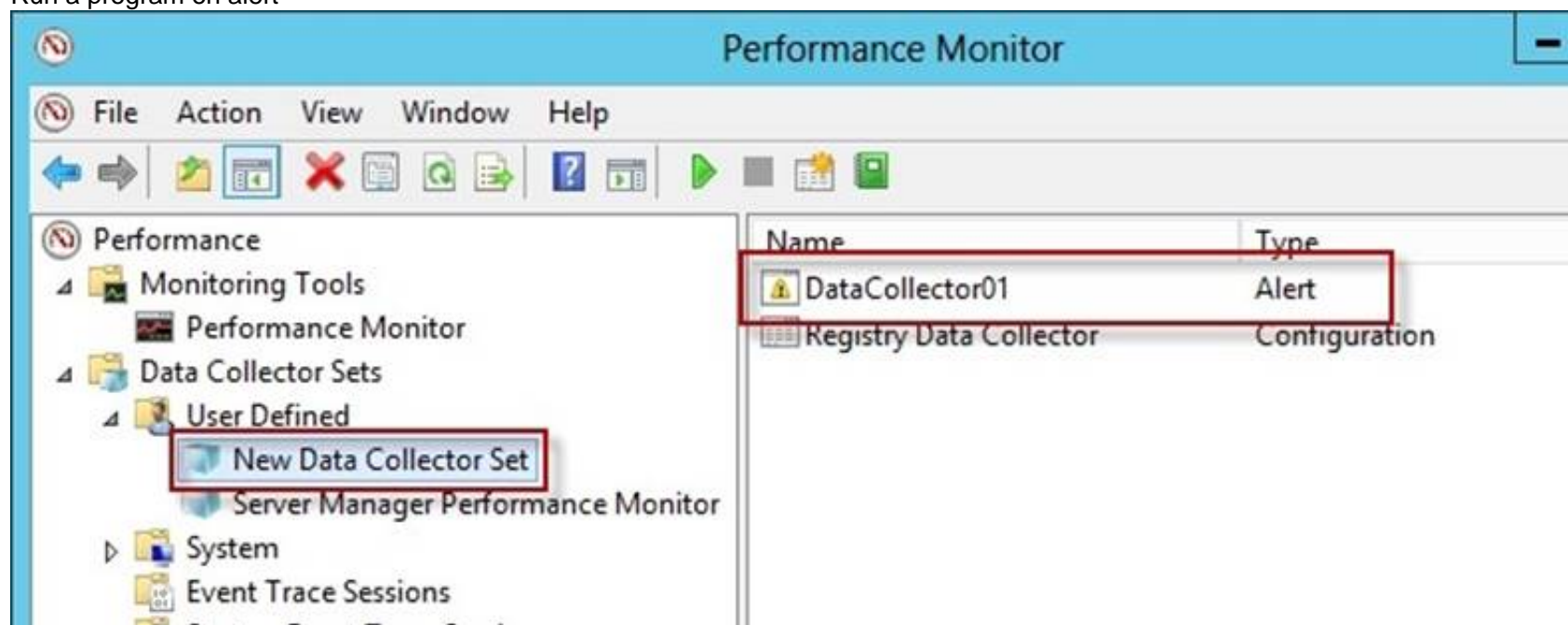
Registry settings

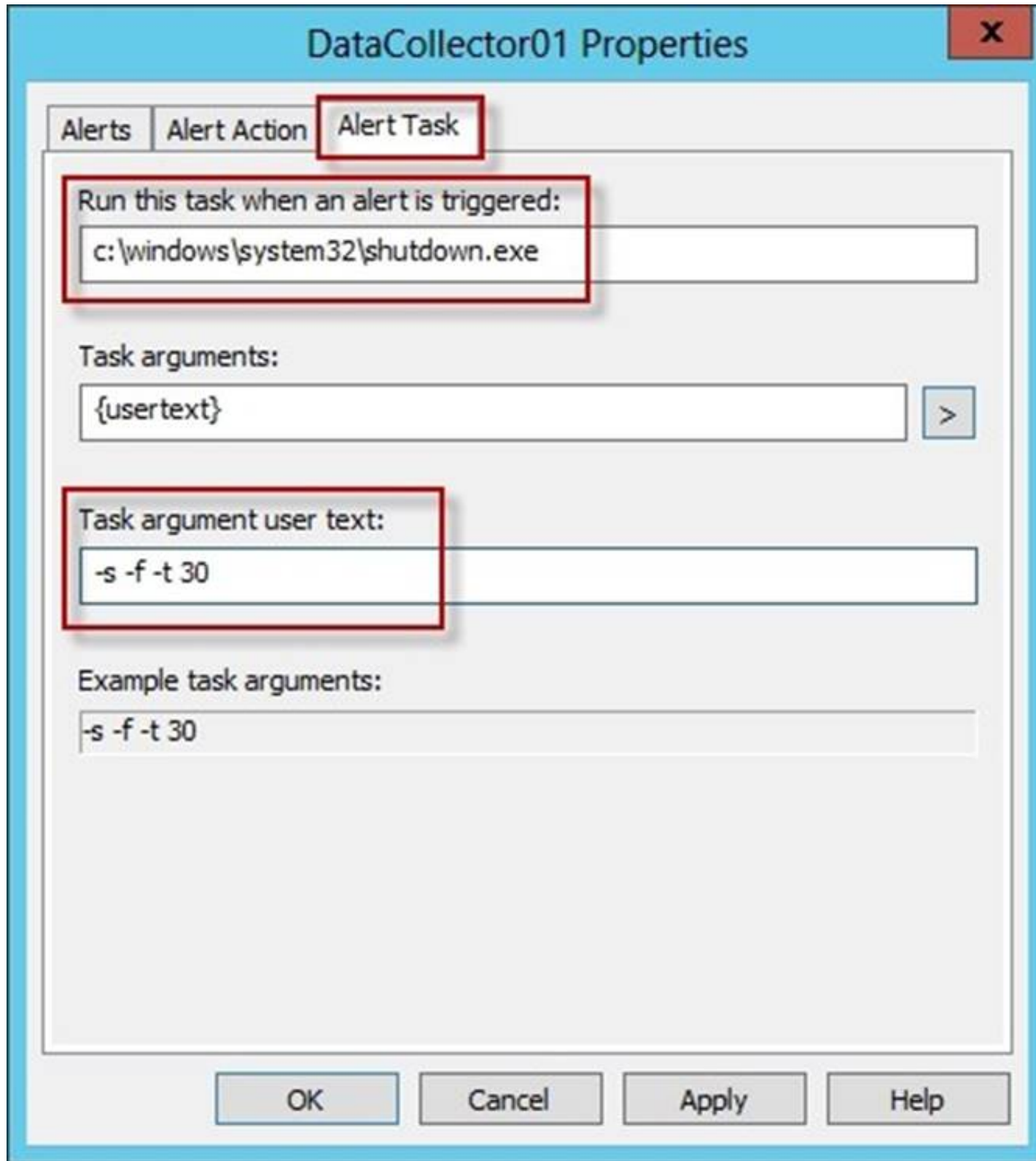






Run a program on alert





**DataCollector01 Properties**

Alerts | Alert Action | **Alert Task**

Run this task when an alert is triggered:

Task arguments:

Task argument user text:

Example task arguments:

OK Cancel Apply Help

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

#### NEW QUESTION 54

- (Topic 2)

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

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

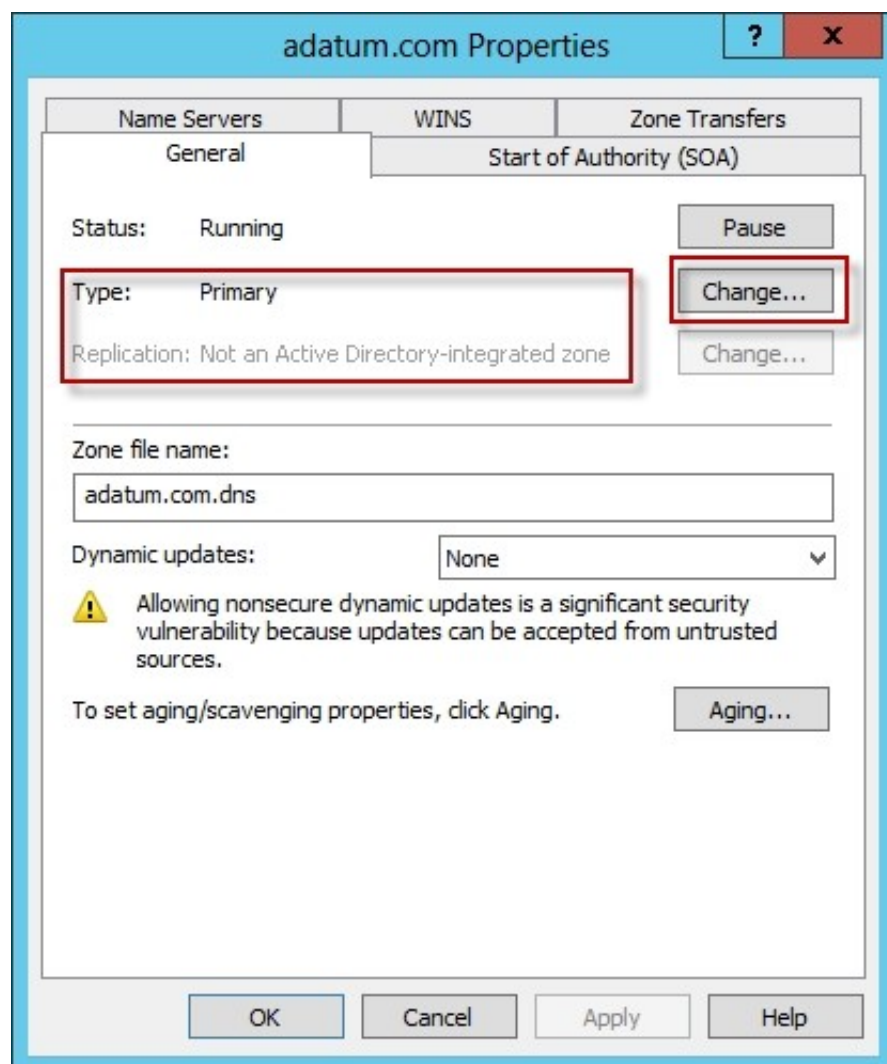
**Answer: C**

#### Explanation:

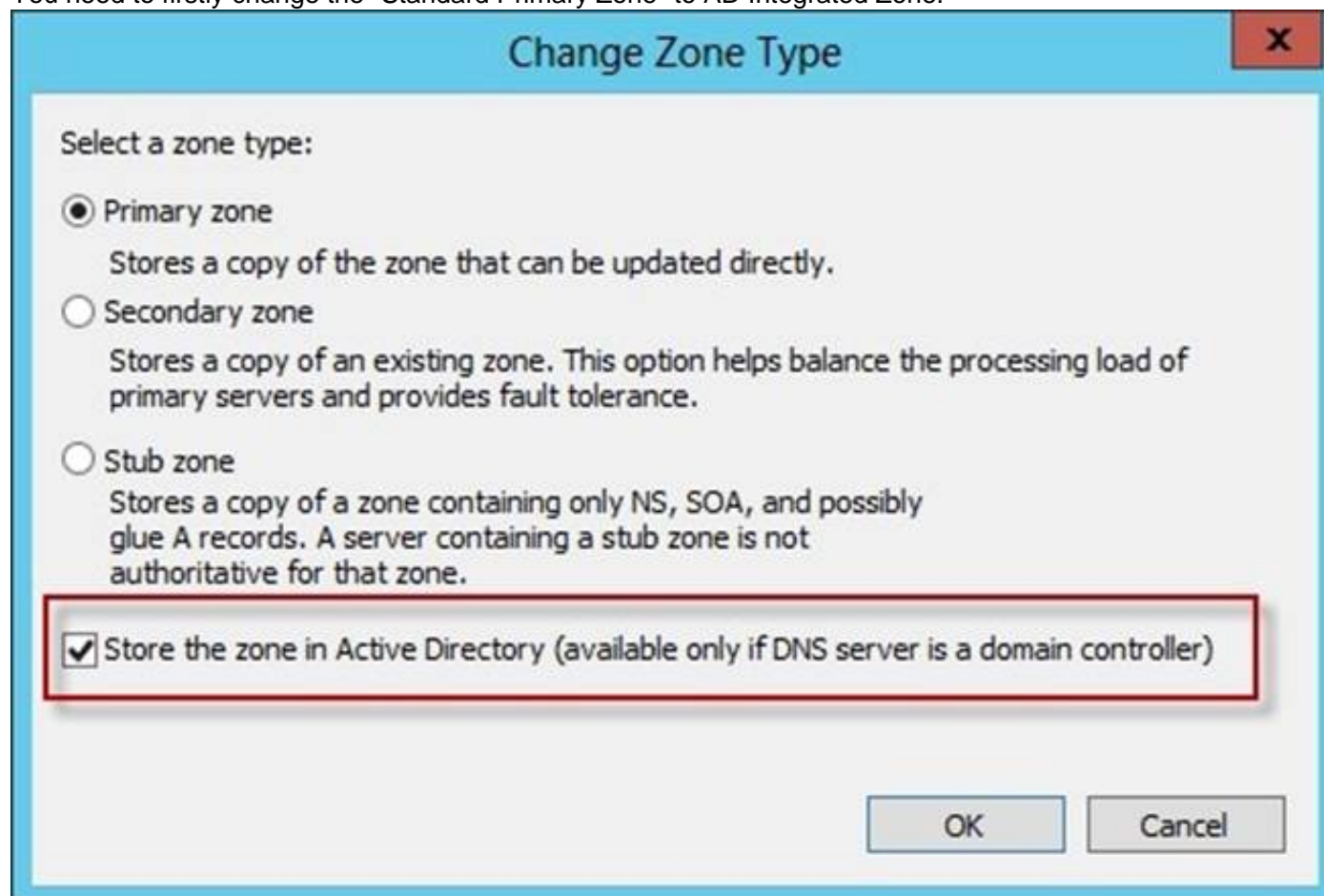
The Zone would need to be changed to a AD integrated zone. When you use directory- integrated zones, you can use access control list (ACL) editing to secure a dnsZone object container in the directory tree. This feature provides detailed access to either the zone or a specified resource record in the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

DNS update security is available only for zones that are integrated into Active Directory. After you integrate a zone, you can use the access control list (ACL) editing features that are available in the DNS snap-in to add or to remove users or groups from the ACL for a specific zone or for a resource record. Standard (not an Active Directory integrated zone) has no Security settings:

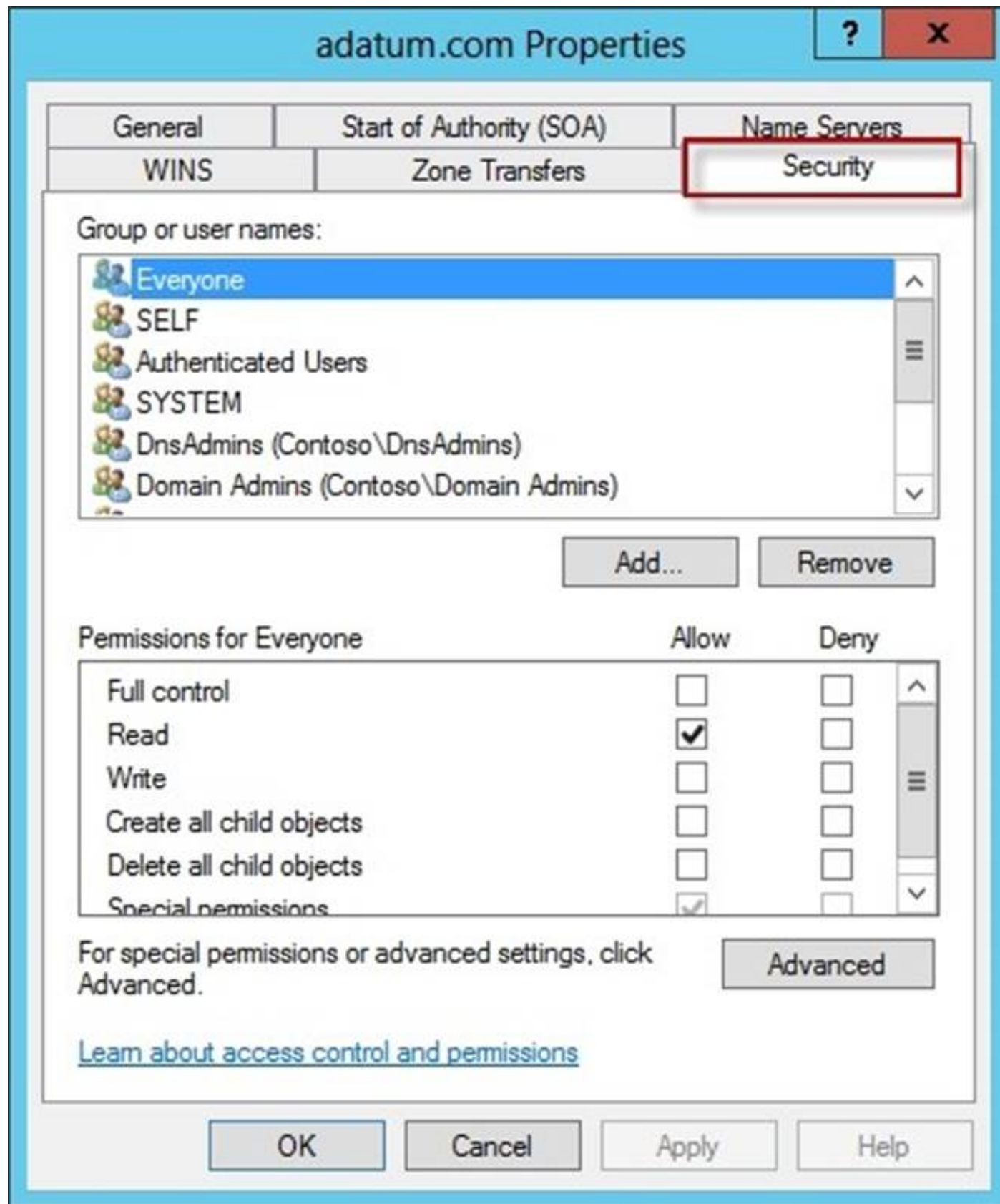




You need to firstly change the "Standard Primary Zone" to AD Integrated Zone:



Now there's Security tab:



**adatum.com Properties**

General Start of Authority (SOA) Name Servers  
WINS Zone Transfers **Security**

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- DnsAdmins (Contoso\DnsAdmins)
- Domain Admins (Contoso\Domain Admins)

Add... Remove

Permissions for Everyone

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

[Learn about access control and permissions](#)

OK Cancel Apply Help

References:

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

#### NEW QUESTION 55

- (Topic 2)

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

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

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

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

**Answer:** A

**Explanation:**

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

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

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

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

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

References:

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

**NEW QUESTION 56**

HOTSPOT - (Topic 2)

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

Server1 has the following BitLocker Drive Encryption (BitLocker) settings:

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

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

Answer Area

Answer Area

<div></div>	<div></div>	<div></div>	<div></div>
Add-BitLockerKeyProtector	-MountPoint C:	-AdAccountOrGroupProtector Contoso\Server	-Service
Enable-BitLockerAutoUnlock	-MountPoint D:	-Pin \$SecureString	TpmAndPinAndStartupKeyProtecto
			-TpmAndPinProtector

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

<div></div>	<div></div>	<div></div>	<div></div>
Add-BitLockerKeyProtector	-MountPoint C:	-AdAccountOrGroupProtector Contoso\Server	-Service
Enable-BitLockerAutoUnlock	-MountPoint D:	-Pin \$SecureString	TpmAndPinAndStartupKeyProtecto
			-TpmAndPinProtector



#### NEW QUESTION 61

- (Topic 2)

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

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

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

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

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

**Answer:** A

#### Explanation:

Audit User Account Management

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

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

? A user account password is set or changed.

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

? The Directory Services Restore Mode password is set.

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

? Credential Manager credentials are backed up or restored.

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

#### NEW QUESTION 62

- (Topic 2)

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

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

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

You need to ensure that you can clone DC6. What should you do?

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

**Answer:** D

#### Explanation:

A deployed Windows Server 2012 domain controller (virtualized or physical) that hosts the PDC emulator role (DC1). To verify whether the PDC emulator role is hosted on a Windows Server 2012 domain controller, run the following Windows PowerShell command:

Get-ADComputer (Get-ADDomainController -Discover -Service "PrimaryDC").name

-Propertyoperatingsystemversion|fl

Reference: [http://technet.microsoft.com/en-us/library/hh831734.aspx#steps\\_deploy\\_vdc](http://technet.microsoft.com/en-us/library/hh831734.aspx#steps_deploy_vdc)

#### NEW QUESTION 66

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2003, Windows Server 2008 R2, or Windows Server 2012 R2.

A support technician accidentally deletes a user account named User1. You need to use tombstone reanimation to restore the User1 account. Which tool should you use?

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

**Answer: C**

**Explanation:**

Use Ldp.exe to restore a single, deleted Active Directory object

This feature takes advantage of the fact that Active Directory keeps deleted objects in the database for a period of time before physically removing them.

use Ldp.exe to restore a single, deleted Active Directory object

The LDP.exe tool, included with Windows Server 2012, allows users to perform operations against any LDAP-compatible directory, including Active Directory. LDP is used to view objects stored in Active Directory along with their metadata, such as security descriptors and replication metadata.

References:

<http://www.petri.co.il/manually-undeleting-objects-windows-active-directory-ad.htm>

<http://www.petri.co.il/manually-undeleting-objects-windows-active-directory-ad.htm>

<http://technet.microsoft.com/en-us/magazine/2007.09.tombstones.aspx>

[http://technet.microsoft.com/nl-nl/library/dd379509\(v=ws.10\).aspx#BKMK\\_2](http://technet.microsoft.com/nl-nl/library/dd379509(v=ws.10).aspx#BKMK_2)

<http://technet.microsoft.com/en-us/library/hh875546.aspx>

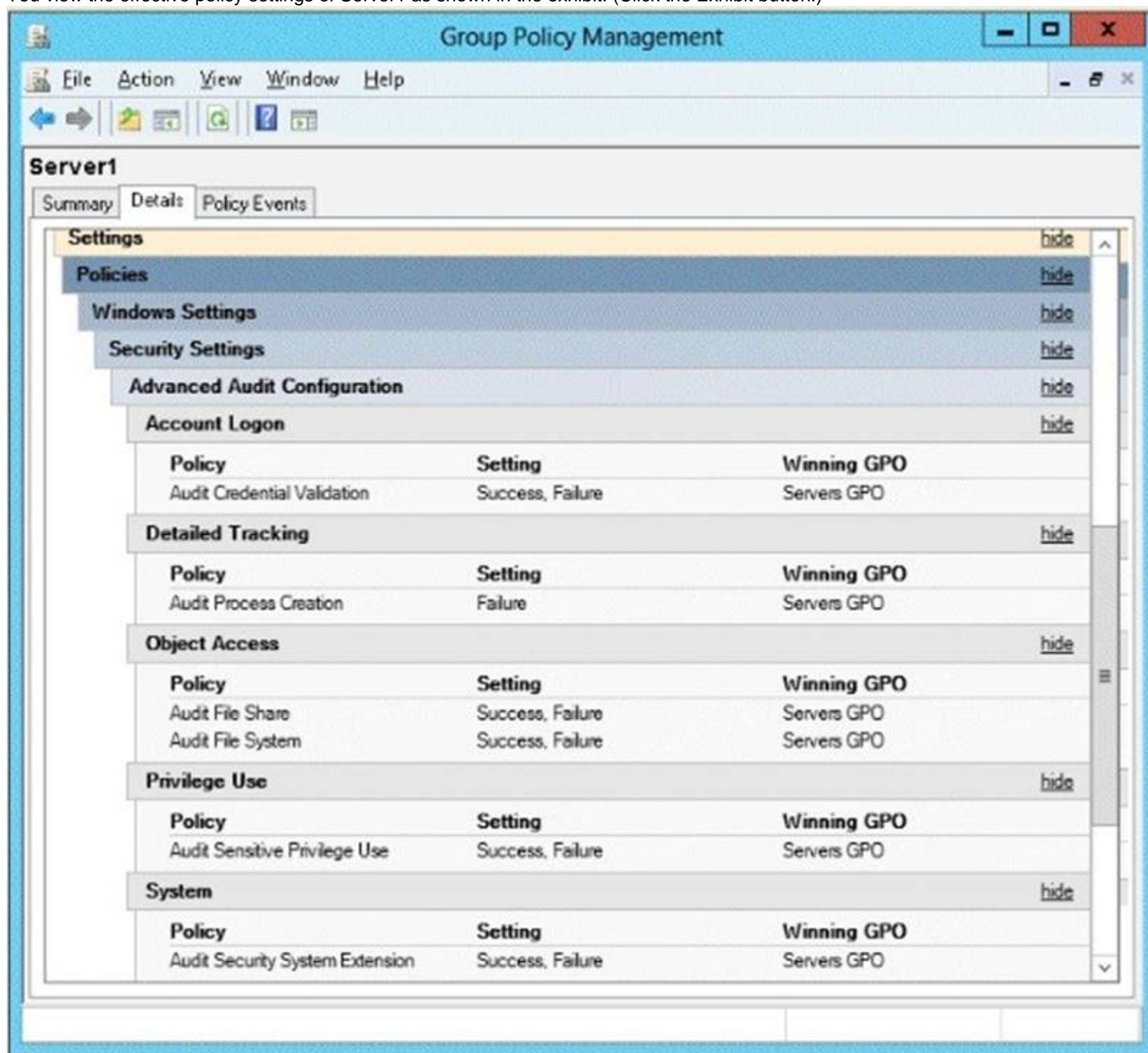
[http://technet.microsoft.com/en-us/library/dd560651\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd560651(v=ws.10).aspx)

**NEW QUESTION 67**

- (Topic 2)

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

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



Policy	Setting	Winning GPO
<b>Account Logon</b>		
Audit Credential Validation	Success, Failure	Servers GPO
<b>Detailed Tracking</b>		
Audit Process Creation	Failure	Servers GPO
<b>Object Access</b>		
Audit File Share	Success, Failure	Servers GPO
Audit File System	Success, Failure	Servers GPO
<b>Privilege Use</b>		
Audit Sensitive Privilege Use	Success, Failure	Servers GPO
<b>System</b>		
Audit Security System Extension	Success, Failure	Servers GPO

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

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

What should you configure?

- A. the Audit File Share setting of Servers GPO

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

**Answer: D**

**Explanation:**

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

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

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

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

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

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

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

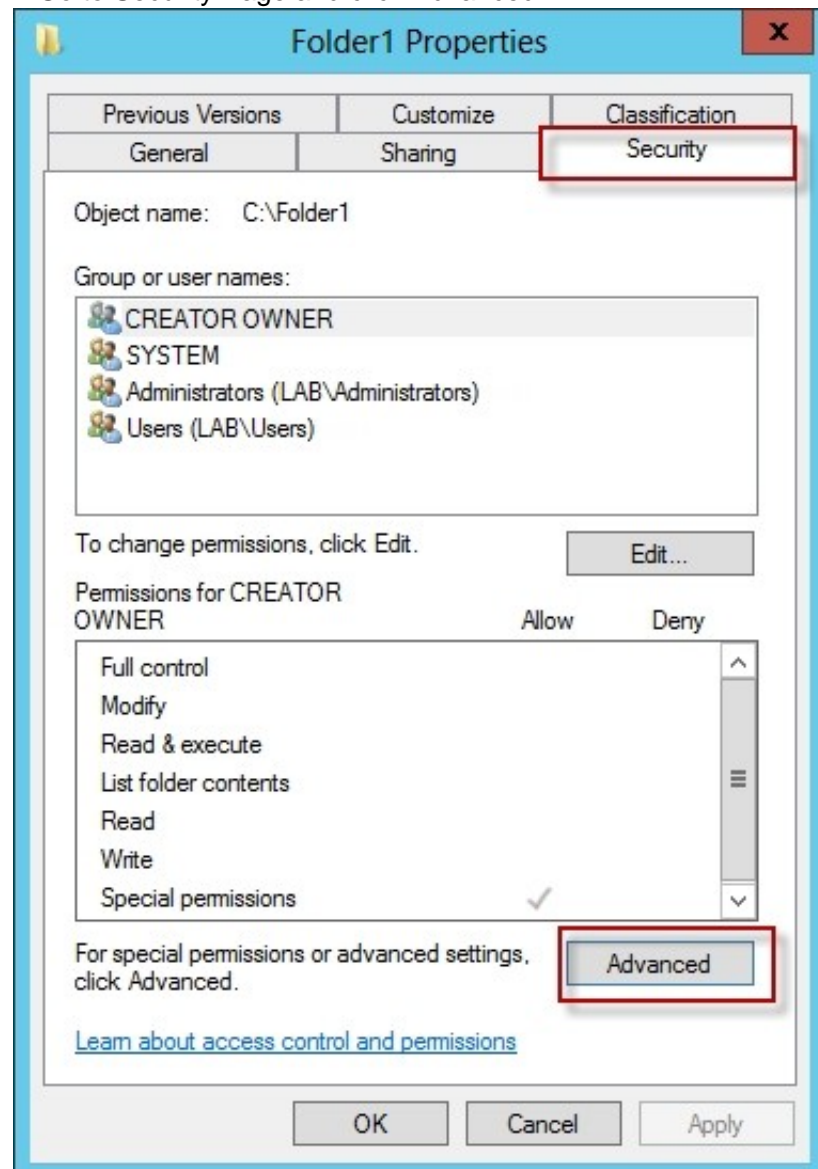
? Click start and run "secpol. msc" without quotes.

? Open the Local Policies\Audit Policy

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

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

? Go to Security Page and click Advanced.



? Click Auditing and Edit.

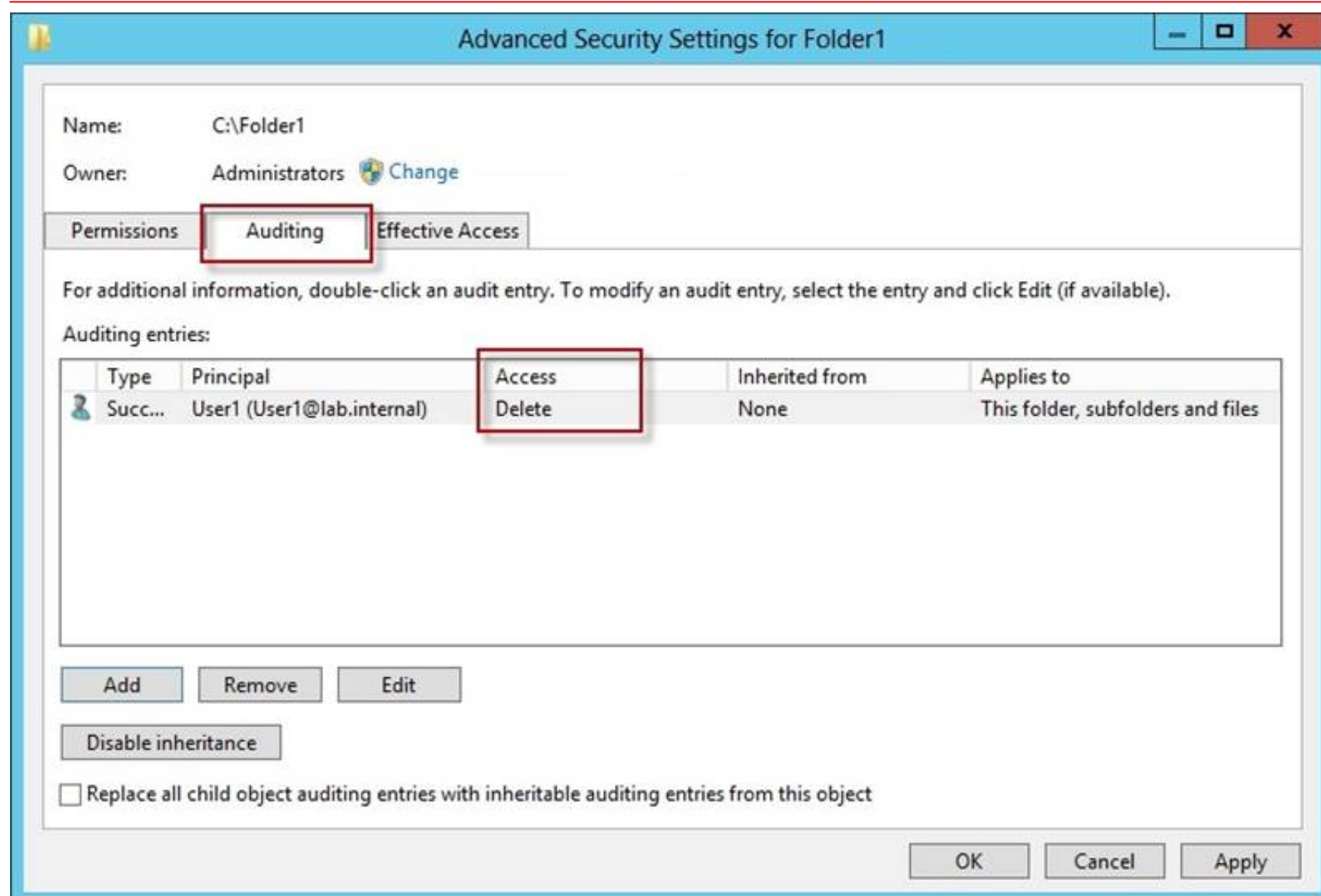
? Click add, type everyone in the Select User, Computer, or Group.

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

? Tick on the box "Change permissions"

? Click OK.





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

References:

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

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

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

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

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

## NEW QUESTION 68

HOTSPOT - (Topic 2)

Your network contains a DNS server named Server1 that runs Windows Server 2012 R2. Server1 has a zone named contoso.com. The network contains a server named Server2 that runs Windows Server 2008 R2. Server1 and Server2 are members of an Active Directory domain named contoso.com.

You change the IP address of Server2.

Several hours later, some users report that they cannot connect to Server2.

On the affected users' client computers, you flush the DNS client resolver cache, and the users successfully connect to Server2.

You need to reduce the amount of time that the client computers cache DNS records from contoso.com.

Which value should you modify in the Start of Authority (SOA) record? To answer, select the appropriate setting in the answer area.

contoso.com Properties

Name Servers

WINS

Zone Transfers

General

Start of Authority (SOA)

Serial number:

234

Increment

Primary server:

server 1.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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

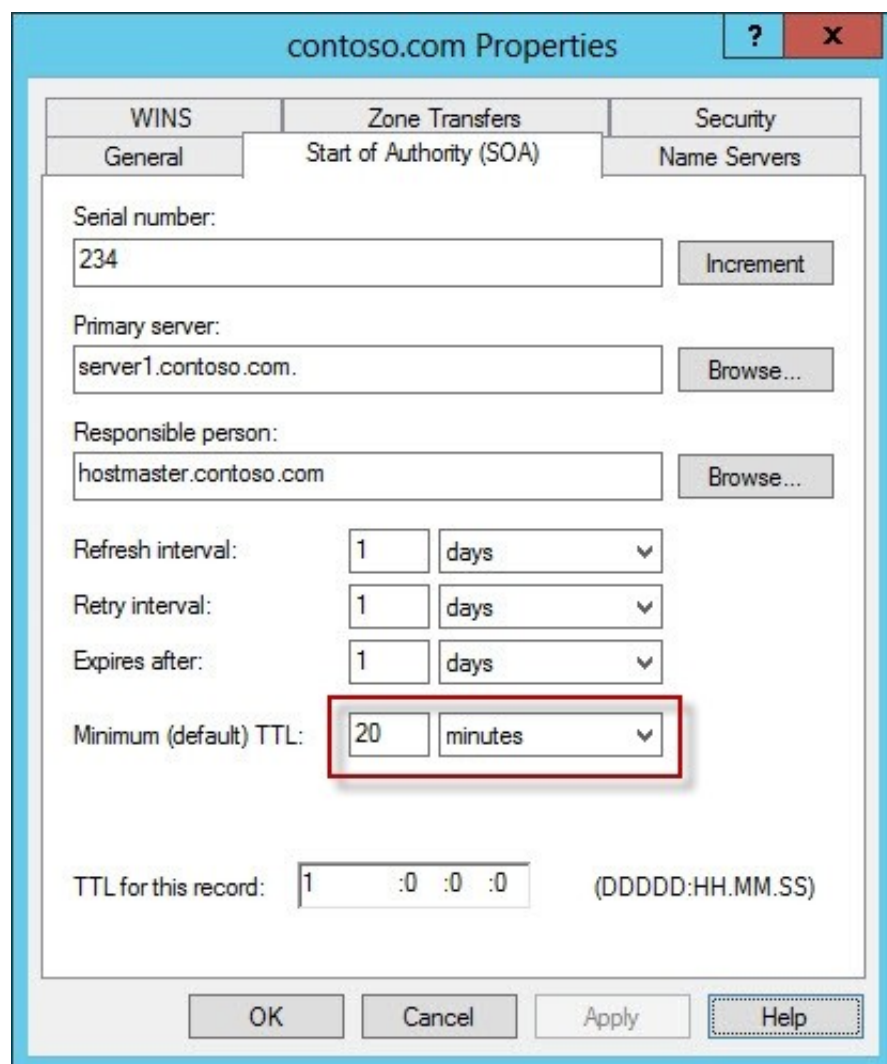
The Default TTL, is just that a default for newly created records. Once the records are created their TTL is independent of the Default TTL on the SOA. Microsoft DNS implementation copies the Default TTL setting to all newly created records their by giving them all independent TTL settings.

SOA Minimum Field: The SOA minimum field has been overloaded in the past to have three different meanings, the minimum TTL value of all RRs in a zone, the default TTL of RRs which did not contain a TTL value and the TTL of negative responses.

Despite being the original defined meaning, the first of these, the minimum TTL value of all RRs in a zone, has never in practice been used and is hereby deprecated. The second, the default TTL of RRs which contain no explicit TTL in the master zone file, is relevant only at the primary server. After a zone transfer all RRs have explicit TTLs and it is impossible to determine whether the TTL for a record was explicitly set or derived from the default after a zone transfer. Where a server does not require RRs to include the TTL value explicitly, it should provide a mechanism, not being the value of the MINIMUM field of the SOA record, from which the missing TTL values are obtained. How this is done is implementation dependent.

TTLs also occur in the Domain Name System (DNS), where they are set by an authoritative name server for a particular resource record. When a caching (recursive) nameserver queries the authoritative nameserver for a resource record, it will cache that record for the time (in seconds) specified by the TTL. If a stub resolver queries the caching nameserver for the same record before the TTL has expired, the caching server will simply reply with the already cached resource record rather than retrieve it from the authoritative nameserver again.

Shorter TTLs can cause heavier loads on an authoritative nameserver, but can be useful when changing the address of critical services like Web servers or MX records, and therefore are often lowered by the DNS administrator prior to a service being moved, in order to minimize disruptions.



```
C:\Windows\system32>ipconfig /displaydns
```

Windows IP Configuration

```
dc1
-----
Record Name . . . . . : dc1.home.local
Record Type . . . . . : 1
Time To Live . . . . . : 1196
Data Length . . . . . : 4
Section . . . . . : Answer
A <Host> Record . . . . : 192.168.1.10
```

```
> set type=soa
> dc1
Server: dc1.home.local
Address: 192.168.1.10

home.local
primary name server = dc1.home.local
responsible mail addr = hostmaster.home.local
serial = 281
refresh = 900 <15 mins>
retry = 600 <10 mins>
expire = 300 <5 mins>
default TTL = 1200 <20 mins>
dc1.home.local internet address = 192.168.1.10
```

#### NEW QUESTION 69

HOTSPOT - (Topic 2)

You have a server named Server1 that has the Network Policy and Access Services server role installed.

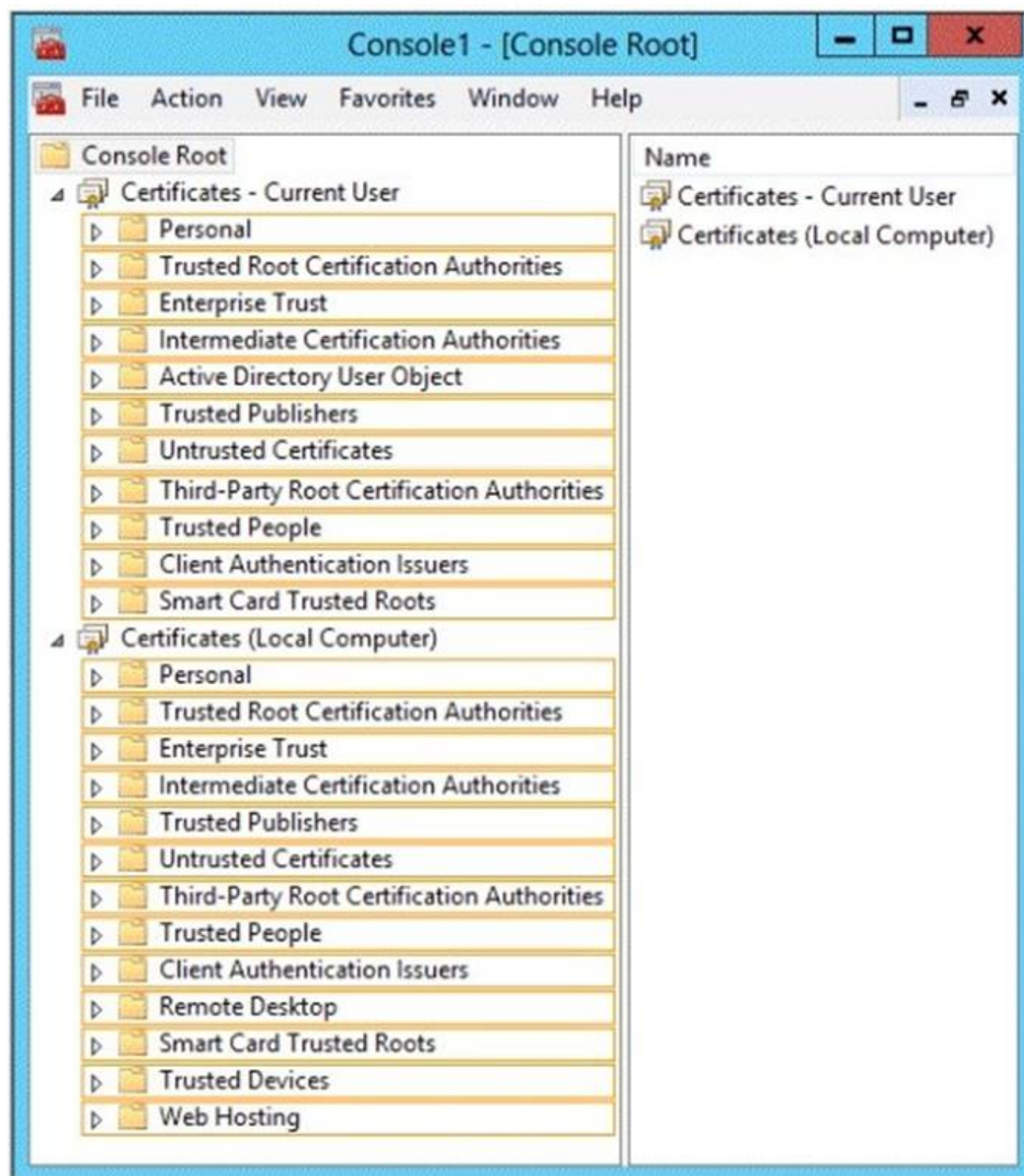
You plan to configure Network Policy Server (NPS) on Server1 to use certificate-based authentication for VPN connections.

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.





- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

When organizations deploy their own public key infrastructure (PKI) and install a private trusted root CA, their 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 certificate store. After this occurs, the domain member computers trust certificates that are issued by the organization trusted root CA.

For example, if you install AD CS, the CA sends its certificate to the domain member computers in your organization and they store the CA certificate in the Trusted Root Certification Authorities certificate store on the local computer. If you also configure and autoenroll a server certificate for your NPS servers and then deploy PEAP-MS-CHAP v2 for wireless connections, all domain member wireless client computers can successfully authenticate your NPS servers using the NPS server certificate because they trust the CA that issued the NPS server certificate.

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 that 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.

**References:**

<http://technet.microsoft.com/en-us/library/cc730811.aspx> <http://technet.microsoft.com/en-us/library/cc730811.aspx>  
<http://technet.microsoft.com/en-us/library/cc772401%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/ee407543%28v=ws.10%29.aspx>

**NEW QUESTION 74**

HOTSPOT - (Topic 2)

You have a server named LON-SVR1 that runs Windows Server 2012 R2. LON-SVR1 has the Remote Access server role installed. LON-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.)

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

Your company purchases an additional router named Router1. Router1 has an interface that connects to the perimeter network and an interface that connects to the Internet. The IP address of the interface that connects to the perimeter network is 172.16.0.2.

You need to ensure that LON-SVR1 will route traffic to the Internet by using Router1 if the current default gateway is unavailable.

How should you configure the static route on LON-SVR1? To answer, select the appropriate static route in the answer area.

IPv4 Static Route

Interface: Local Area Connection

Destination: 0 . 0 . 0 . 0

Network mask: 0 . 0 . 0 . 0

Gateway: 172 . 16 . 0 . 2

Metric: 300

☒ Use this route to initiate demand-dial connections

[For more information](#)

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

- A. Mastered  
B. Not Mastered

**Answer:** A

#### Explanation:

Metric: Specifies an integer cost metric (ranging from 1 to 9999) for the route, which is used when choosing among multiple routes in the routing table that most closely match the destination address of a packet being forwarded. The route with the lowest metric is chosen. The metric can reflect the number of hops, the speed of the path, path reliability, path throughput, or administrative properties.

A metric is a value that is assigned to an IP route for a particular network interface that identifies the cost that is associated with using that route.

The metric that is assigned to specific default gateways can be configured independently for each gateway. This setup enables a further level of control over the metric that is used for the local routes.

#### NEW QUESTION 78

- (Topic 2)

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



are configured as shown in the following table.

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

All client computers run Windows 8 Enterprise.

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

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

You need to ensure that the client computers can discover HRA servers automatically. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

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

**Answer:** ABE

**Explanation:**

Requirements for HRA automatic discovery

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

Client computers must be running Windows Vista® with Service Pack 1 (SP1) or Windows XP with Service Pack 3 (SP3).

The HRA server must be configured with a Secure Sockets Layer (SSL) certificate. The EnableDiscovery registry key must be configured on NAP client computers. DNS SRV records must be configured.

The trusted server group configuration in either local policy or Group Policy must be cleared.

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

**NEW QUESTION 81**

- (Topic 2)

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.

**Answer:** B

**Explanation:**

PSOs cannot be applied to organizational units (OUs) directly. If your users are organized into OUs, consider creating global security groups that contain the users from these OUs and then applying the newly defined finegrained password and account lockout policies to them. If you move a user from one OU to another, you must update user memberships in

the corresponding global security groups.

Go ahead and hit "OK" and then close out of all open windows. Now that you have created a password policy, we need to apply it to a user/group. In order to do so, you must have "write" permissions on the PSO object. We're doing this in a lab, so I'm Domain Admin. Write permissions are not a problem

1. Open Active Directory Users and Computers (Start, point to Administrative Tools, and then click Active Directory Users and Computers).
2. On the View menu, ensure that Advanced Features is checked.
3. In the console tree, expand Active Directory Users and Computers\yourdomain\System>Password Settings Container
4. In the details pane, right-click the PSO, and then click Properties.
5. Click the Attribute Editor tab.
6. Select the msDS-PsoAppliesTo attribute, and then click Edit.

**NEW QUESTION 83**

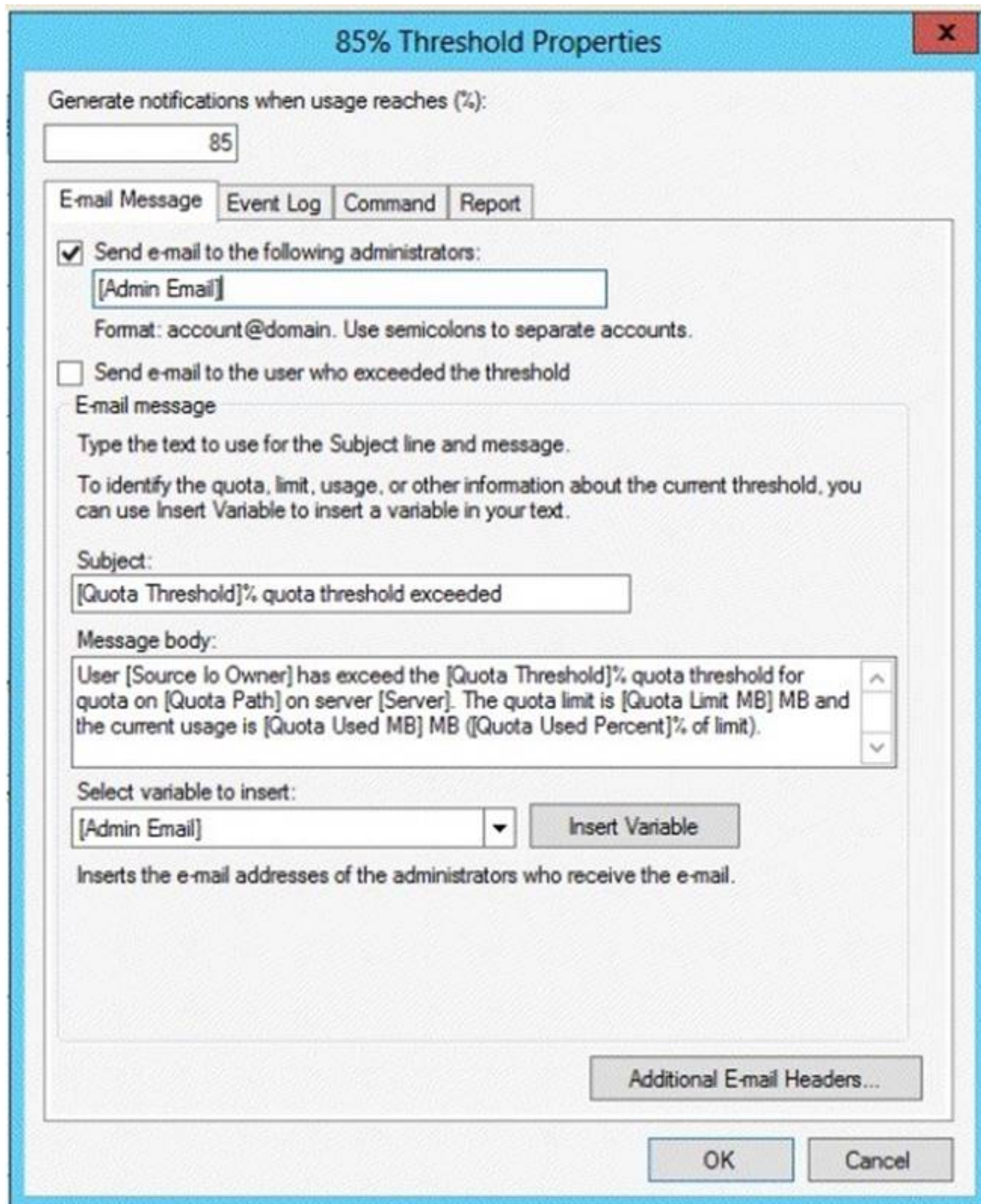
- (Topic 2)

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

Server1 has the File Server Resource Manager role service installed.

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





**85% Threshold Properties**

Generate notifications when usage reaches (%):

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

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

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

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

**Subject:**

**Message body:**

**Select variable to insert:**

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

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

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

**Answer: D**

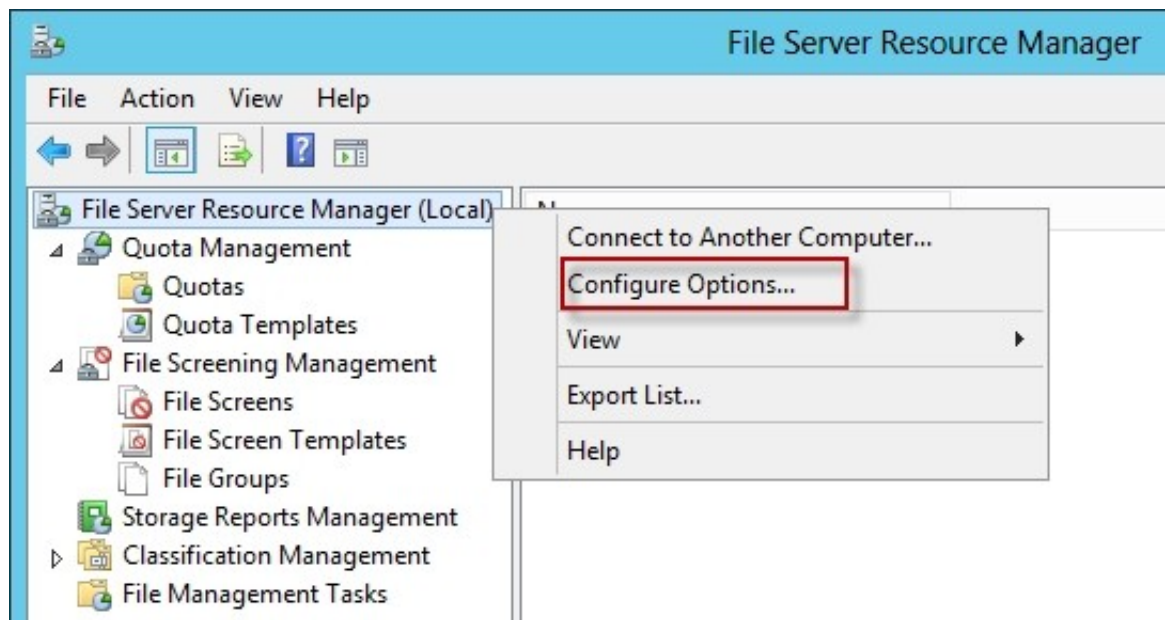
**Explanation:**

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

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

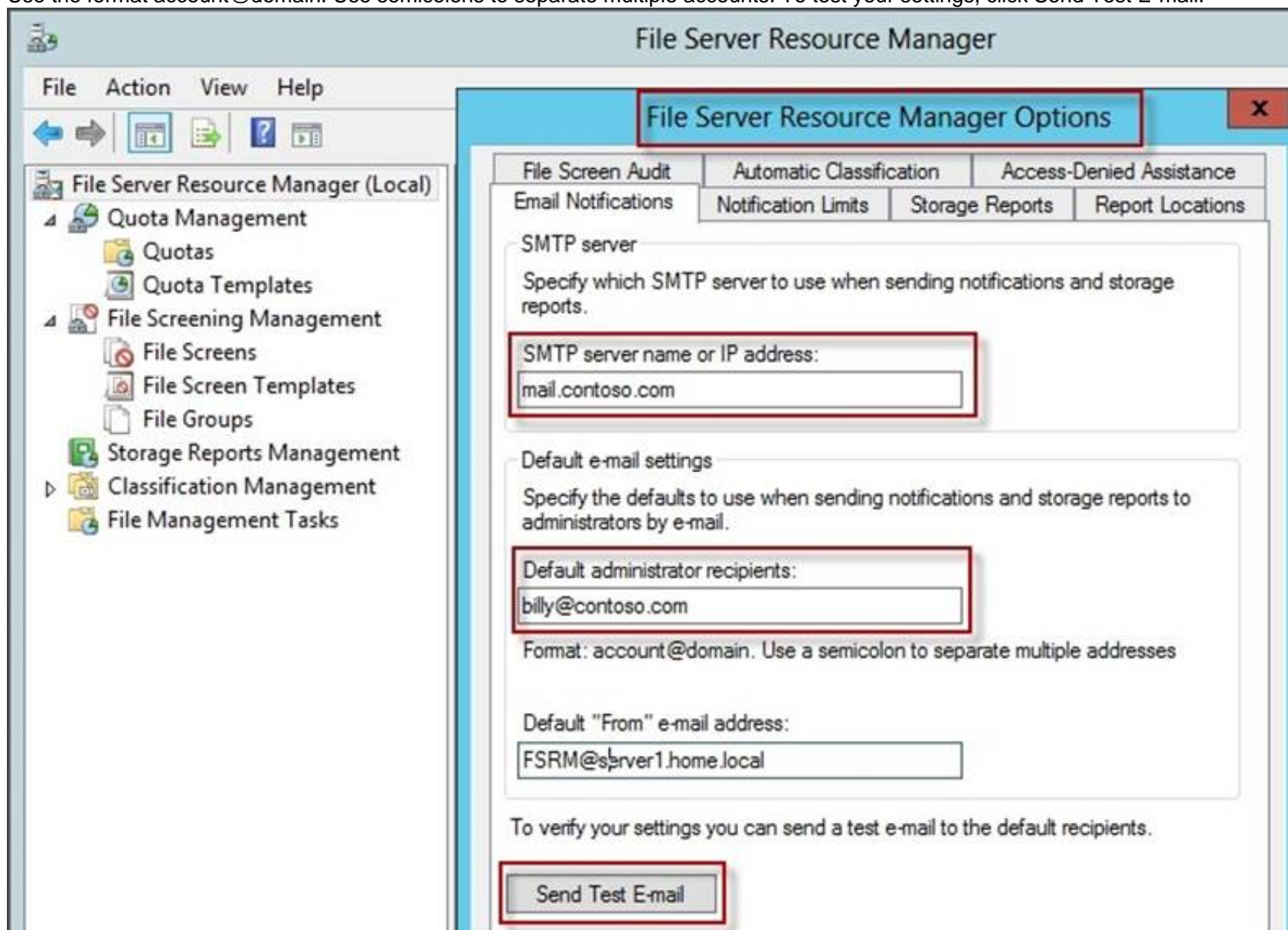
To configure e-mail options

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

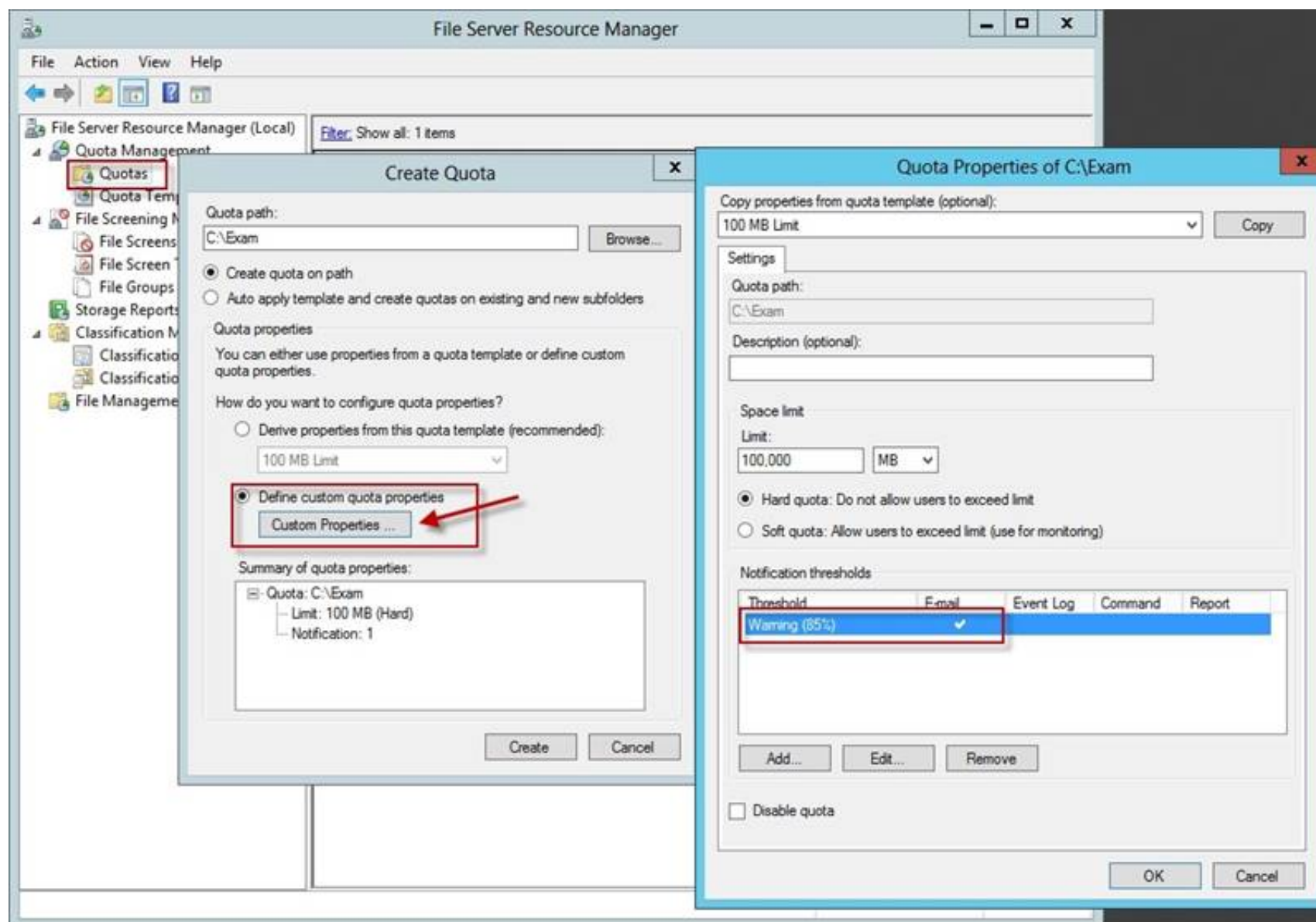


On the E-mail Notifications tab, under SMTP server name or IP address, type the host name or the IP address of the SMTP server that will forward e-mail notifications.

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







#### NEW QUESTION 85

- (Topic 3)

Your network contains one Active Directory domain. The domain contains a DirectAccess deployment.

You need to ensure that when the DirectAccess connection is active, the connection appears as "Contoso Internal Network -Authorized Users Only" on the DirectAccess clients.

What should you configure in the DirectAccess client Group Policy object (GPO)?

- A. Friendly Name
- B. Corporate Resources
- C. User Interface
- D. Prefer Local Names Allowed

**Answer: A**

#### NEW QUESTION 86

- (Topic 3)

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

You need to ensure that you can view update reports and computer reports on Server01.

Which two components should you install? Each correct answer presents part of the solution.

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

**Answer: BD**

#### NEW QUESTION 88

- (Topic 3)

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

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

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

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

What should you configure?

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

**Answer: D**



**Explanation:**

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

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

**NEW QUESTION 93**

- (Topic 3)

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.

**Answer: C**

**NEW QUESTION 97**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.

You need to identify whether the members of the Protected Users group will be prevented from authenticating by using NTLM.

Which cmdlet should you use?

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

**Answer: D**

**Explanation:**

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

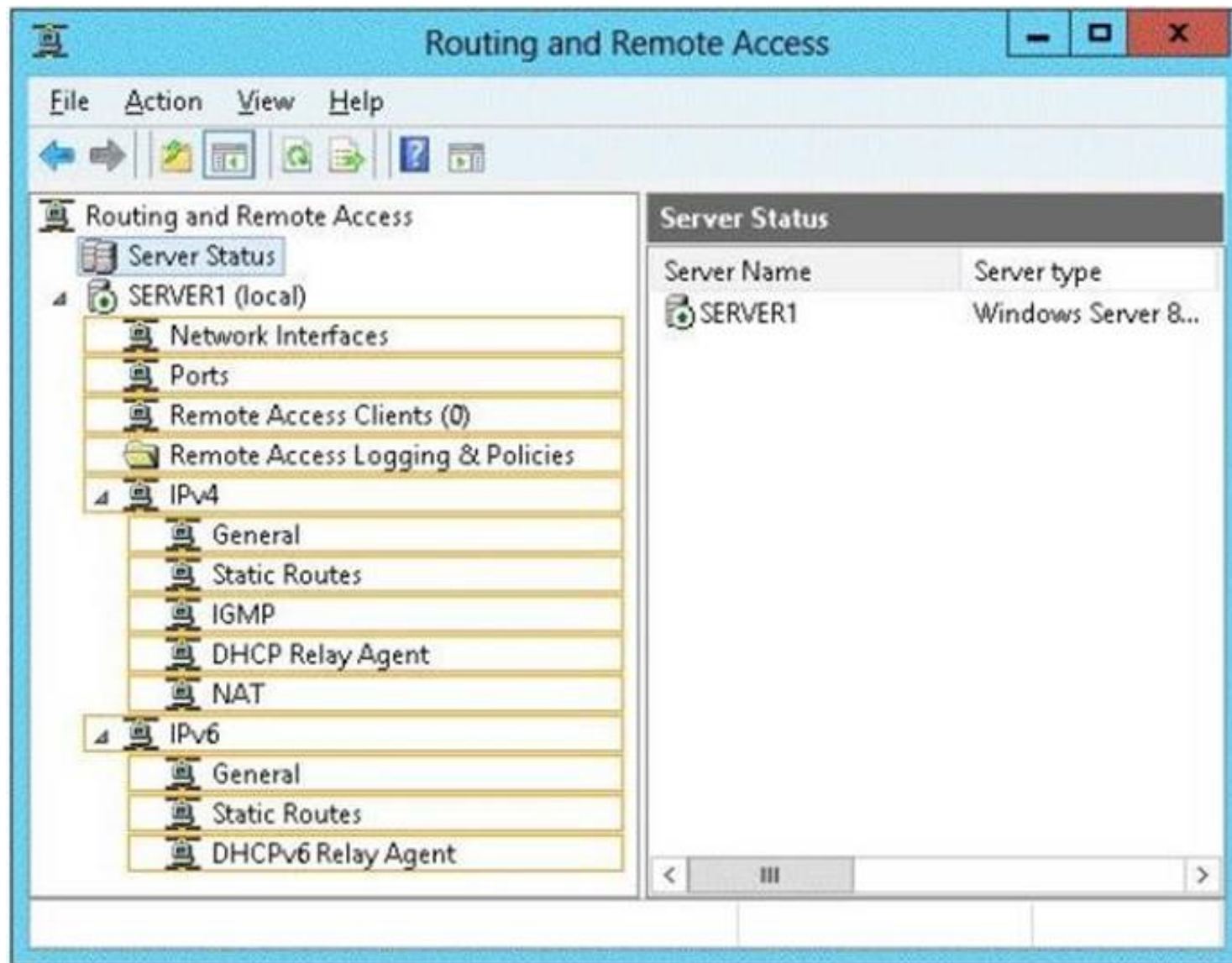
**NEW QUESTION 99**

HOTSPOT - (Topic 3)

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 configure Server1 as a network address translation (NAT) server. Which node should you use to add the NAT routing protocol?

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References: [https://technet.microsoft.com/en-us/library/dd469812\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dd469812(v=ws.11).aspx)

**NEW QUESTION 100**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

References:

<https://technet.microsoft.com/en-GB/library/jj134239.aspx>

**NEW QUESTION 101**

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. You create a new user account named Admin5. You need to ensure that Admin5 can create Group Policy objects (GPOs) and link the GPOs to all of the organizational units (OUs) in the domain. Admin5 must be prevented from modifying GPOs created by other administrators. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Answer:** CD

**NEW QUESTION 106**

- (Topic 3)

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012 R2. The domain contains two domain controllers. The domain controllers are configured as shown in the following table.

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

Active Directory Recycle Bin is enabled.

You discover that a support technician accidentally removed 100 users from an Active Directory group named Group1 an hour ago.

You need to restore the membership of Group1. What should you do?

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

**Answer:** D

#### NEW QUESTION 110

HOTSPOT - (Topic 3)

Your network contains one Active directory forest named contoso.com. The forest contains

a single domain. All domain controllers are virtual machines that run Windows Server 2012 R2. The functional level of the domain and the forest is Windows Server 2012 R2.

The forest contains the domain controllers configured as shown in the following table.

Domain controller name	Configuration
DC01	Active Directory Lightweight Directory Services (AD LDS) Domain naming master Schema master Global catalog DNS server
DC02	Active Directory Certificate Services (AD CS) Relative identifier (ID) master Infrastructure master PDC emulator master DNS server
DC03	Global catalog DHCP server DNS server
DC04	Internet Information Services (IIS) Global catalog DNS server

In the table below, select the domain controller that can be cloned by using domain controller cloning and select the domain controller that must be online to perform domain controller cloning.

NOTE: Make only one selection in each column.

Domain controller	Can be cloned by using domain controller cloning	Must be online to perform domain controller cloning
DC01	<input type="radio"/>	<input type="radio"/>
DC02	<input type="radio"/>	<input type="radio"/>
DC03	<input type="radio"/>	<input type="radio"/>
DC04	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A



**Explanation:**

References:

<http://blogs.technet.com/b/canitpro/archive/2013/06/12/step-by-step-domain-controller-cloning.aspx>

Domain controller	Can be cloned by using domain controller cloning	Must be online to perform domain controller cloning
DC01	<input type="radio"/>	<input type="radio"/>
DC02	<input type="radio"/>	<input checked="" type="radio"/>
DC03	<input type="radio"/>	<input type="radio"/>
DC04	<input checked="" type="radio"/>	<input type="radio"/>

PDC Emulator must be online to perform Domain Controller Cloning. The following server roles are not supported for cloning:

Dynamic Host Configuration Protocol (DHCP) Active Directory Certificate Services (AD CS)

Active Directory Lightweight Directory Services (AD LDS) [https://technet.microsoft.com/en-us/library/hh831734.aspx#virtualized\\_dc\\_cloning](https://technet.microsoft.com/en-us/library/hh831734.aspx#virtualized_dc_cloning)

<http://blogs.technet.com/b/canitpro/archive/2013/06/12/step-by-step-domain-controller-cloning.aspx>

**NEW QUESTION 112**

- (Topic 3)

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

DirectAccess is deployed to the network.

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

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

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

Which Group Policy setting should you configure?

- A. Configure Group Policy slow link detection.
- B. Configure Direct Access connections as a fast network connection.
- C. Configure wireless policy processing.
- D. Change Group Policy processing to run asynchronously when a slow network connection is detected.

**Answer: A**

**NEW QUESTION 115**

- (Topic 3)

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

**Answer: D**

**Explanation:**

[http://www.windowsnetworking.com/articles\\_tutorials/Configuring-DFS-Namespaces.html](http://www.windowsnetworking.com/articles_tutorials/Configuring-DFS-Namespaces.html)

**NEW QUESTION 117**

- (Topic 3)

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

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

All of the computer accounts for the human resources department are members of a group named HR Computers.

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

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

What should you configure?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 120**

- (Topic 3)

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

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

You deploy a new domain controller named DC3 that runs Windows Server 2012 R2. You discover that you cannot create Password Settings objects (PSOs) by using Active Directory Administrative Center.

You need to ensure that you can create PSOs from Active Directory Administrative Center. What should you do?

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

**Answer: C**

#### NEW QUESTION 125

HOTSPOT - (Topic 3)

Your network contains one Active Directory domain named contoso.com. The domain contains 10 file servers that run Windows Server 2012 R2.

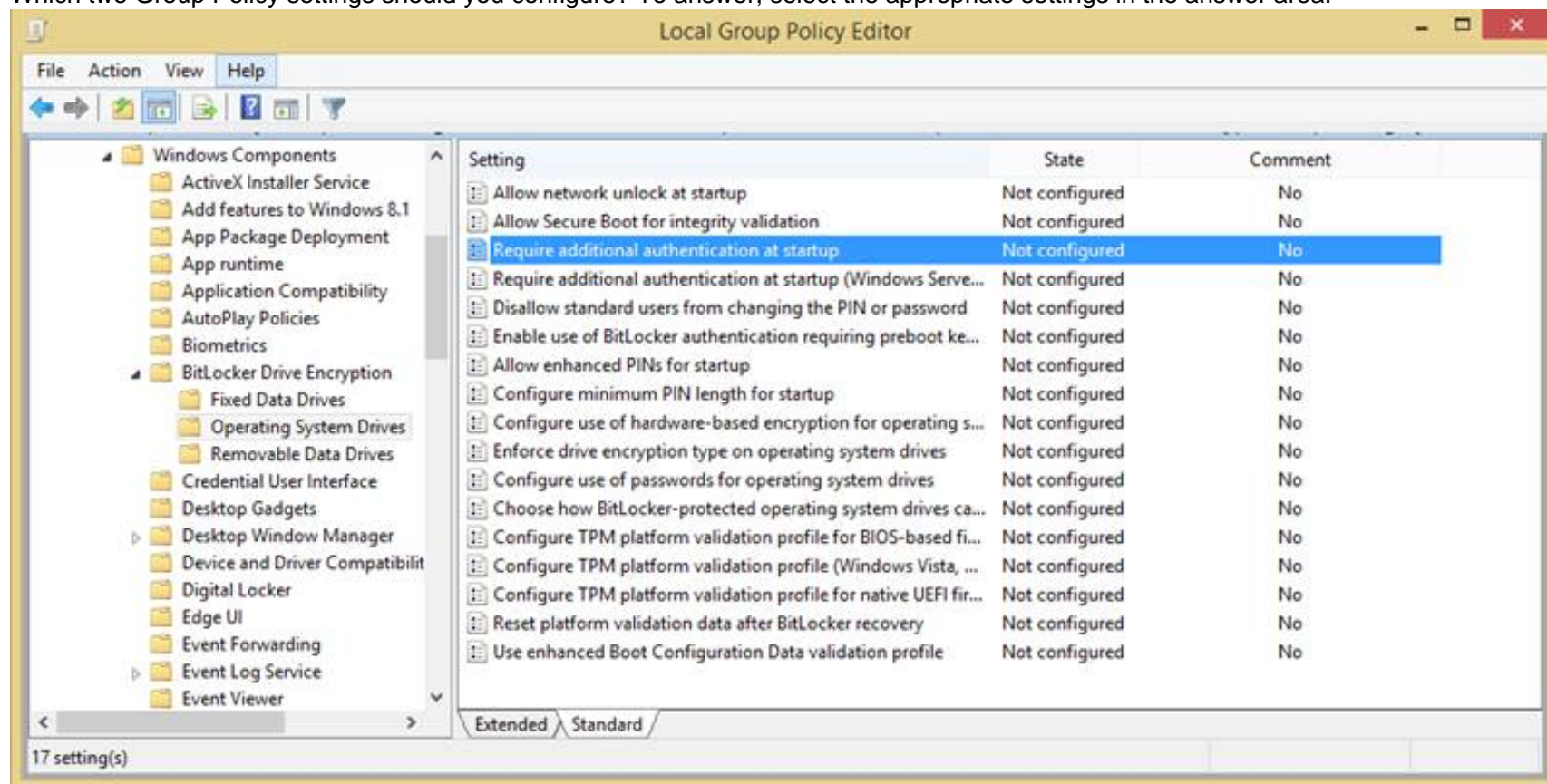
You plan to enable BitLocker Drive Encryption (BitLocker) for the operating system drives of the file servers.

You need to configure BitLocker policies for the file servers to meet the following requirements:

? Ensure that all of the servers use a startup PIN for operating system drives encrypted with BitLocker.

? Ensure that the BitLocker recovery key and recovery password are stored in Active Directory.

Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Choose how BitLocker-protected operating system drives can be recovered: With this policy setting, you can control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. In Save BitLocker recovery information to Active Directory Domain Services, choose which BitLocker recovery information to store in Active Directory Domain Services (AD DS) for operating system drives. If you select Store recovery password and key packages, the BitLocker recovery password and the key package are stored in AD DS. Storing the key package supports recovering data from a drive that is physically corrupted. If you select Store recovery password only, only the recovery password is stored in AD DS.

Require additional authentication at startup: With this policy setting, you can configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker. On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use:

- only the TPM for authentication
- insertion of a USB flash drive containing the startup key
- the entry of a 4-digit to 20-digit personal identification number (PIN)
- a combination of the PIN and the USB flash drive

There are four options for TPM-enabled computers or devices:

- Configure TPM startup
  - o Allow TPM
  - o Require TPM
  - o Do not allow TPM
- Configure TPM startup PIN
  - o Allow startup PIN with TPM
  - o Require startup PIN with TPM
  - o Do not allow startup PIN with TPM
- Configure TPM startup key
  - o Allow startup key with TPM

- o Require startup key with TPM
  - o Do not allow startup key with TPM Configure TPM startup key and PIN
  - o Allow TPM startup key with PIN
  - o Require startup key and PIN with TPM
  - o Do not allow TPM startup key with PIN
- <https://technet.microsoft.com/en-us/library/jj679890.aspx>

**NEW QUESTION 127**

- (Topic 3)  
Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.  
The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.  
You need to identify whether deleted objects can be recovered from the Active Directory Recycle Bin.  
Which cmdlet should you use?

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

**Answer:** E

**Explanation:**

The Get-ADOptionalFeature cmdlet gets an optional feature or performs a search to retrieve multiple optional features from an Active Directory.  
Example: Get-ADOptionalFeature 'Recycle Bin Feature'  
Get the optional feature with the name 'Recycle Bin Feature'.  
Reference: Get-ADOptionalFeature <https://technet.microsoft.com/en-us/library/ee617218.aspx>

**NEW QUESTION 130**

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

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

**Answer:** B

**NEW QUESTION 132**

DRAG DROP - (Topic 3)  
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.

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.	



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Start Server2 by using PXE. Box 2: Add a capture image to Server1. Box 3: Add an install image to Server1. Note:

\* Capture images are Windows Preinstallation Environment (Windows PE) images that allow you to easily capture the install images that you prepare using Sysprep.exe. Instead of using complex command-line tools, once you have run Sysprep.exe on your reference computer, you can boot to the Windows Deployment Services client computer using PXE and select the capture image. When the capture image boots, it starts the Capture Image Wizard, which will guide you through the capture process and optionally upload the new install image to a Windows Deployment Services server.

Steps

/ create a capture image.

/ Create an install image.

/ Add the install image to the Windows Deployment Services server.

**NEW QUESTION 135**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that

runs Windows Server 2012 R2.

You need to identify which domain controller must be online when cloning a domain controller.

Which cmdlet should you use?

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

**Answer:** D

**Explanation:**

One requirement for cloning a domain controller is an existing Windows Server 2012 DC that hosts the PDC emulator role. You can run the Get-ADDomain and retrieve which server has the PDC emulator role.

Example: Command Prompt: C:\PS> Get-ADDomain

Output would include a line such as: PDCEmulator : Fabrikam-DC1.Fabrikam.com

Incorrect:

Not A: The Get-ADGroupMember cmdlet gets the members of an Active Directory group. Members can be users, groups, and computers.

Not E: The Get-ADOptionalFeature cmdlet gets an optional feature or performs a search to retrieve multiple optional features from an Active Directory.

Not F: The Get-ADAuthorizationGroup cmdlet gets the security groups from the specified user, computer or service accounts token.

Reference: Step-by-Step: Domain Controller Cloning <http://blogs.technet.com/b/canitpro/archive/2013/06/12/step-by-step-domain-controller-cloning.aspx>

Reference: Get-ADDomain <https://technet.microsoft.com/en-us/library/ee617224.aspx>

**NEW QUESTION 138**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The domain contains a server named Server01 that runs Windows Server 2012 R2.

Server01 does not have a Trusted Platform Module (TPM).

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

Which Group policy setting should you configure?

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

**Answer:** A

**NEW QUESTION 141**

- (Topic 3)

You have a DNS server that runs Windows Server 2012 R2. The server hosts the zone for contoso.com and is accessible from the Internet.

You need to create a DNS record for the Sender Policy Framework (SPF) to list the hosts that are authorized to send email for contoso.com.

Which type of record should you create?

- A. mail exchanger (MX)
- B. resource record signature (RRSIG)
- C. text (TXT)
- D. name server (NS)

**Answer:** C

**NEW QUESTION 145**

- (Topic 3)

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 148**

.....

## About ExamBible

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

## Found in 1998

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

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

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



### NEW QUESTION 1

- (Topic 1)

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

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

Server1 provides VPN access to external users.

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

What should you run?

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

**Answer: C**

#### Explanation:

Add-RemoteAccessRadius

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

AccountingOnOffMsg<String>

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

? Enabled.

? Disabled. This is the default value.

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

### NEW QUESTION 2

- (Topic 1)

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

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

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

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

**Answer: C**

#### Explanation:

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

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

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

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

auditpol /resourceSACL

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

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

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

References:

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

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

### NEW QUESTION 3

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 P.2.

Server1 has the Network Policy and Access Services server role installed.

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

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

Which authentication method should you identify?

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

**Answer: C**

#### Explanation:

802.1X uses EAP, EAP-TLS, EAP-MS-CHAP v2, and PEAP authentication methods:

? EAP (Extensible Authentication Protocol) uses an arbitrary authentication method, such as certificates, smart cards, or credentials.

? EAP-TLS (EAP-Transport Layer Security) is an EAP type that is used in certificate-based security environments, and it provides the strongest authentication and key determination method.

? EAP-MS-CHAP v2 (EAP-Microsoft Challenge Handshake Authentication Protocol

version 2) is a mutual authentication method that supports password-based user or computer authentication.

? PEAP (Protected EAP) is an authentication method that uses TLS to enhance the security of other EAP authentication protocols.

#### NEW QUESTION 4

- (Topic 1)

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

You create a global group named RODC\_Admins.

You need to provide the members of RODC\_Admins with the ability to manage the hardware and the software on R0DC1. The solution must not provide RODC\_Admins with the ability to manage Active Directory objects. What should you do?

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

**Answer: D**

#### Explanation:

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

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

#### NEW QUESTION 5

- (Topic 1)

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

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

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

- A. Rid master
- B. Domain naming master
- C. PDC emulator
- D. Infrastructure master

**Answer: C**

#### Explanation:

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

Reference:

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

#### NEW QUESTION 6

- (Topic 1)

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

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

You need to ensure that end-to-end encryption is used between clients and Server2 when the clients connect to the network by using DirectAccess. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Answer:** BE

**Explanation:**

Unsure about these answers:

? A public key infrastructure must be deployed.

? Windows Firewall must be enabled on all profiles.

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

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

Windows Server® 2012 R2

Windows 8.1 Enterprise

Windows Server® 2012

Windows 8 Enterprise Windows Server® 2008 R2 Windows 7 Ultimate

Windows 7 Enterprise

? Force tunnel configuration is not supported with KerbProxy authentication.

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

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

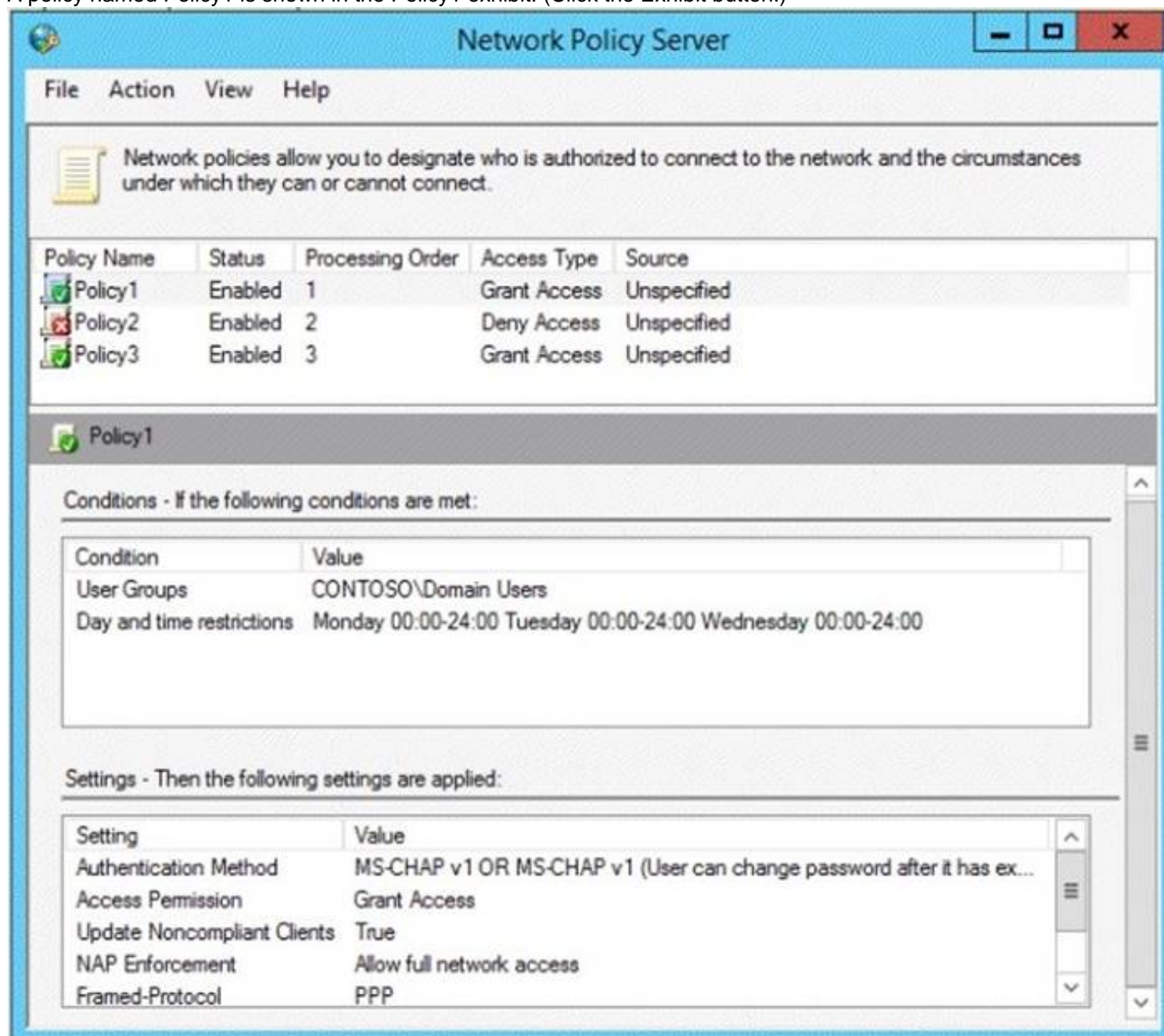
**NEW QUESTION 7**

HOTSPOT - (Topic 1)

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

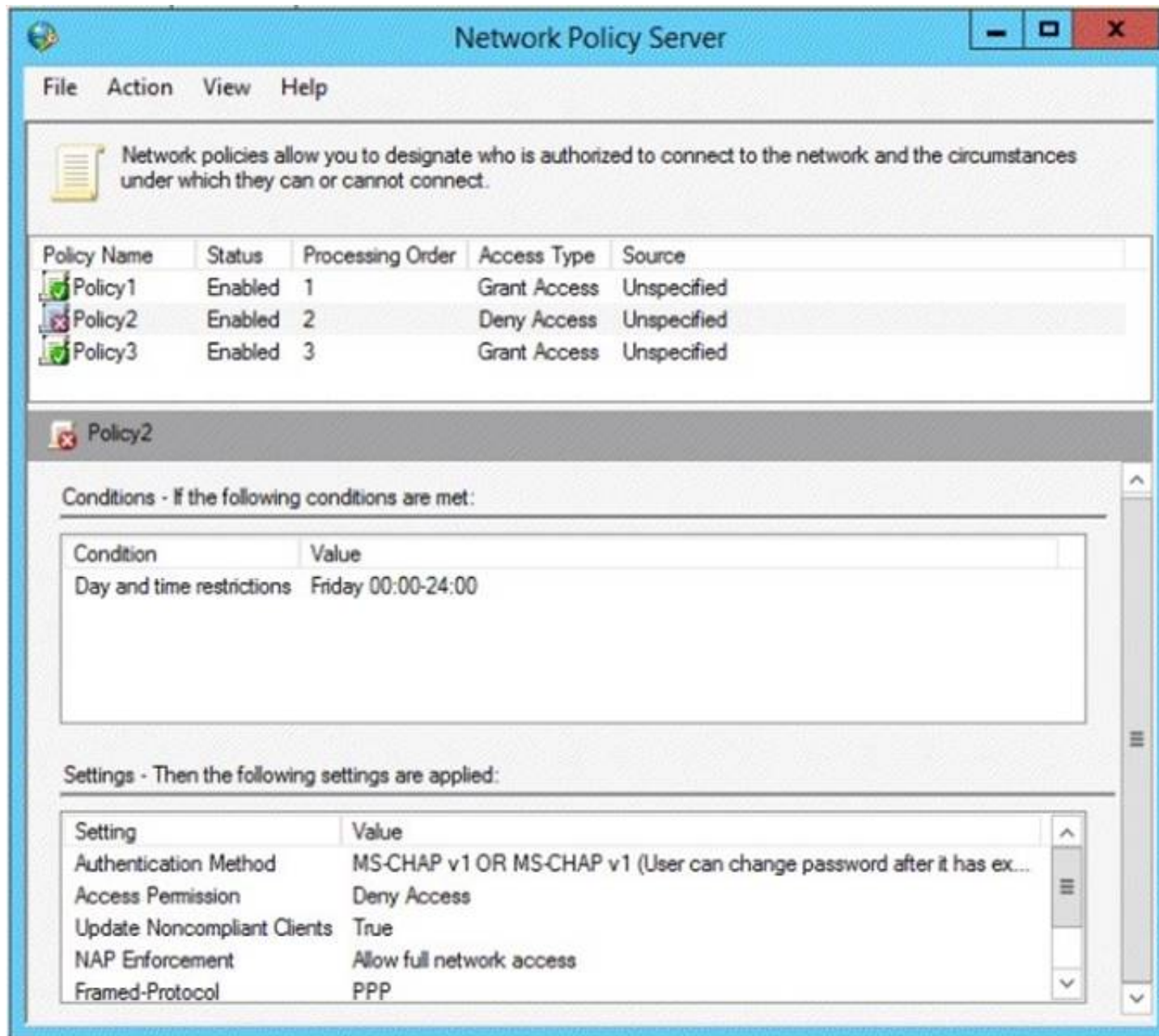
The Network Access Permission for User1 is set to Control access through NPS Network Policy. The Network Access Permission for User2 is set to Allow access.

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

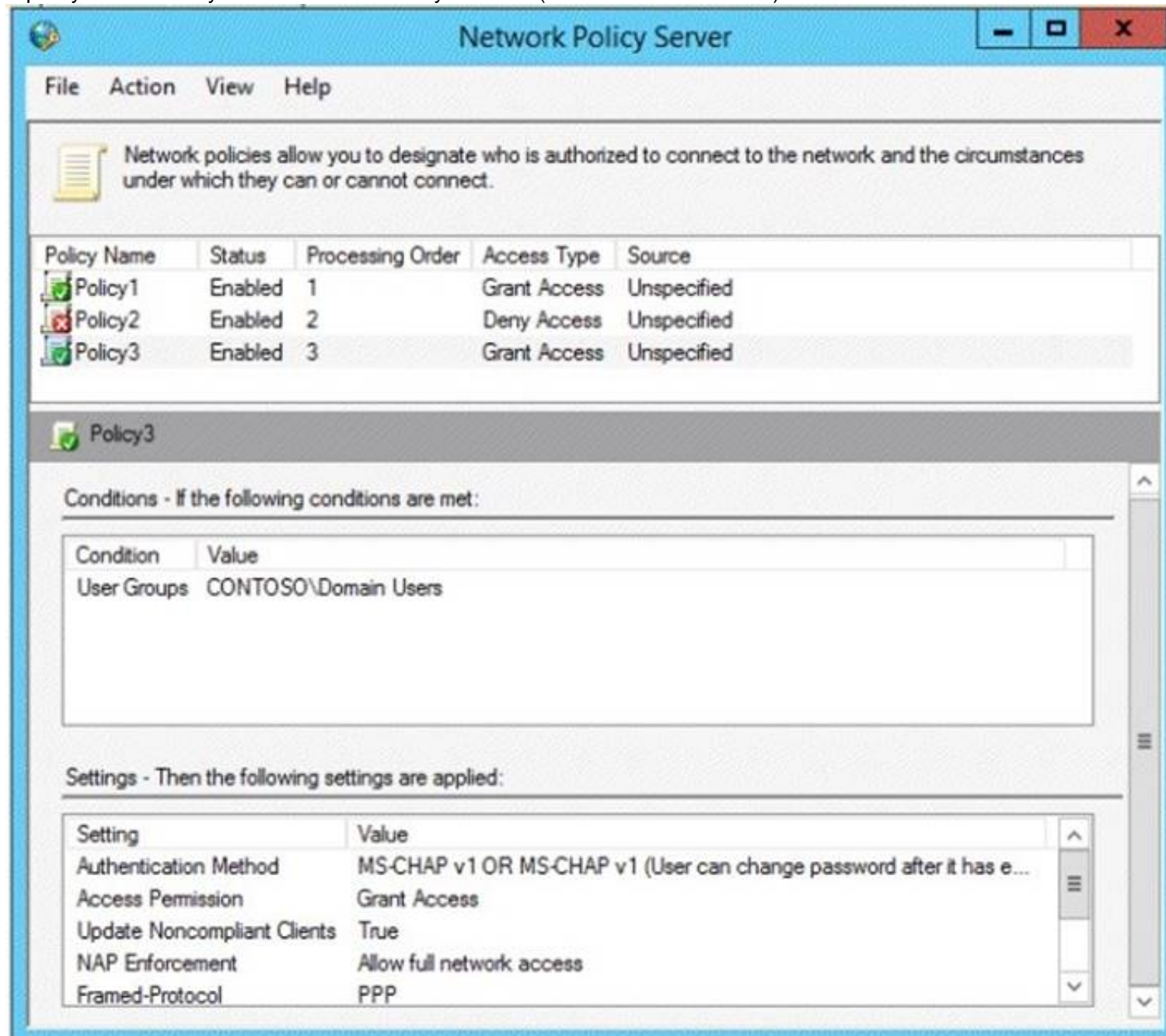


A policy named Policy2 is shown in the Policy2 exhibit. (Click the Exhibit button.)





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



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

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

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 8

HOTSPOT - (Topic 1)

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

User name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

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

Answer Area

User1:

User2:

User3:

#### Answer Area

User1:   
Policy1  
Policy2  
Policy3

User2:   
Policy1  
Policy2  
Policy3

User3:   
Policy1  
Policy2  
Policy3

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

Policies are processed in this order:

-Policy2 (applies only to members of Group1)

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

-Policy3 (applies only to members of Group2)

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

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

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

#### NEW QUESTION 9

- (Topic 1)

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

You deploy a new domain controller named DC1 that runs Windows Server 2012 R2. You log on to DC1 by using an account that is a member of the Domain Admins group. You discover that you cannot create Password Settings objects (PSOs) by using Active

Directory Administrative Center.

You need to ensure that you can create PSOs from Active Directory Administrative Center. What should you do?

- A. Modify the membership of the Group Policy Creator Owners group.
- B. Transfer the PDC emulator operations master role to DC1.
- C. Upgrade all of the domain controllers that run Window Server 2008.
- D. Raise the functional level of the domain.

**Answer:** D

#### Explanation:

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

Step 1: Create a PSO

Applies To: Windows Server 2008, Windows Server 2008 R2

ce:

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

#### NEW QUESTION 10

DRAG DROP - (Topic 1)

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

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

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



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

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

References:

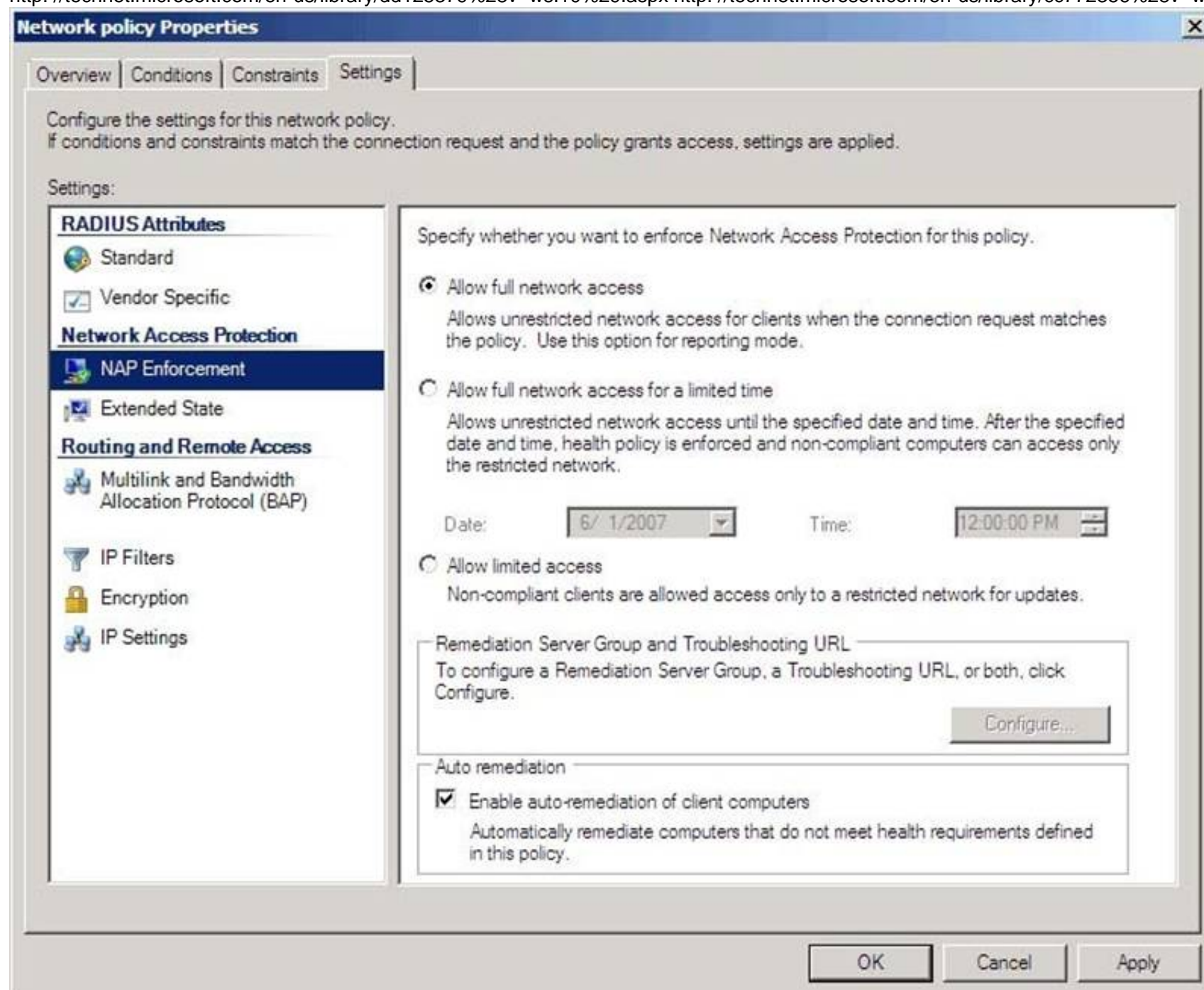
<http://technet.microsoft.com/es-es/library/dd314198%28v=ws.10%29.aspx>

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

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

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

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



**Network policy Properties**

Overview | Conditions | Constraints | Settings

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

Settings:

**RADIUS Attributes**

- Standard
- ☒ Vendor Specific

**Network Access Protection**

- NAP Enforcement**
  - ☒ Extended State

**Routing and Remote Access**

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

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

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

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

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

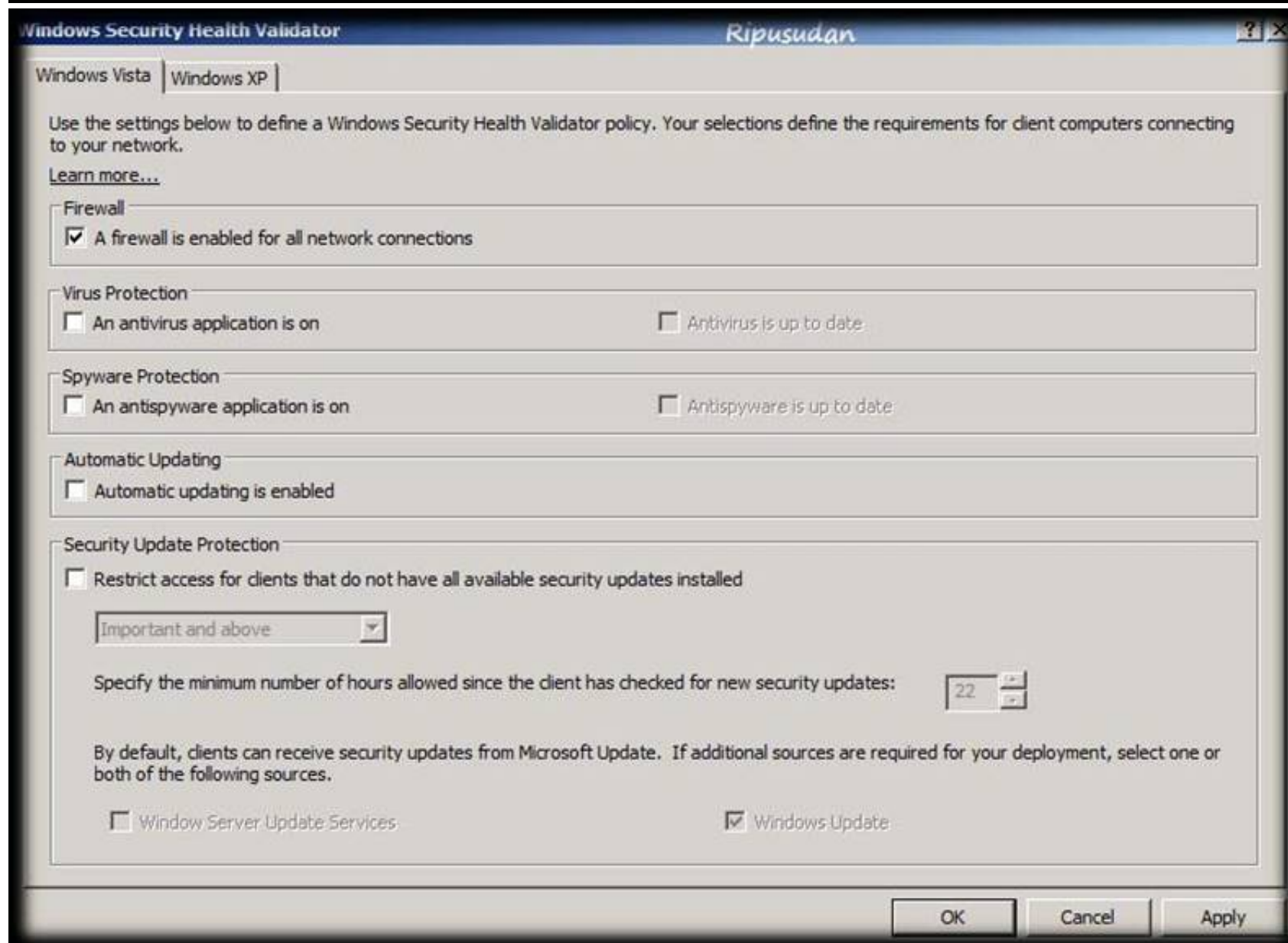
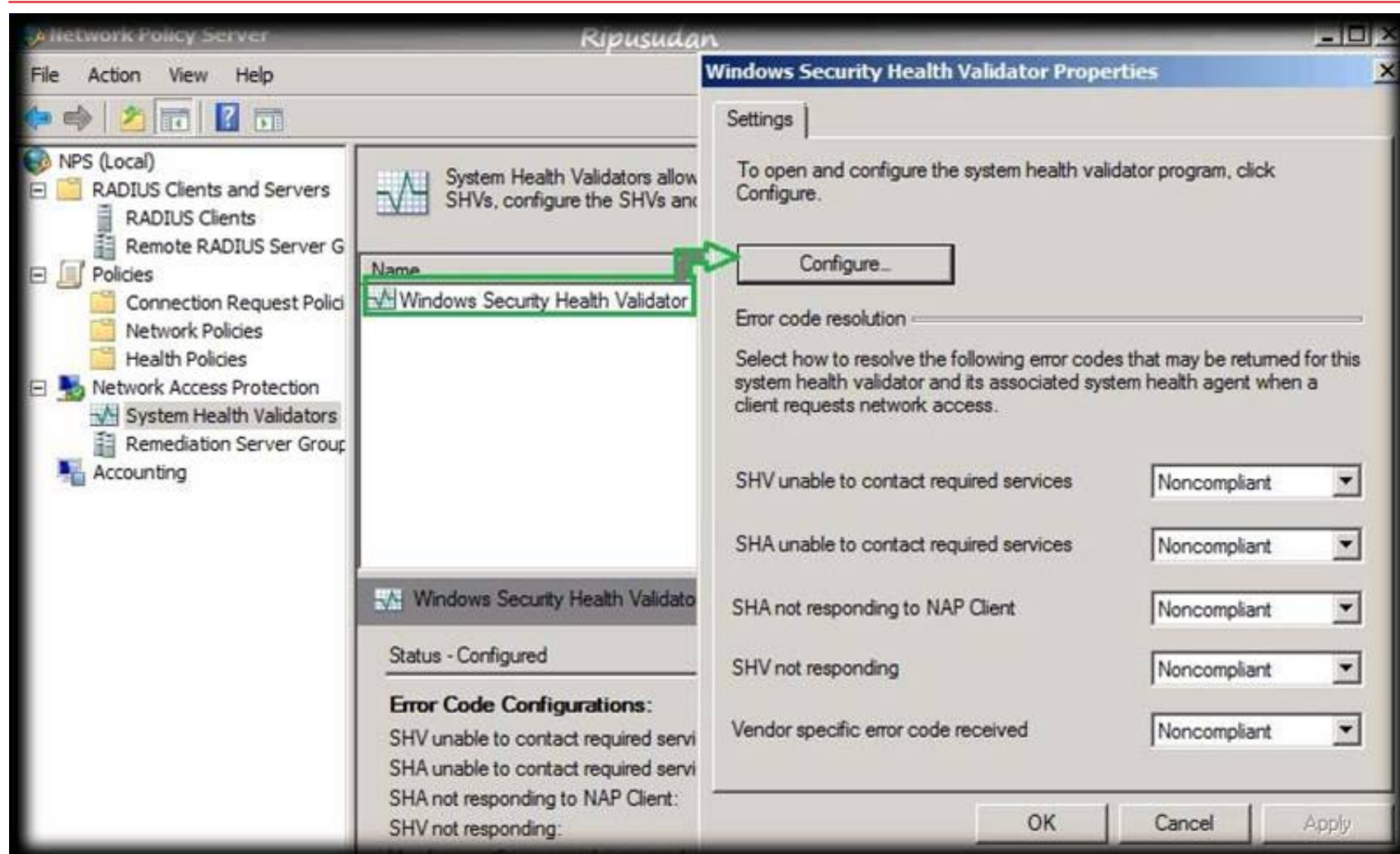
☐ Allow limited access  
 Non-compliant clients are allowed access only to a restricted network for updates.

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

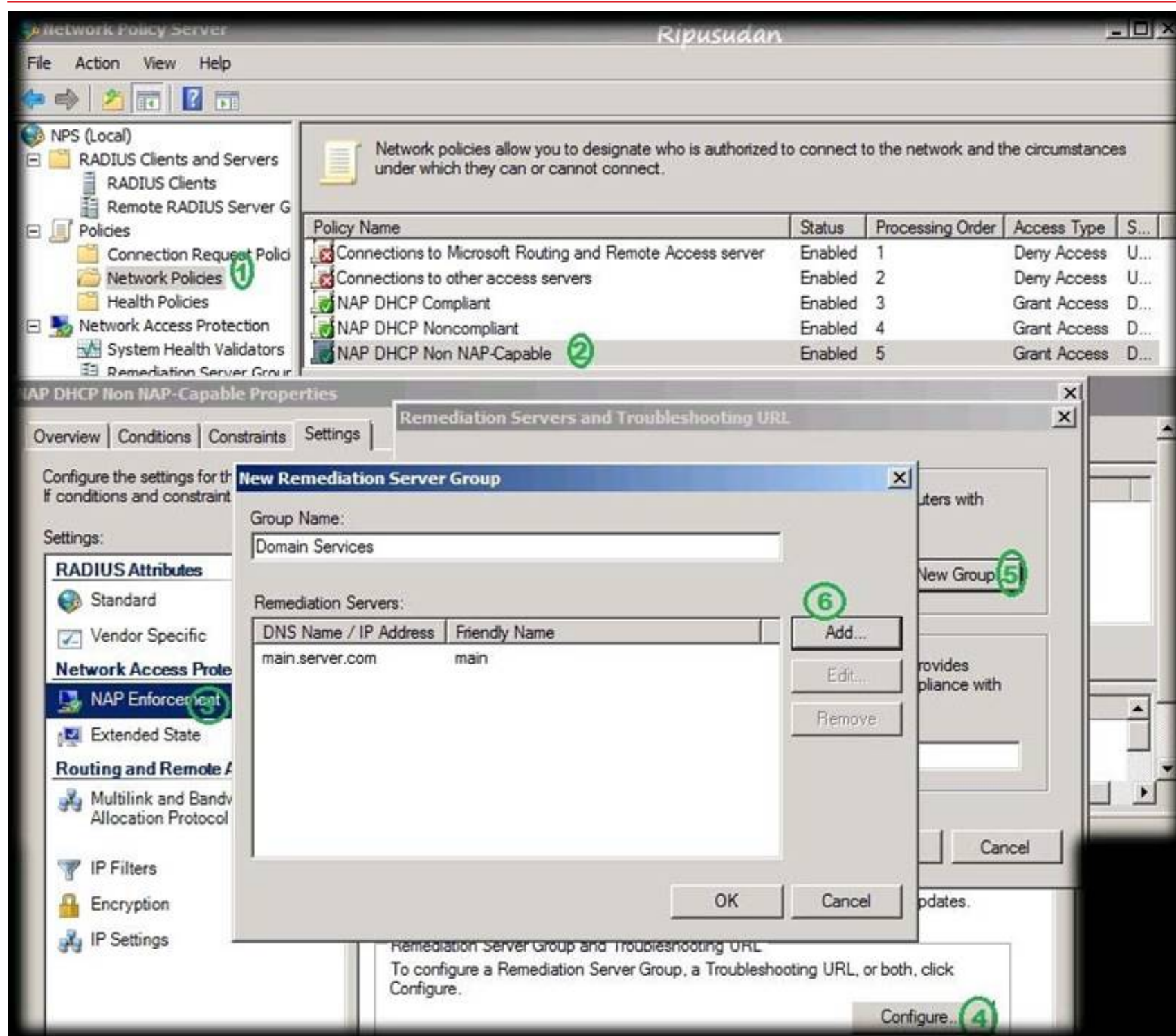
Auto remediation

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

OK Cancel Apply







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

\* Example measurements of health include:

The operational status of Windows Firewall. Is the firewall enabled or disabled?

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

#### NEW QUESTION 10

- (Topic 1)

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

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

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

What should you configure?

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

**Answer: B**

#### Explanation:

To configure data management for a Data Collector Set

1. In Windows Performance Monitor, expand Data Collector Sets and click User Defined.
2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click Data Manager.
3. On the Data Manager tab, you can accept the default values or make changes according to your data retention policy. See the table below for details on each option.

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

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

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

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

#### NEW QUESTION 14

- (Topic 1)

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



The domain 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. Gpedi
- F. msc
- G. Import-GPO
- H. Restore-GPO
- I. Set-GPInheritance
- J. Set-GPLink
- K. Set-GPPermission
- L. Gpupdate
- M. Add-ADGroupMember

**Answer:** J

**Explanation:**

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

-Replace <SwitchParameter>

Specifies that the existing permission level for the group or user is removed before the new permission level is set. If a security principal is already granted a permission level that is higher than the specified permission level and you do not use the Replace parameter, no change is made.

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

**NEW QUESTION 18**

- (Topic 1)

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

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

Which tool should you use?

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

**Answer:** C

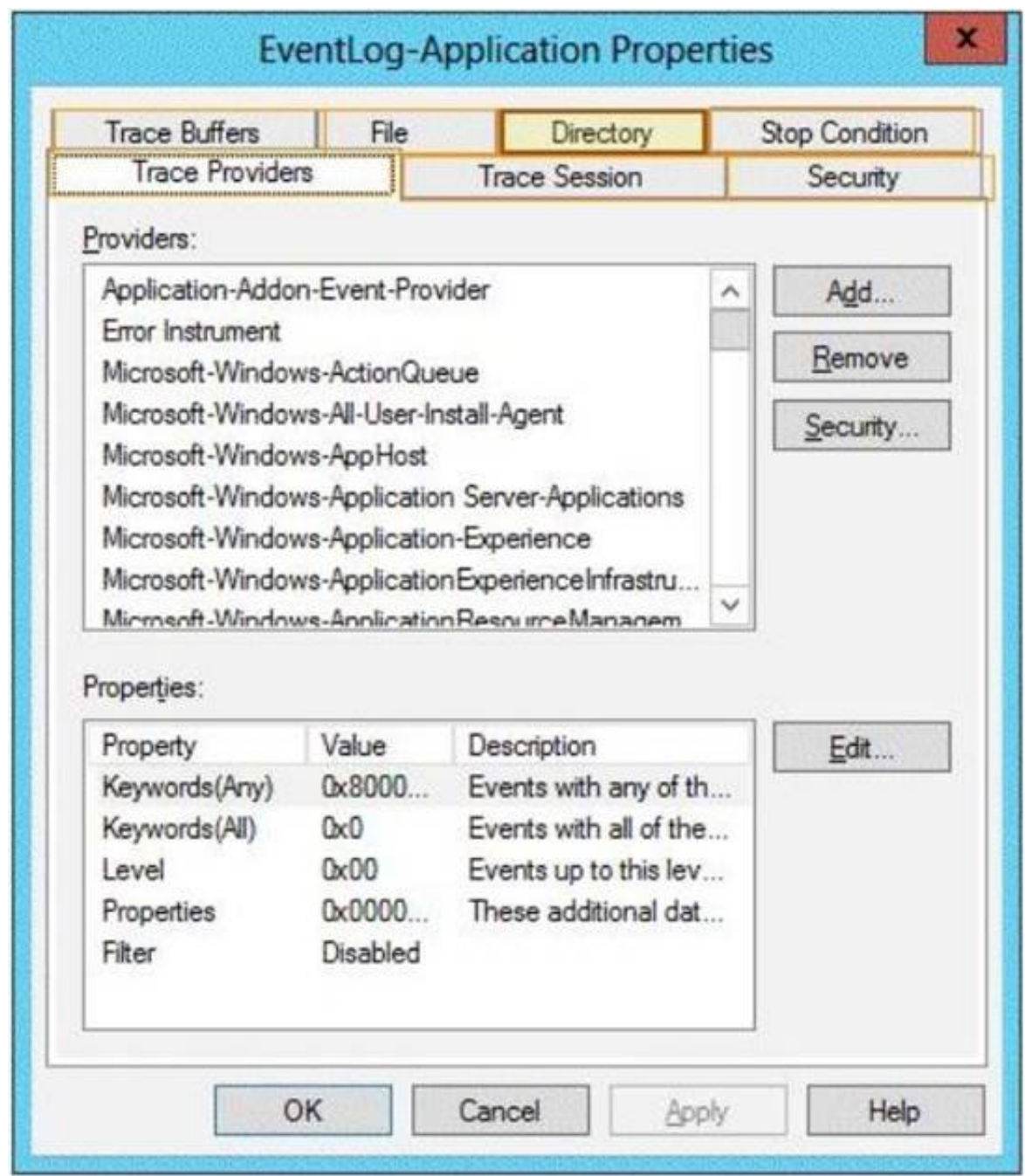
**NEW QUESTION 19**

HOTSPOT - (Topic 1)

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

You enable the EventLog-Application event trace session.

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 20

DRAG DROP - (Topic 1)

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

	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.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Note:

\* At a command prompt, specify the package identity to remove it from the image. You can remove multiple packages on one command line.

DISM /Image: C:\test\offline /Remove-Package /PackageName: Microsoft.Windows.Calc. Demo~6595b6144ccf1df~x86~en~1.0.0.0 /PackageName: Micro  
 /Cleanup-Image

Performs cleanup or recovery operations on the image.

**NEW QUESTION 23**

- (Topic 1)

You are a network administrator of an Active Directory domain named contoso.com.

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

You enable Network Access Protection (NAP) on all of the DHCP scopes on Server1. You need to create a DHCP policy that will apply to all of the NAP non-compliant DHCP

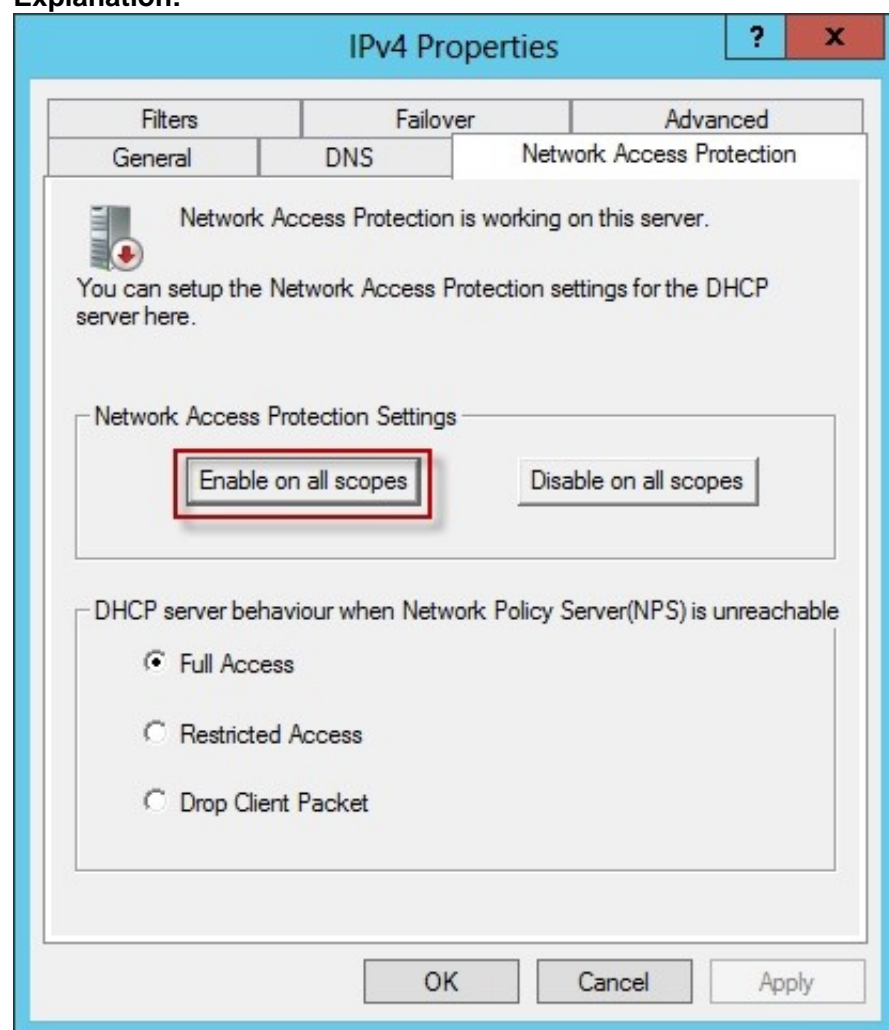
clients.

Which criteria should you specify when you create the DHCP policy?

- A. The client identifier
- B. The user class
- C. The vendor class
- D. The relay agent information

**Answer:** B

**Explanation:**



To configure a NAP-enabled DHCP server

? On the DHCP server, click Start, click Run, in Open, type dhcpgmt. smc, and then press ENTER.

? In the DHCP console, open <servername>\IPv4.

? Right-click the name of the DHCP scope that you will use for NAP client computers, and then click Properties.

? On the Network Access Protection tab, under Network Access Protection Settings, choose Enable for this scope, verify that Use default Network Access Protection profile is selected, and then click OK.

? In the DHCP console tree, under the DHCP scope that you have selected, right- click Scope Options, and then click Configure Options.

? On the Advanced tab, verify that Default User Class is selected next to User class.

? Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by compliant NAP client computers, and then click Add.

? Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each router to be used by compliant NAP client computers, and then click Add.

? Select the 015 DNS Domain Name check box, and in String value, under Data entry, type your organization's domain name (for example, woodgrovebank. local), and then click Apply. This domain is a full-access network assigned to compliant NAP clients.

? On the Advanced tab, next to User class, choose Default Network Access Protection Class.

? Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by noncompliant NAP client computers, and then click Add. This can be the same default gateway that is used by compliant NAP clients.

? Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each DNS server to be used by noncompliant NAP client computers, and then click Add. These can be the same DNS servers used by compliant NAP clients.

? Select the 015 DNS Domain Name check box, and in String value, under Data entry, type a name to identify the restricted domain (for example, restricted. Woodgrovebank. local), and then click OK. This domain is a restricted-access network assigned to noncompliant NAP clients.

? Click OK to close the Scope Options dialog box.

? Close the DHCP console.



Reference: <http://technet.microsoft.com/en-us/library/dd296905%28v=ws.10%29.aspx>

#### NEW QUESTION 26

- (Topic 1)

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

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

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

What should you do?

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

**Answer: A**

#### Explanation:

WSUS Reporting Rollup Sample Tool

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

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

#### NEW QUESTION 31

- (Topic 1)

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

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

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

What should you do?

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

**Answer: A**

#### Explanation:

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

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

2. Start group policy by running the following command:

`%SYSTEMROOT%\System32\gpedit.msc`.

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

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

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

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

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

#### NEW QUESTION 32

- (Topic 1)

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.

**Answer: D**

#### Explanation:

To configure an existing RRAS server to support both VPN remote access and NAT routing:

1. Open Server Manager.
2. Expand Roles, and then expand Network Policy and Access Services.
3. Right-click Routing and Remote Access, and then click Properties.

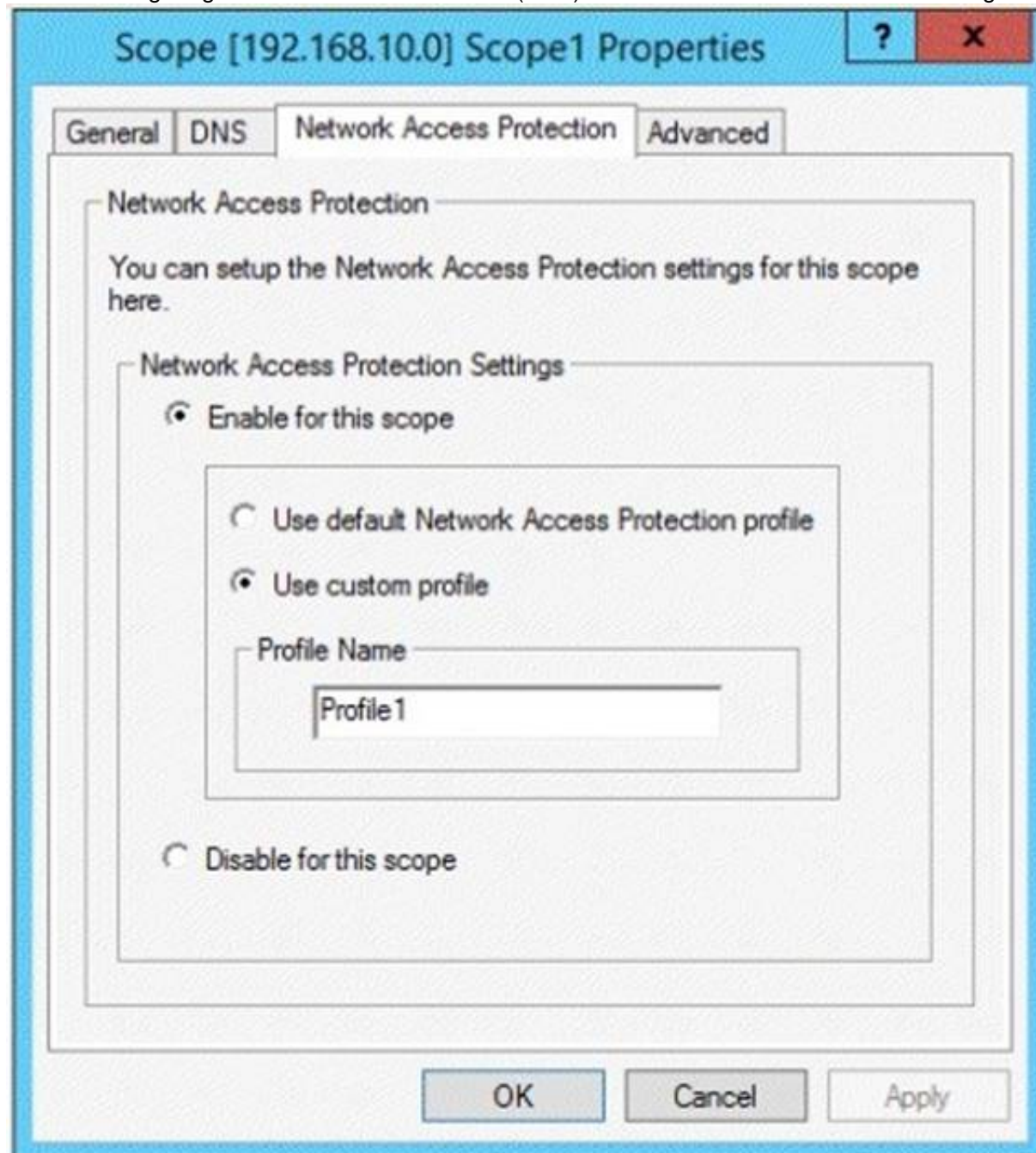
4. Select IPv4 Remote access Server or IPv6 Remote access server, or both.

**NEW QUESTION 33**

HOTSPOT - (Topic 1)

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.

**Answer Area**

Server1:

Server2:

**Answer Area**

Server1:   
Health Policies  
Identity-Type  
MS-Service Class  
Service-Type

Server2:   
filters  
a policy  
scope options  
server options  
a User class  
a Vendor class

A. Mastered



B. Not Mastered

**Answer:** A

**Explanation:**

Health Policies Server Options

\* Health policy on the NAP server.

\* The DHCP server must be NAP enabled.

Note: With DHCP enforcement, a computer must be compliant to obtain an unlimited access IP address configuration from a DHCP server. For noncompliant computers, network access is limited by an IP address configuration that allows access only to the restricted network. DHCP enforcement enforces health policy requirements every time a DHCP client attempts to lease or renew an IP address configuration. DHCP enforcement also actively monitors the health status of the NAP client and renews the IPv4 address configuration for access only to the restricted network if the client becomes noncompliant.

**NEW QUESTION 35**

- (Topic 2)

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

Server1 stores update files locally in C:\Updates.

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

A. From the Update Services console, run the Windows Server Update Services Configuration Wizard.

B. From a command prompt, run wsusutil.exe and specify the movecontent parameter.

C. From the Update Services console, configure the Update Files and Languages option.

D. From a command prompt, run wsusutil.exe and specify the export parameter.

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 38**

- (Topic 2)

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

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

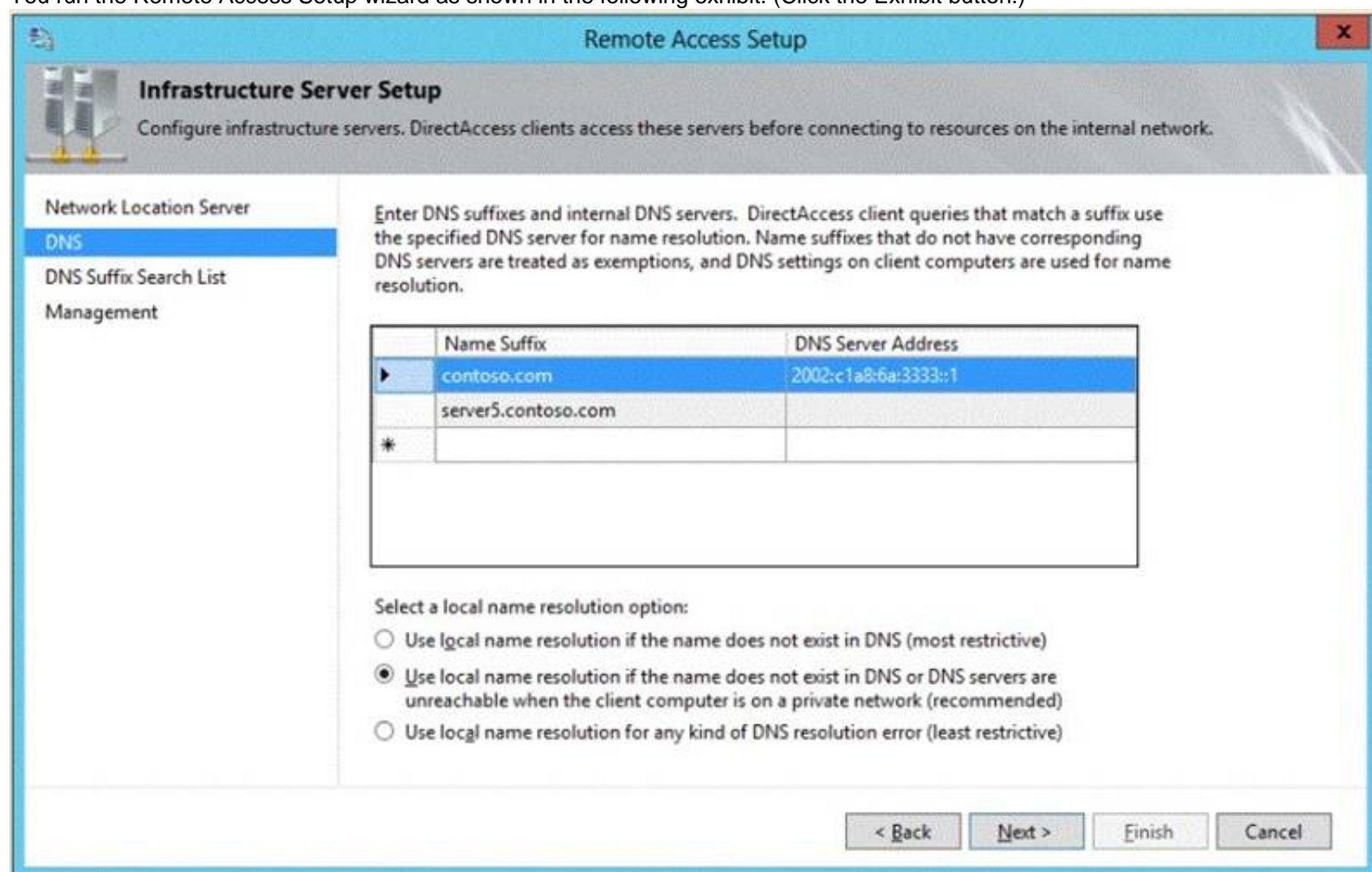
Internal DNS name: server1.contoso.com

External DNS name: da1.contoso.com

Internal IPv6 address: 2002:c1a8:6a:3333::1

External IPv4 address: 65.55.37.62

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



**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

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

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

A. A Name Suffix value of da1.contoso.com and a blank DNS Server Address value



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

**Answer:** A

**Explanation:**

Split-brain DNS is the use of the same DNS domain for both Internet and intranet resources. For example, the Contoso Corporation is using split brain DNS; contoso.com is the domain name for intranet resources and Internet resources. Internet users use http:

http://www.contoso.com to access Contoso's public Web site and Contoso employees on the Contoso intranet use http://www.contoso.com to access Contoso's intranet Web site. A Contoso employee with their laptop that is not a DirectAccess client on the intranet that accesses http://www.contoso.com sees the intranet Contoso Web site. When they take their laptop to the local coffee shop and access that same URL, they will see the public Contoso Web site.

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

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

References:

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

**NEW QUESTION 42**

DRAG DROP - (Topic 2)

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

You need to create an Active Directory snapshot on DC1. Which four commands should you run?

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

Commands	Answer Area
dsamain.exe	1
snapshot	
create	
ntdsutil.exe	
activate instance ntds	
wbadmin.exe	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: ntdsutil

Box 2: snapshot

Box 3: activate instance ntds Box 4: create

Note:

Create a snapshot of AD DS in Windows Server 2012 R2 by using NTDSUTIL

1 – On the domain server, open command prompt and type ntdsutil and press Enter. 2- Next, type snapshot and press Enter.

3 – Next, type activate instance ntds and press Enter.

4 – Next, type create (this create command is to generate a snapshot of my AD) and press Enter.

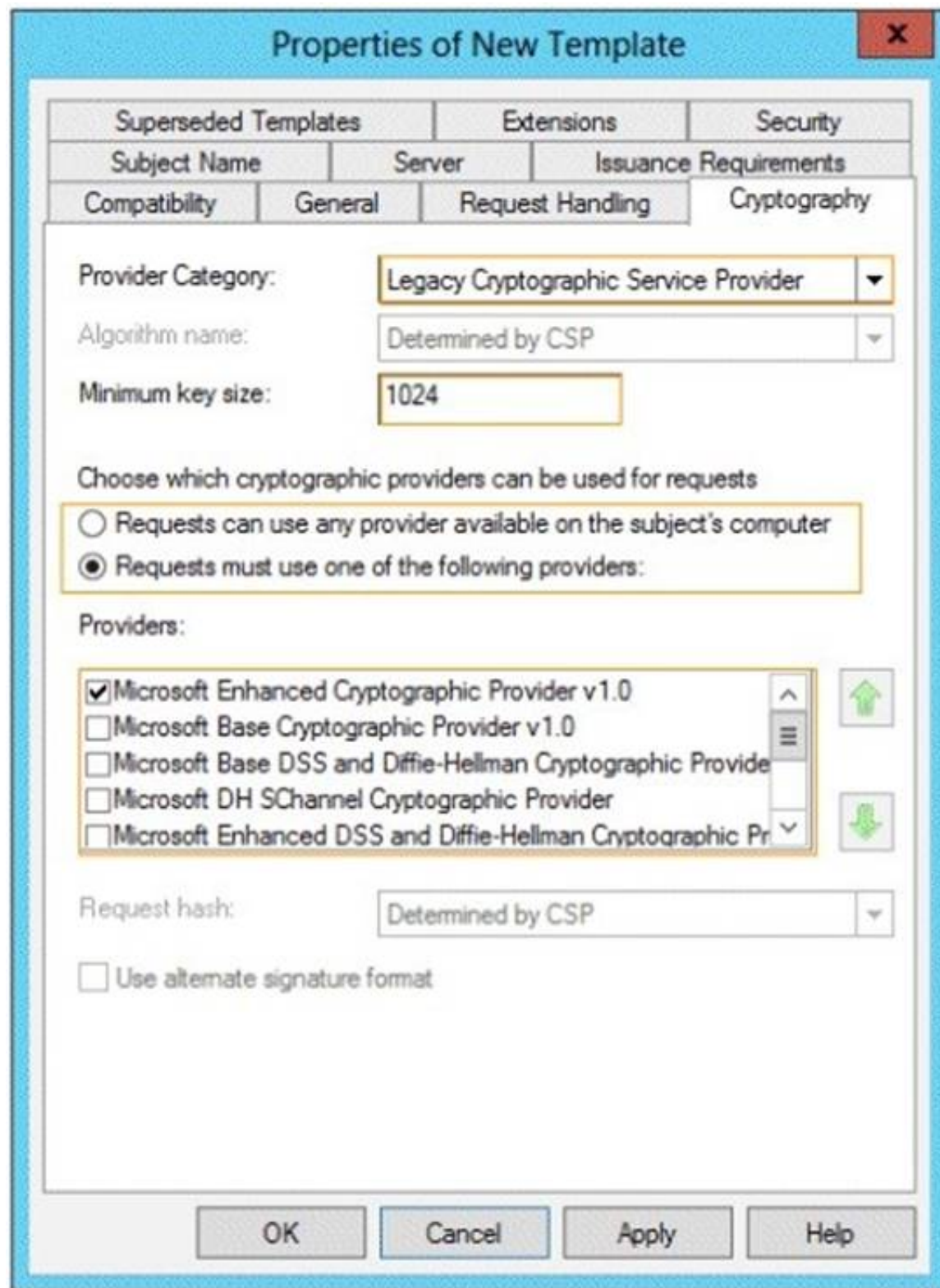
**NEW QUESTION 45**

HOTSPOT - (Topic 2)

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.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 50**

- (Topic 2)

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

**Answer:** BC

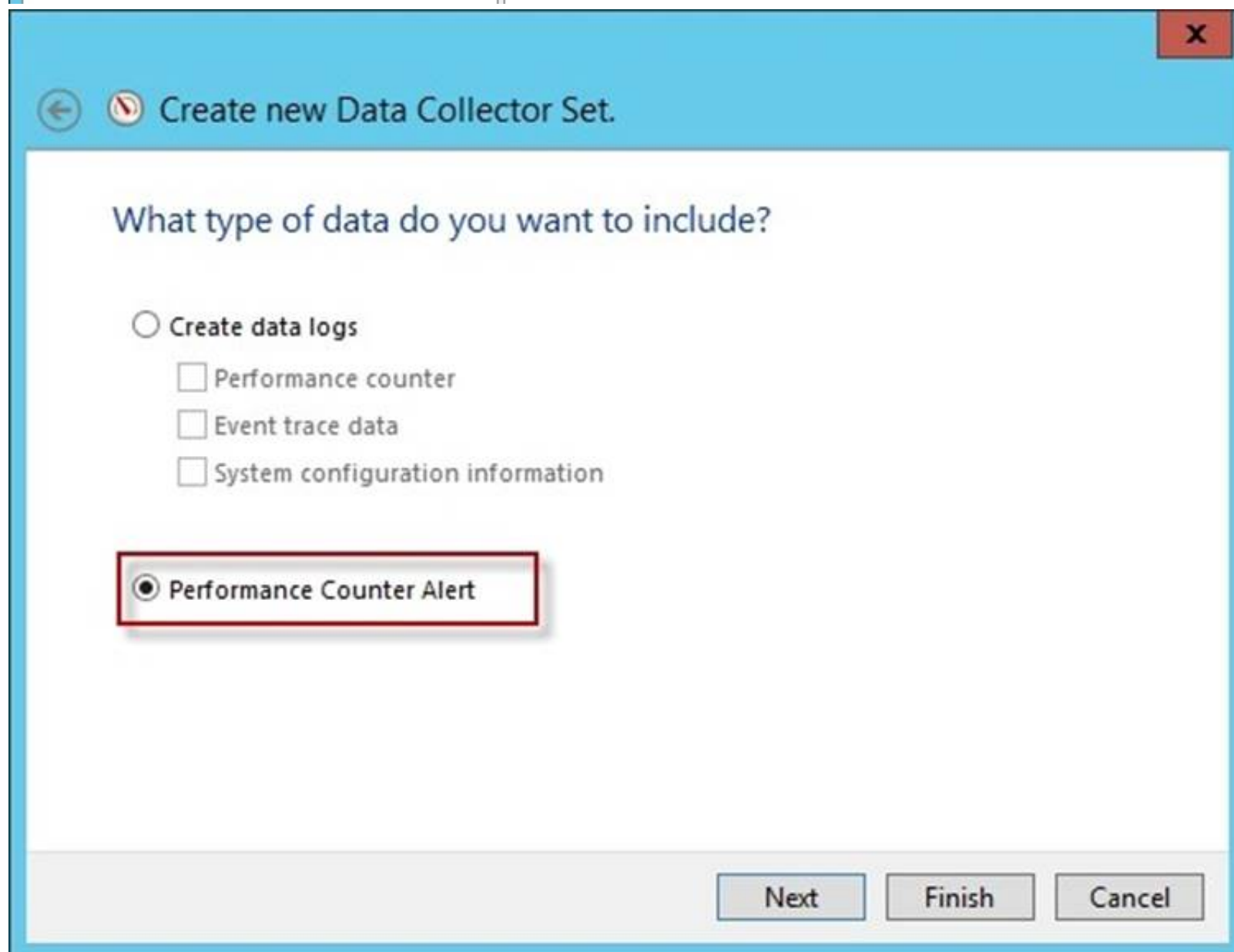
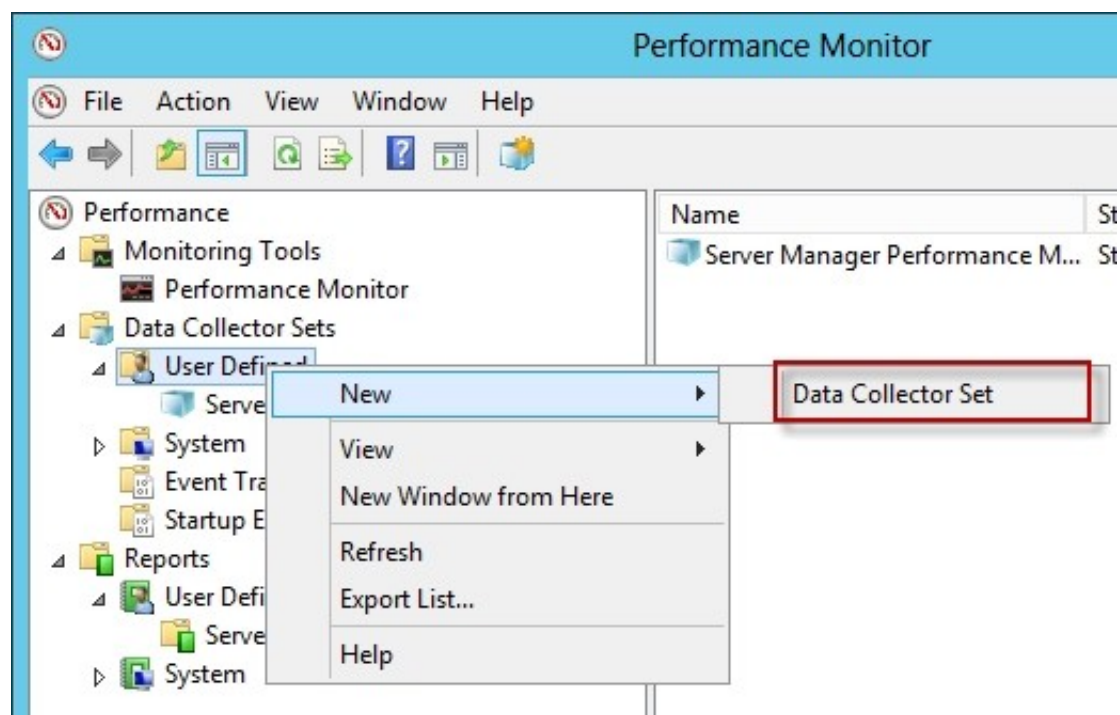
**Explanation:**

Automatically run a program when the amount of total free disk space on Server1 drops below 10 percent of capacity.

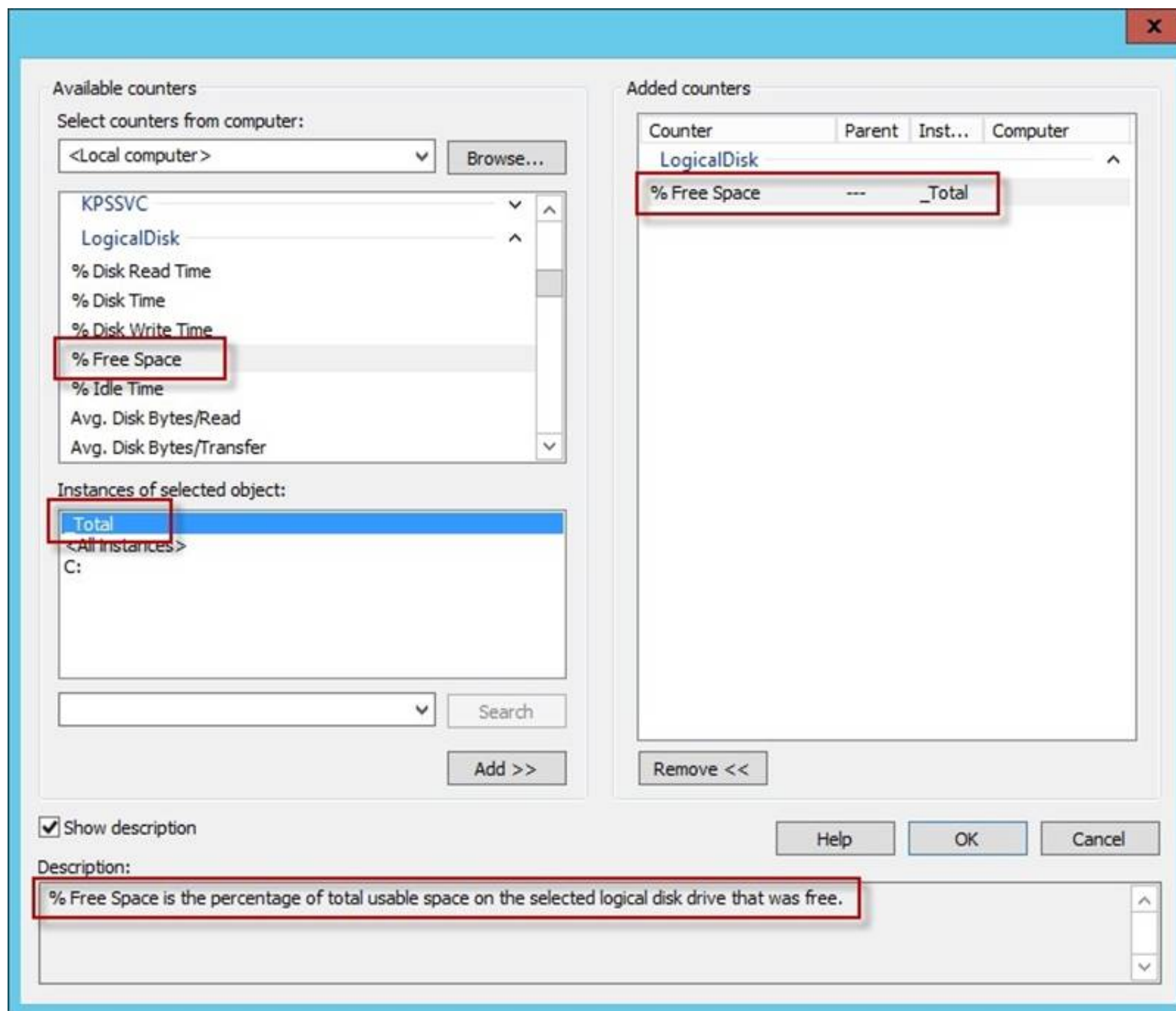
You can also configure alerts to start applications and performance logs Log the current values of several registry settings.

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

Total free disk space







Available counters

Select counters from computer:

<Local computer> Browse...

Available counters list:

- KPSSVC
- LogicalDisk
- % Disk Read Time
- % Disk Time
- % Disk Write Time
- % Free Space**
- % Idle Time
- Avg. Disk Bytes/Read
- Avg. Disk Bytes/Transfer

Instances of selected object:

**Total**

<All instances>

C:

Search

Add >>

Added counters

Counter	Parent	Inst...	Computer
LogicalDisk			
<b>% Free Space</b>	---	<b>_Total</b>	

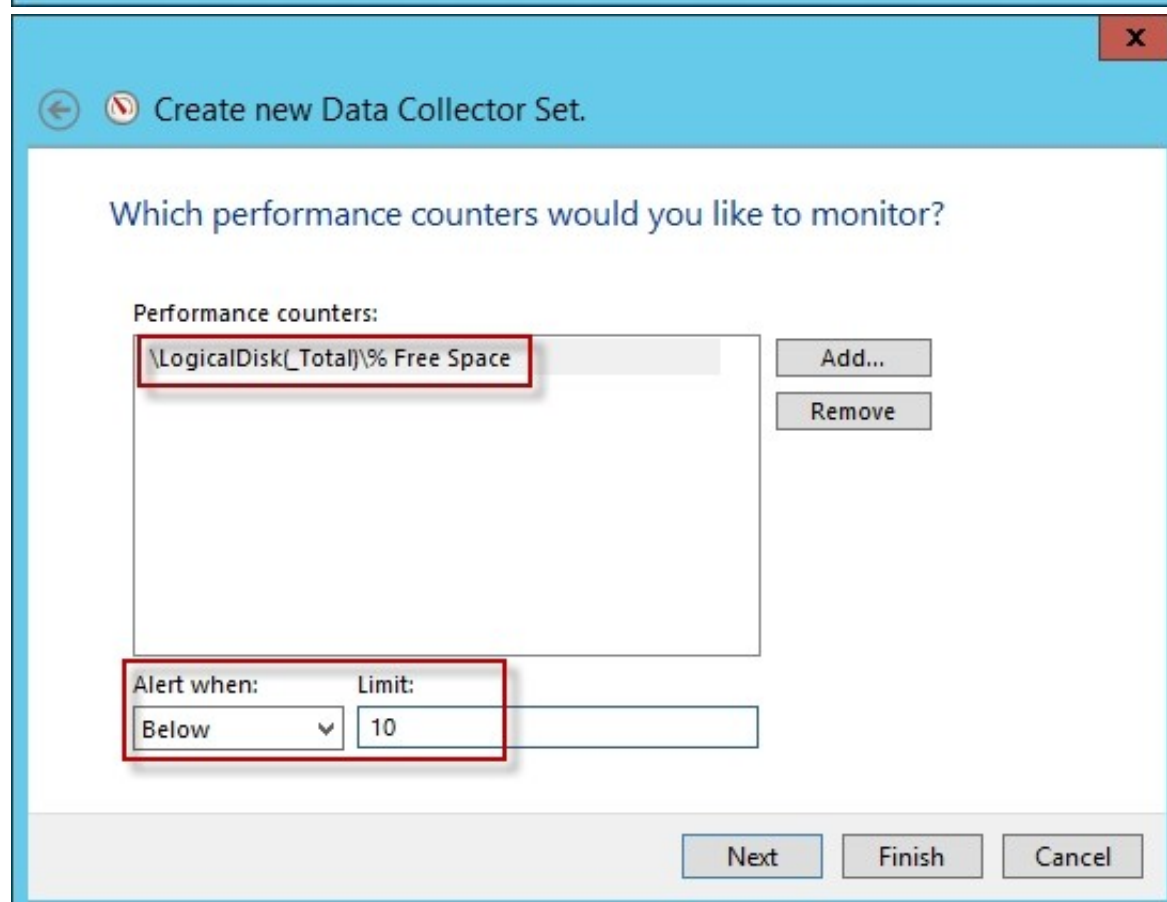
Remove <<

☒ Show description

Description:

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

Help OK Cancel



← Create new Data Collector Set.

Which performance counters would you like to monitor?

Performance counters:

**\LogicalDisk(\_Total)\% Free Space**

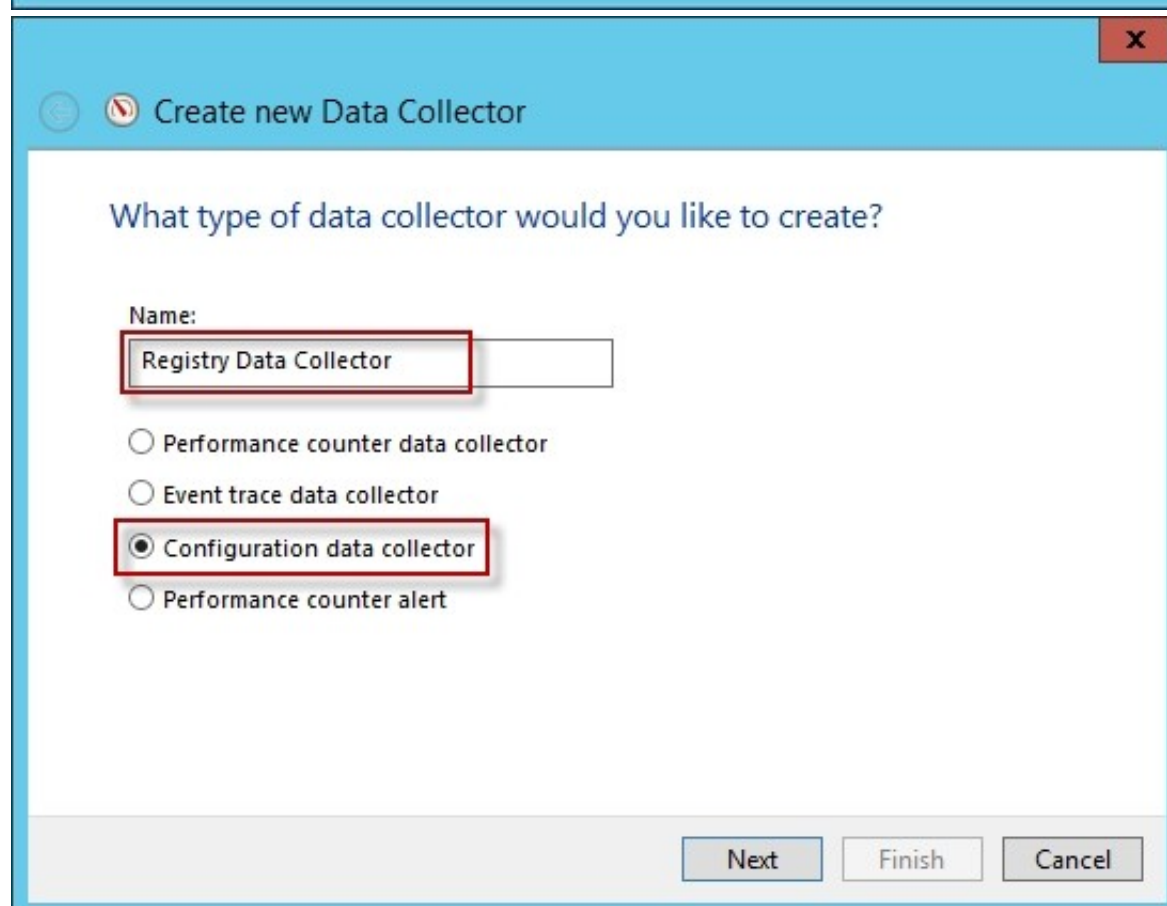
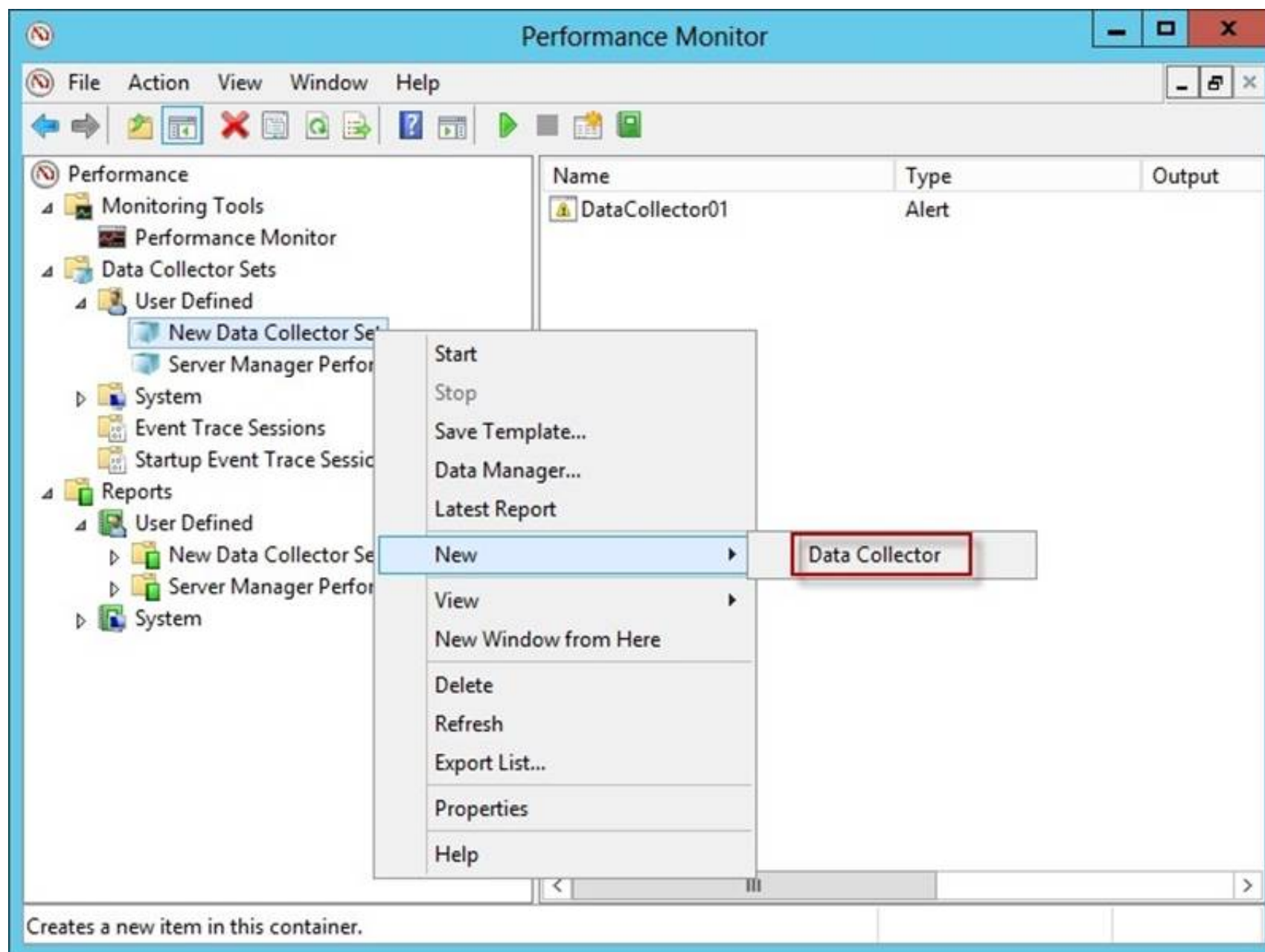
Add... Remove

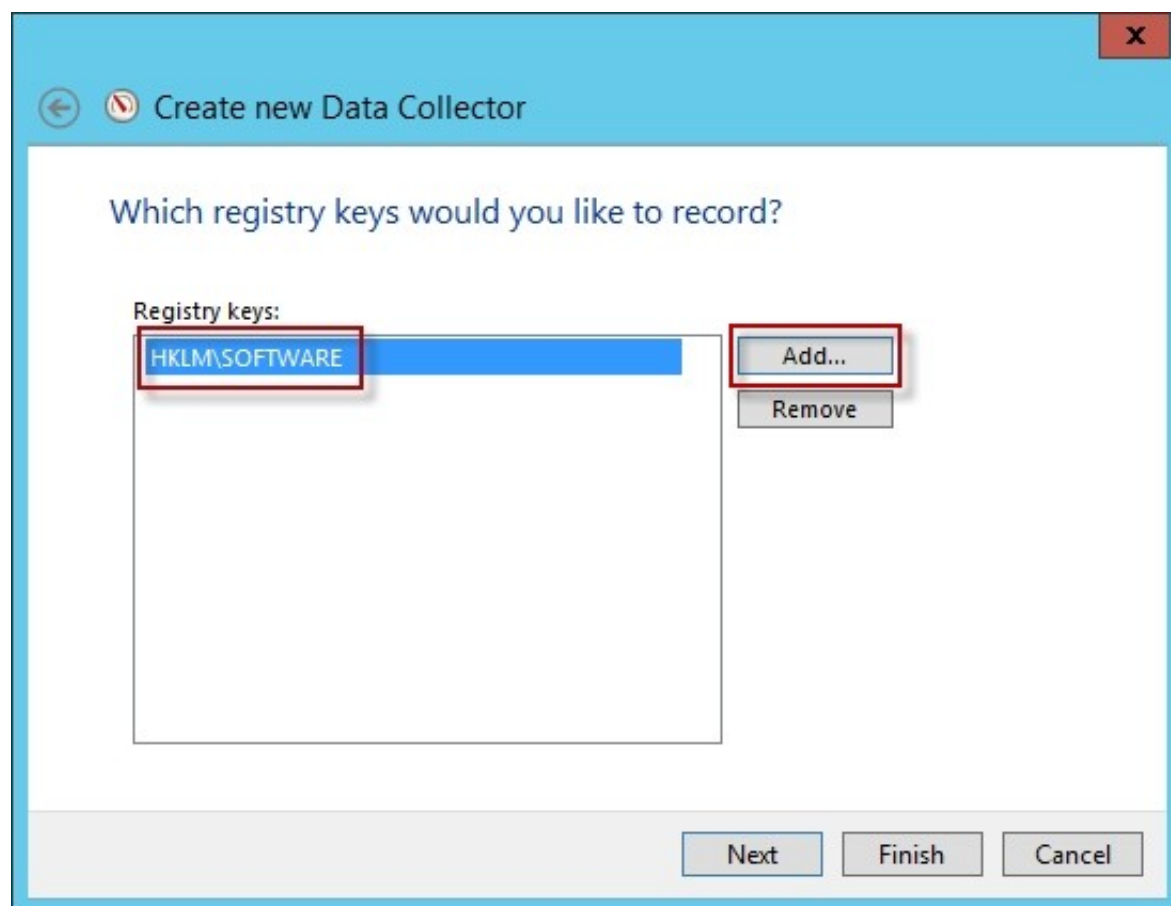
Alert when: Limit:

**Below** **10**

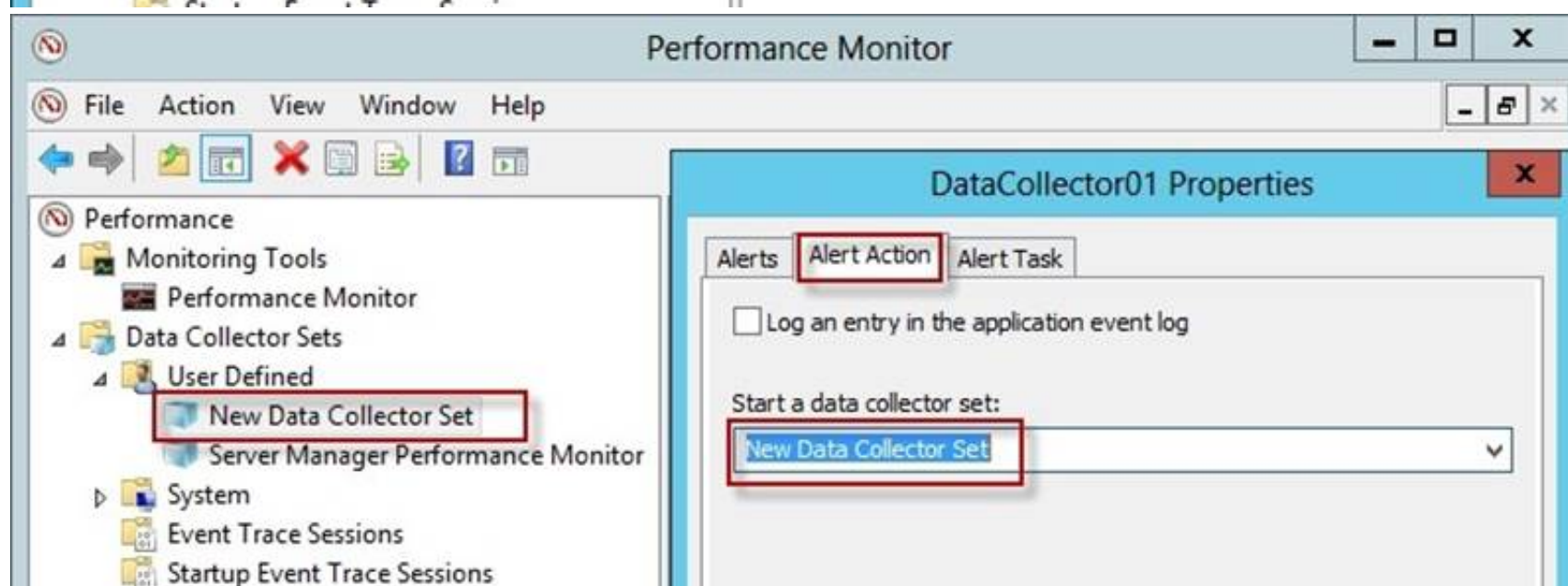
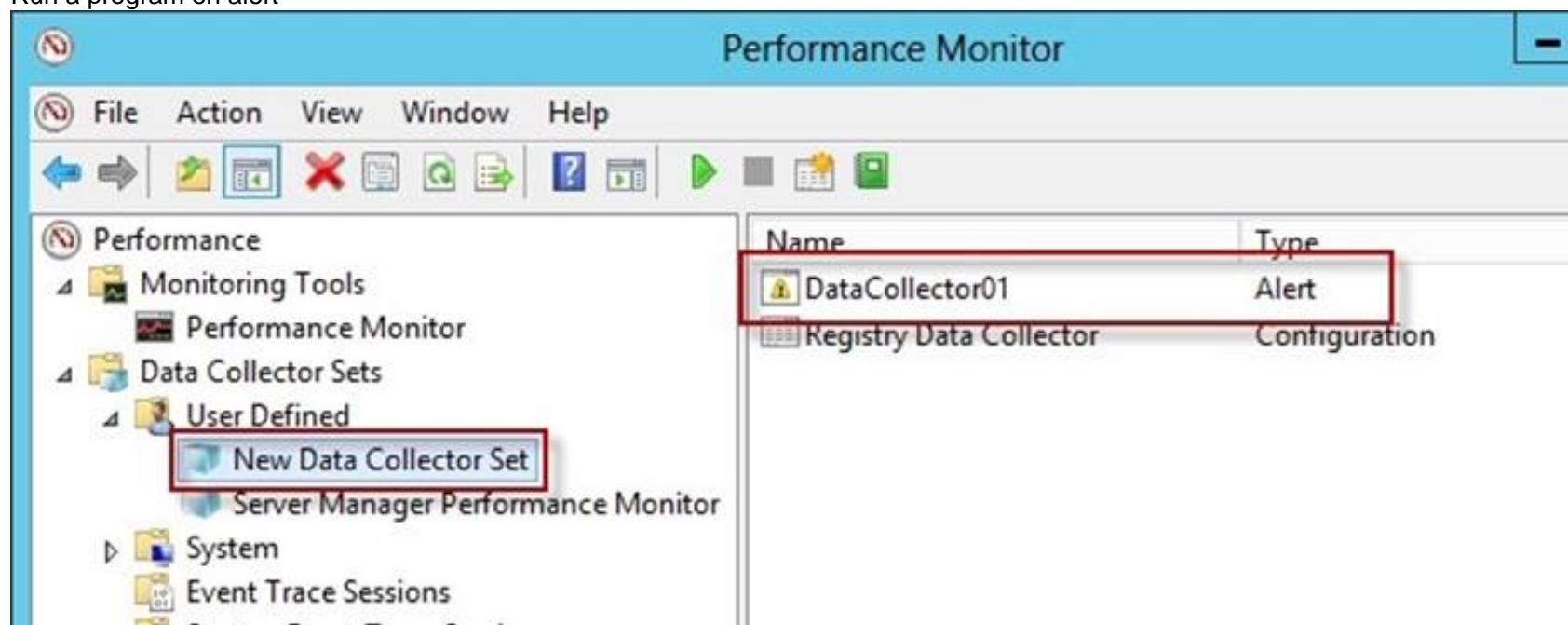
Next Finish Cancel

Registry settings

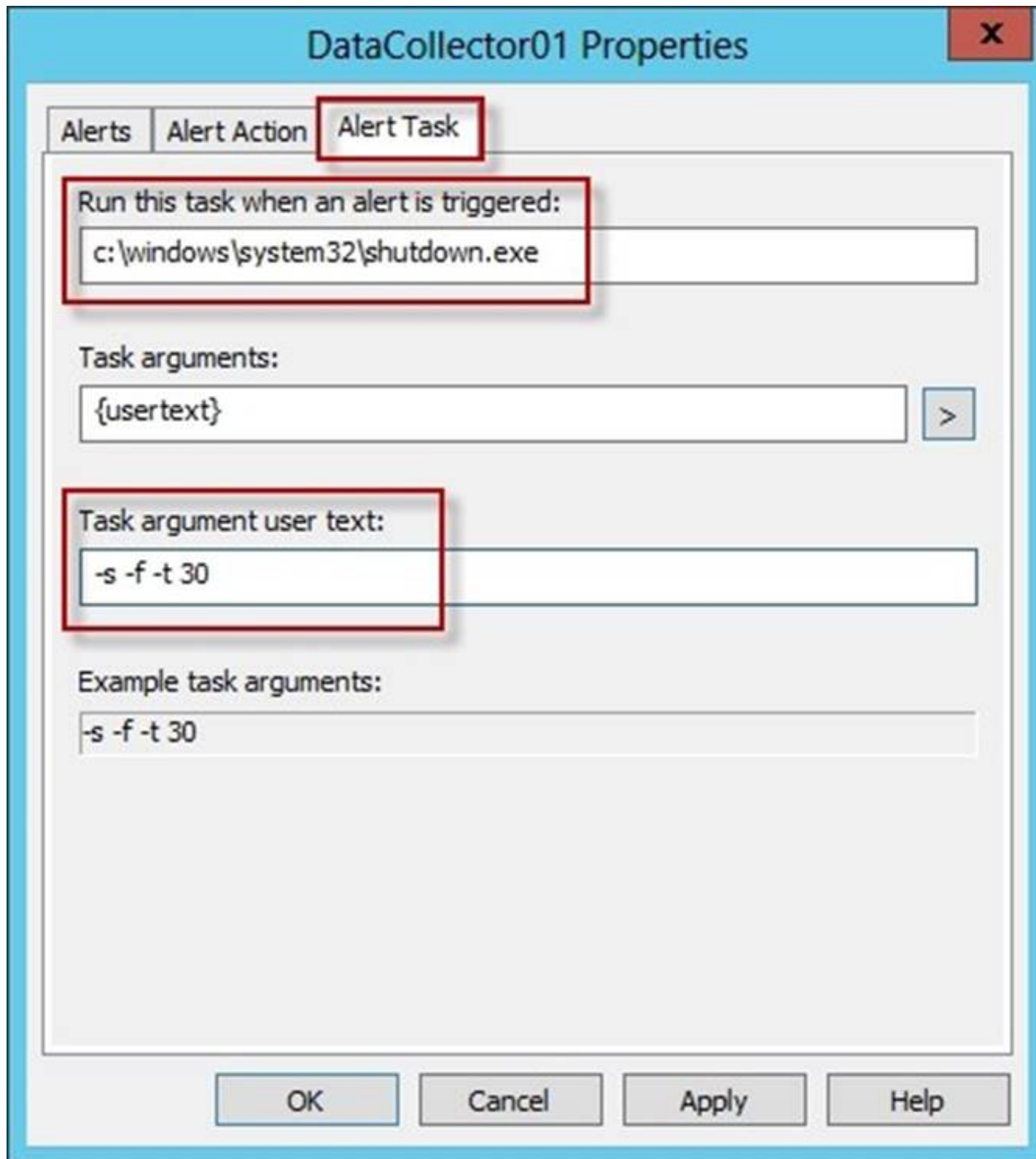




Run a program on alert







**DataCollector01 Properties**

Alerts | Alert Action | **Alert Task**

Run this task when an alert is triggered:

Task arguments:

Task argument user text:

Example task arguments:

OK Cancel Apply Help

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

#### NEW QUESTION 54

- (Topic 2)

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

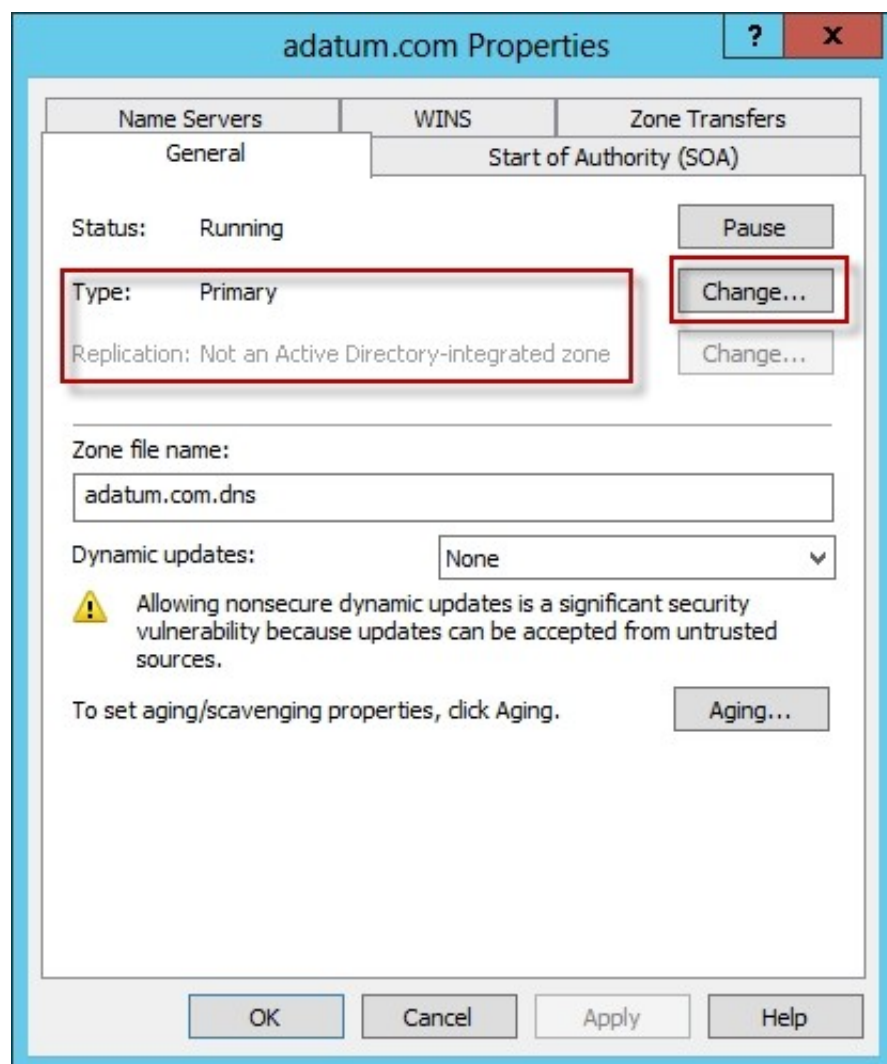
- A. Run the Zone Signing Wizard for the zone.
- B. From the properties of the zone, modify the start of authority (SOA) record.
- C. From the properties of the zone, change the zone type.
- D. Run the New Delegation Wizard for the zone.

**Answer: C**

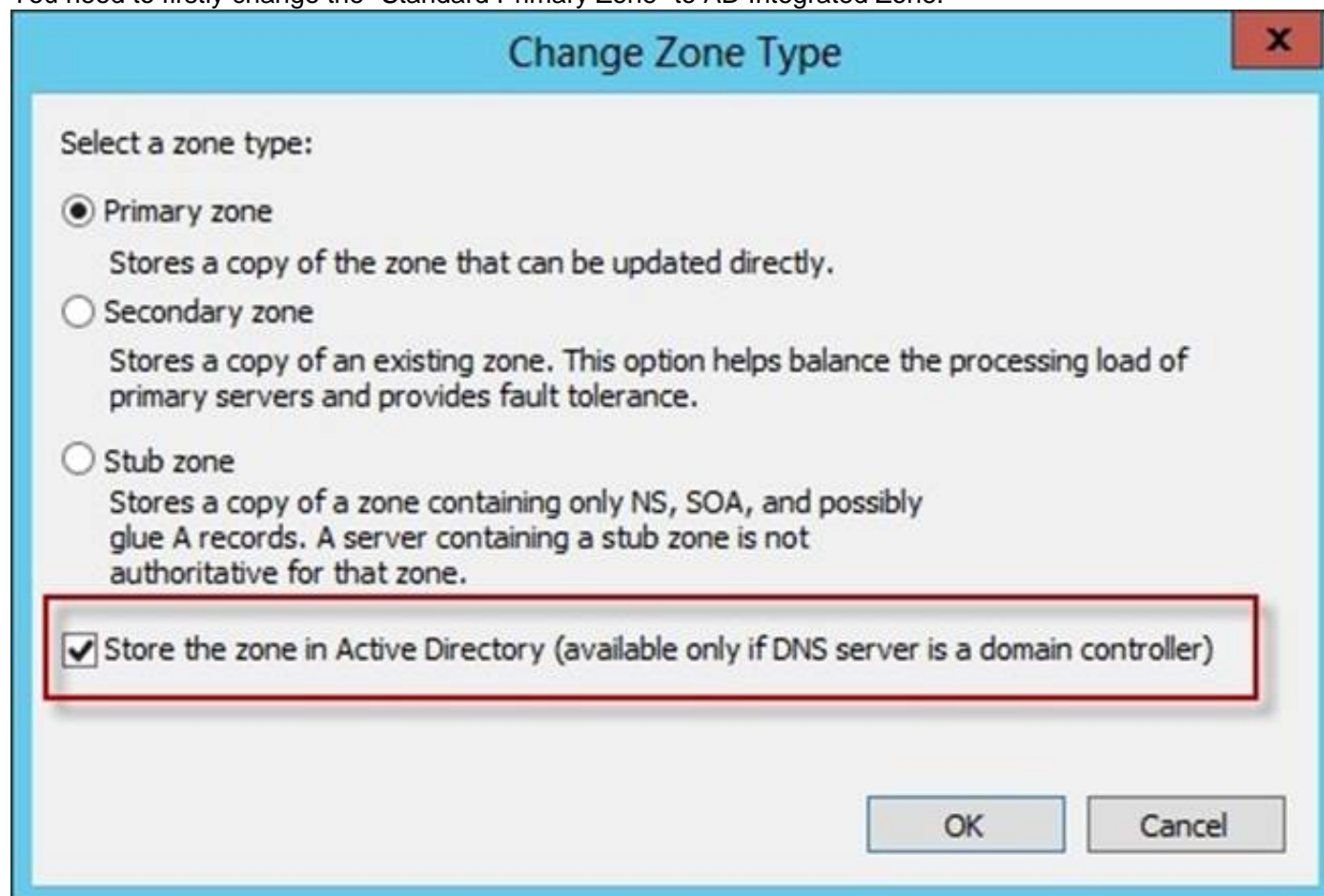
#### Explanation:

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

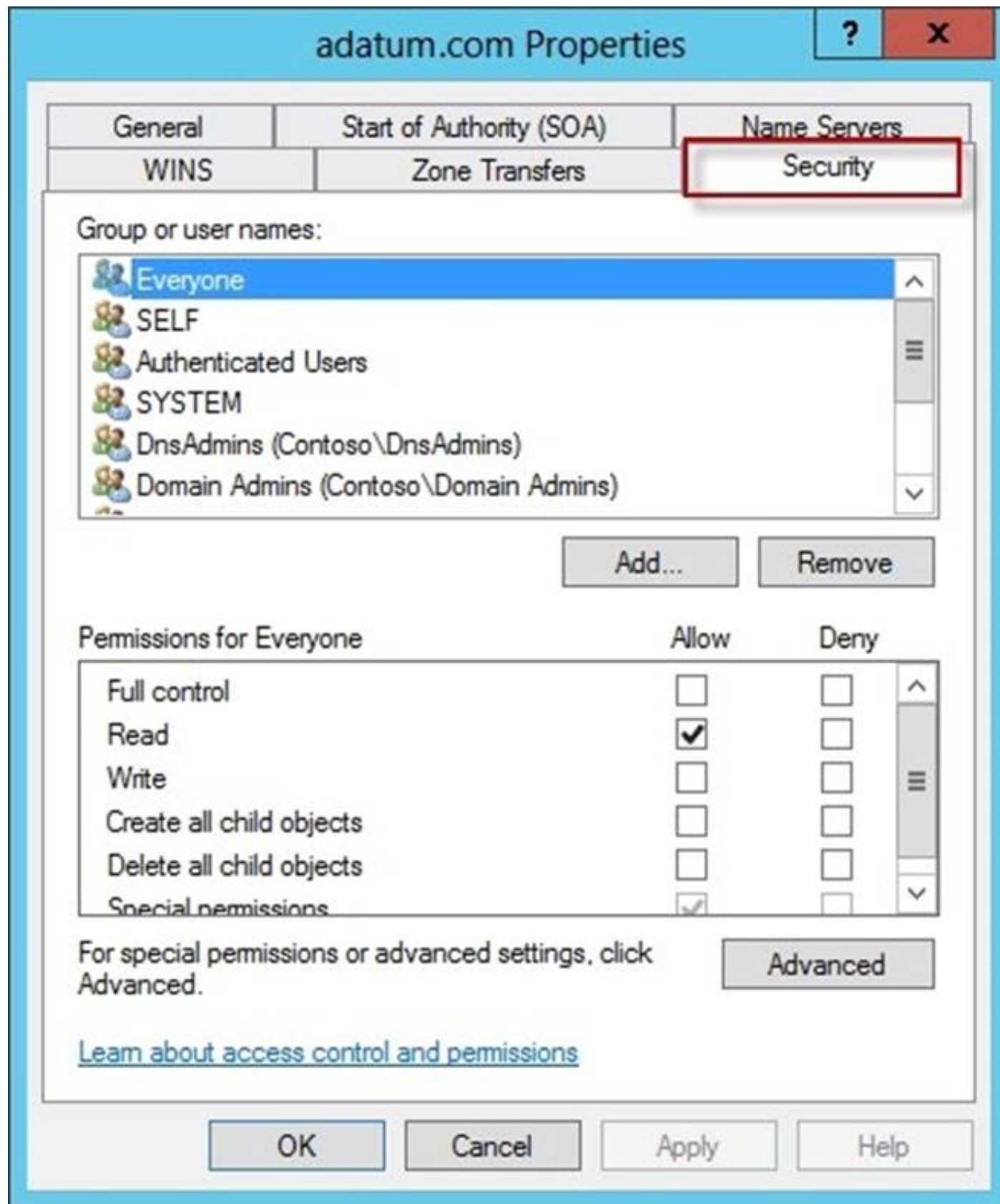
DNS update security is available only for zones that are integrated into Active Directory. After you integrate a zone, you can use the access control list (ACL) editing features that are available in the DNS snap-in to add or to remove users or groups from the ACL for a specific zone or for a resource record. Standard (not an Active Directory integrated zone) has no Security settings:



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



Now there's Security tab:



**adatum.com Properties**

General Start of Authority (SOA) Name Servers  
WINS Zone Transfers **Security**

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- DnsAdmins (Contoso\DnsAdmins)
- Domain Admins (Contoso\Domain Admins)

Add... Remove

Permissions for Everyone

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

[Learn about access control and permissions](#)

OK Cancel Apply Help

References:

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

#### NEW QUESTION 55

- (Topic 2)

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

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

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



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

Answer: A

Explanation:

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

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

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

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

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

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

NEW QUESTION 56

HOTSPOT - (Topic 2)

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

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

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

Answer Area

Answer Area

Add-BitLockerKeyProtector

Enable-BitLockerAutoUnlock

-MountPoint C:

-MountPoint D:

-AdAccountOrGroupProtector Contoso\Server

-Pin \$SecureString

-Service TpmAndPinAndStartupKeyProtecto

-TpmAndPinProtector

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Add-BitLockerKeyProtector

Enable-BitLockerAutoUnlock

-MountPoint C:

-MountPoint D:

-AdAccountOrGroupProtector Contoso\Server

-Pin \$SecureString

-Service TpmAndPinAndStartupKeyProtecto

-TpmAndPinProtector

#### NEW QUESTION 61

- (Topic 2)

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

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

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

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

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

**Answer:** A

#### Explanation:

Audit User Account Management

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

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

? A user account password is set or changed.

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

? The Directory Services Restore Mode password is set.

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

? Credential Manager credentials are backed up or restored.

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

#### NEW QUESTION 62

- (Topic 2)

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

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

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

You need to ensure that you can clone DC6. What should you do?

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

**Answer:** D

#### Explanation:

A deployed Windows Server 2012 domain controller (virtualized or physical) that hosts the PDC emulator role (DC1). To verify whether the PDC emulator role is hosted on a Windows Server 2012 domain controller, run the following Windows PowerShell command:

```
Get-ADComputer (Get-ADDomainController -Discover -Service "PrimaryDC").name
```

```
-Property operatingSystemVersion | fl
```

Reference: [http://technet.microsoft.com/en-us/library/hh831734.aspx#steps\\_deploy\\_vdc](http://technet.microsoft.com/en-us/library/hh831734.aspx#steps_deploy_vdc)

#### NEW QUESTION 66

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2003, Windows Server 2008 R2, or Windows Server 2012 R2.

A support technician accidentally deletes a user account named User1. You need to use tombstone reanimation to restore the User1 account. Which tool should you use?

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

**Answer: C**

**Explanation:**

Use Ldp.exe to restore a single, deleted Active Directory object

This feature takes advantage of the fact that Active Directory keeps deleted objects in the database for a period of time before physically removing them.

use Ldp.exe to restore a single, deleted Active Directory object

The LDP.exe tool, included with Windows Server 2012, allows users to perform operations against any LDAP-compatible directory, including Active Directory. LDP is used to view objects stored in Active Directory along with their metadata, such as security descriptors and replication metadata.

References:

<http://www.petri.co.il/manually-undeleting-objects-windows-active-directory-ad.htm>

<http://www.petri.co.il/manually-undeleting-objects-windows-active-directory-ad.htm>

<http://technet.microsoft.com/en-us/magazine/2007.09.tombstones.aspx>

[http://technet.microsoft.com/nl-nl/library/dd379509\(v=ws.10\).aspx#BKMK\\_2](http://technet.microsoft.com/nl-nl/library/dd379509(v=ws.10).aspx#BKMK_2)

<http://technet.microsoft.com/en-us/library/hh875546.aspx>

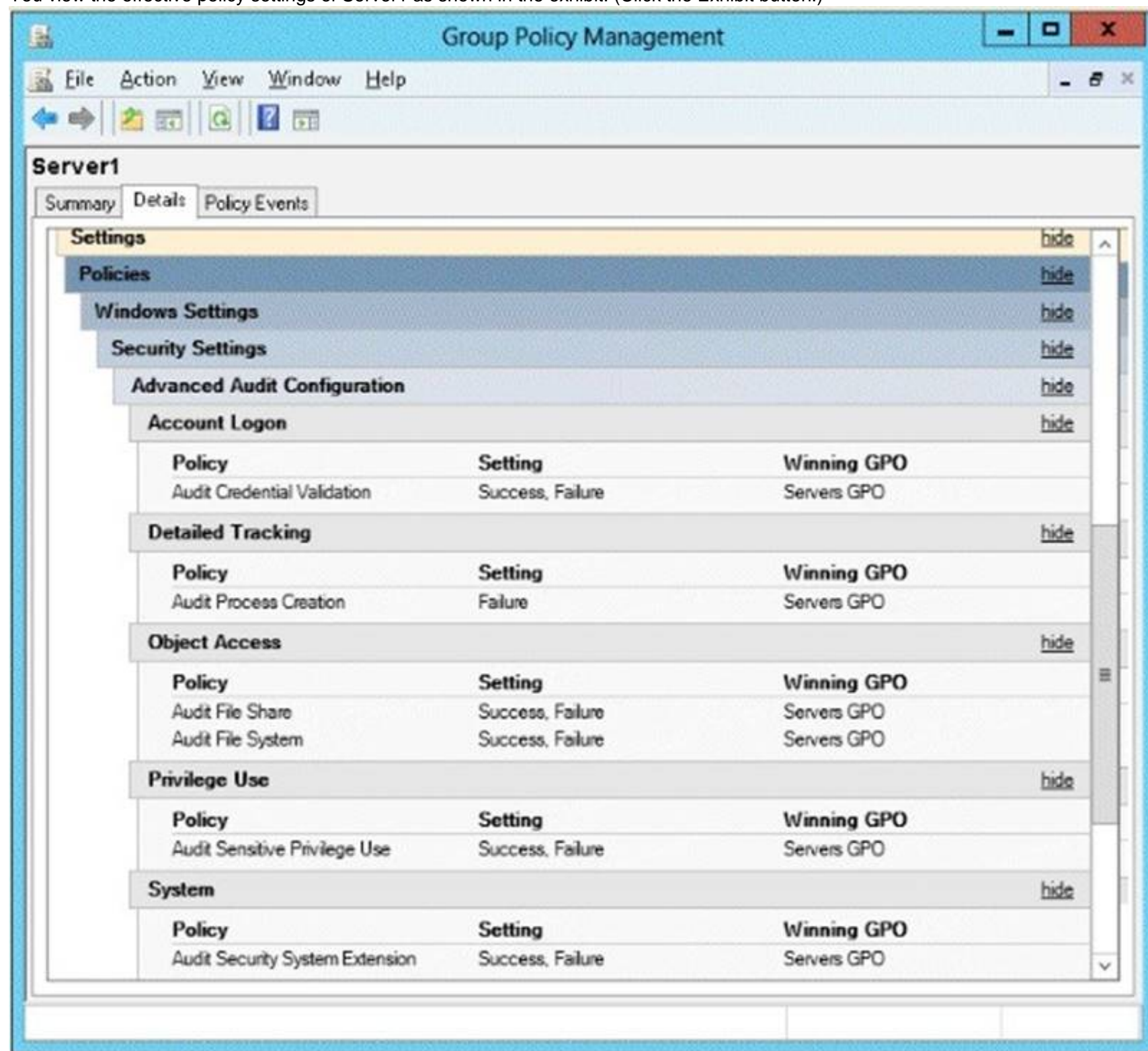
[http://technet.microsoft.com/en-us/library/dd560651\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd560651(v=ws.10).aspx)

**NEW QUESTION 67**

- (Topic 2)

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

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



Policy	Setting	Winning GPO
<b>Account Logon</b>		
Audit Credential Validation	Success, Failure	Servers GPO
<b>Detailed Tracking</b>		
Audit Process Creation	Failure	Servers GPO
<b>Object Access</b>		
Audit File Share	Success, Failure	Servers GPO
Audit File System	Success, Failure	Servers GPO
<b>Privilege Use</b>		
Audit Sensitive Privilege Use	Success, Failure	Servers GPO
<b>System</b>		
Audit Security System Extension	Success, Failure	Servers GPO

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

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

What should you configure?

- A. the Audit File Share setting of Servers GPO



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

**Answer: D**

**Explanation:**

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

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

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

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

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

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

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

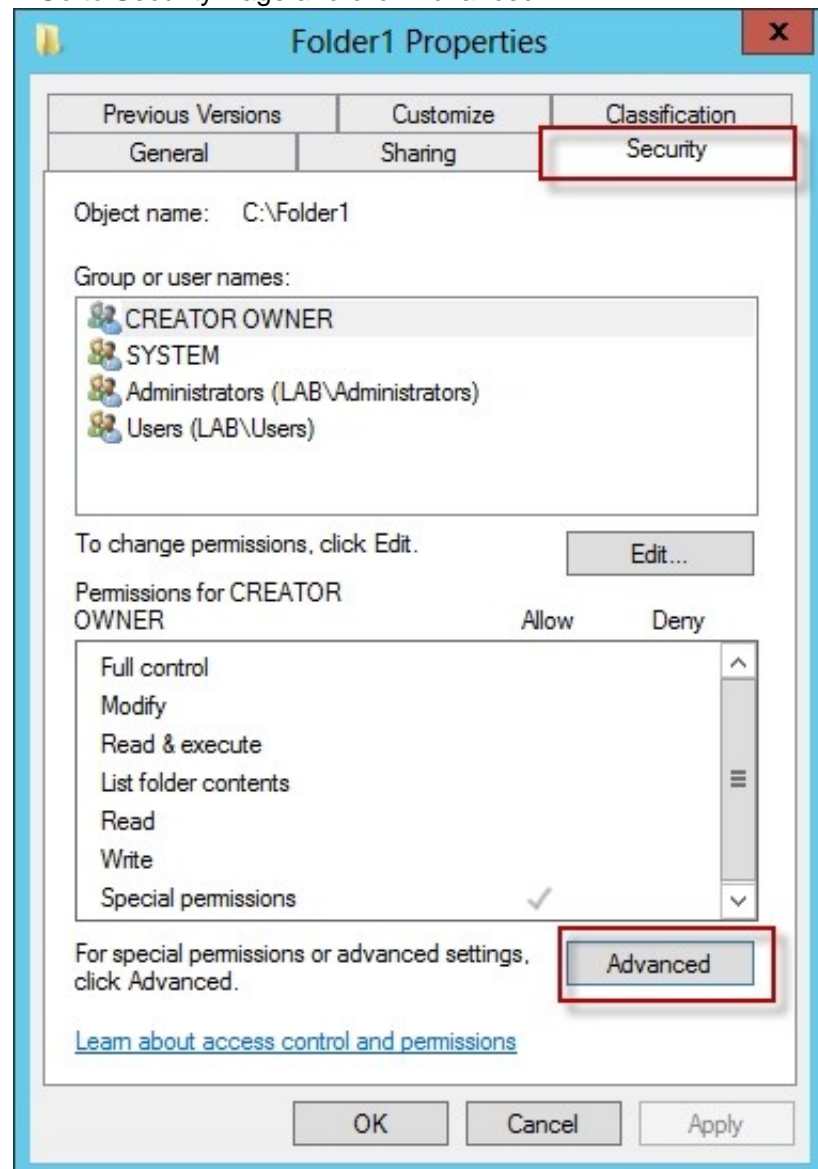
? Click start and run "secpol. msc" without quotes.

? Open the Local Policies\Audit Policy

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

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

? Go to Security Page and click Advanced.



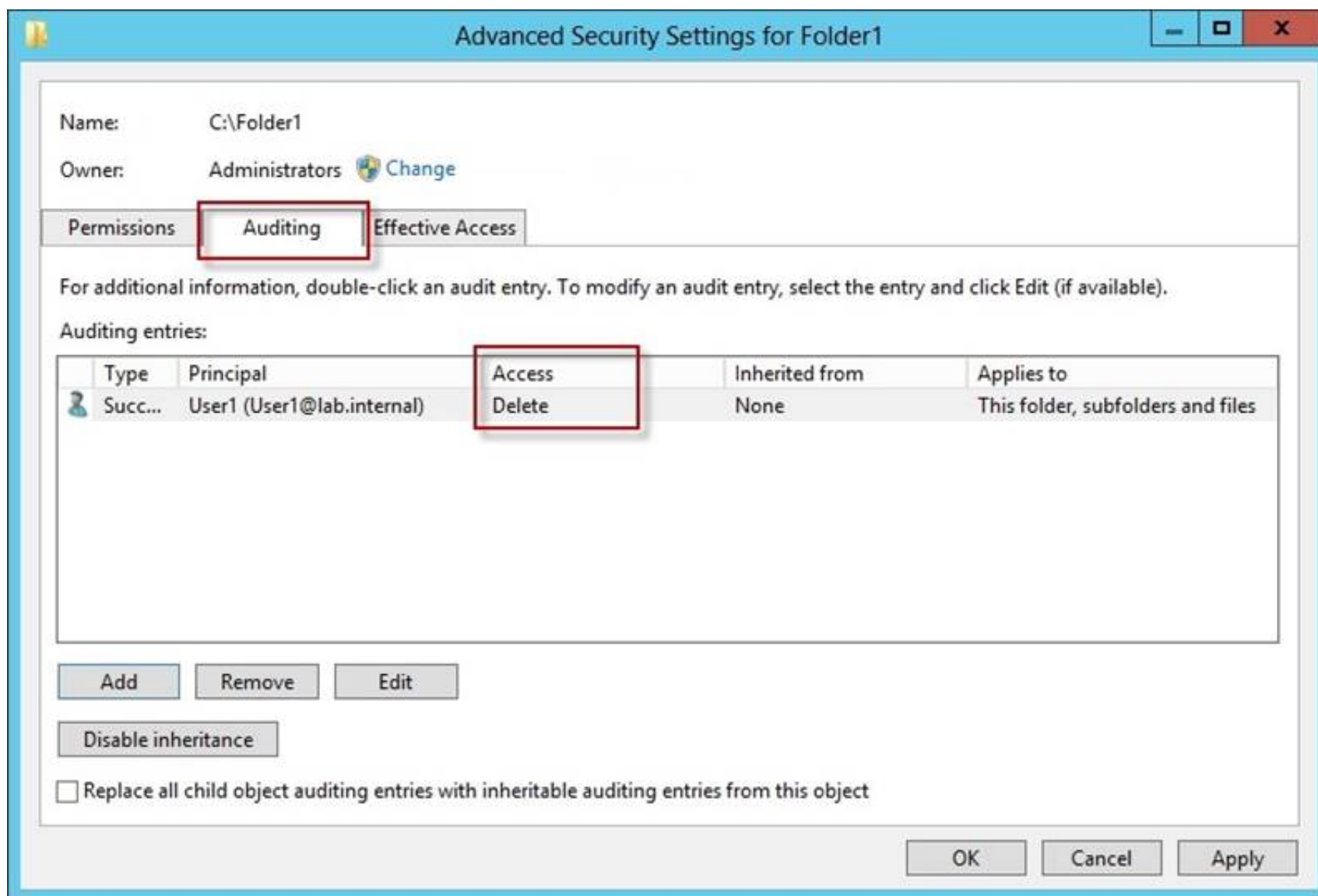
? Click Auditing and Edit.

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

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

? Tick on the box "Change permissions"

? Click OK.



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

References:

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

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

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

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

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

## NEW QUESTION 68

HOTSPOT - (Topic 2)

Your network contains a DNS server named Server1 that runs Windows Server 2012 R2. Server1 has a zone named contoso.com. The network contains a server named Server2 that runs Windows Server 2008 R2. Server1 and Server2 are members of an Active Directory domain named contoso.com.

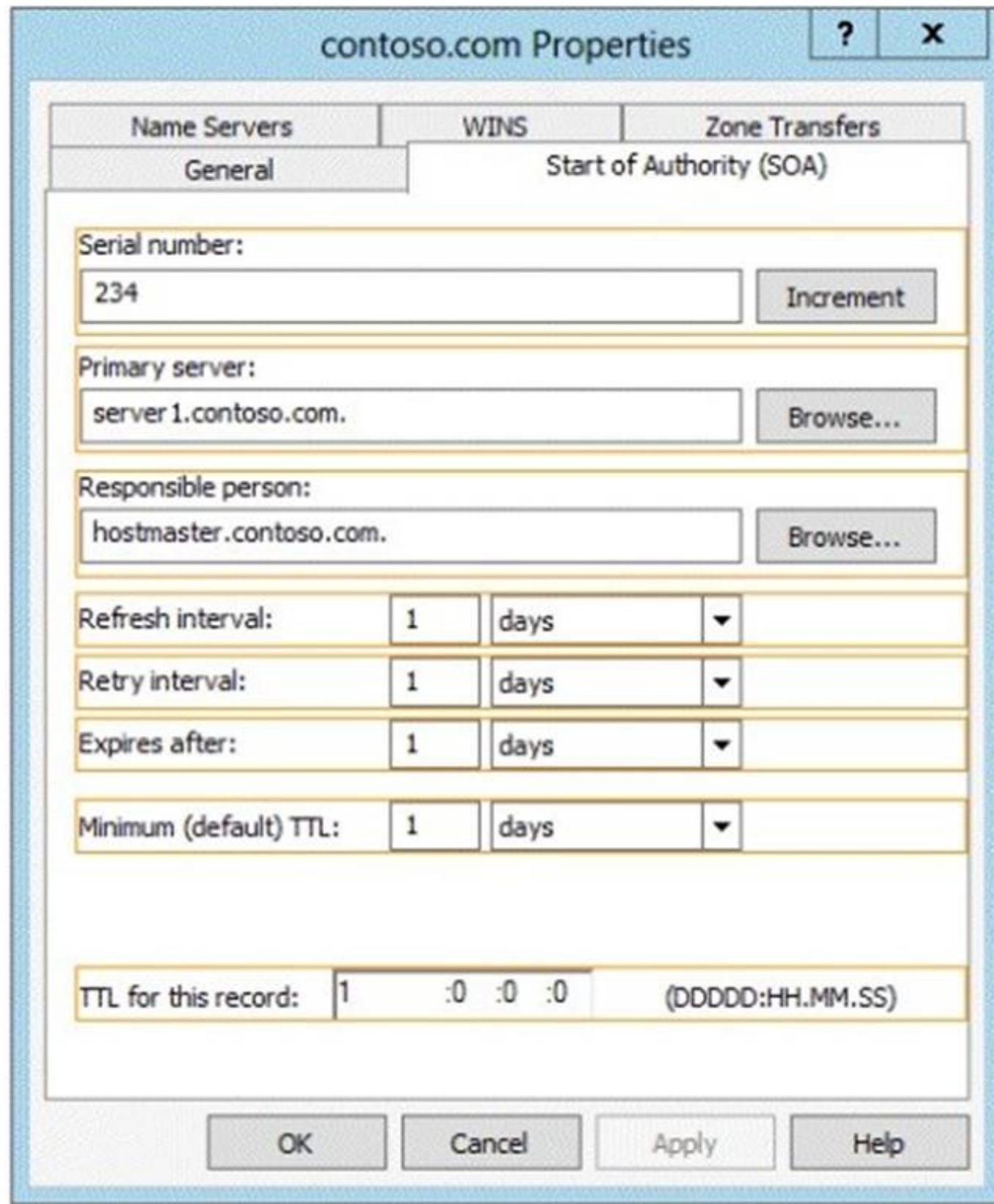
You change the IP address of Server2.

Several hours later, some users report that they cannot connect to Server2.

On the affected users' client computers, you flush the DNS client resolver cache, and the users successfully connect to Server2.

You need to reduce the amount of time that the client computers cache DNS records from contoso.com.

Which value should you modify in the Start of Authority (SOA) record? To answer, select the appropriate setting in the answer area.



The screenshot shows the 'contoso.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The 'Serial number' is 234, 'Primary server' is server 1.contoso.com., and 'Responsible person' is hostmaster.contoso.com. The refresh, retry, and expiration intervals are all set to 1 day. The minimum (default) TTL is 1 day, and the TTL for this record is 1 :0 :0 :0 (DDDD:HH.MM.SS).

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The Default TTL, is just that a default for newly created records. Once the records are created their TTL is independent of the Default TTL on the SOA. Microsoft DNS implementation copies the Default TTL setting to all newly created records their by giving them all independent TTL settings.

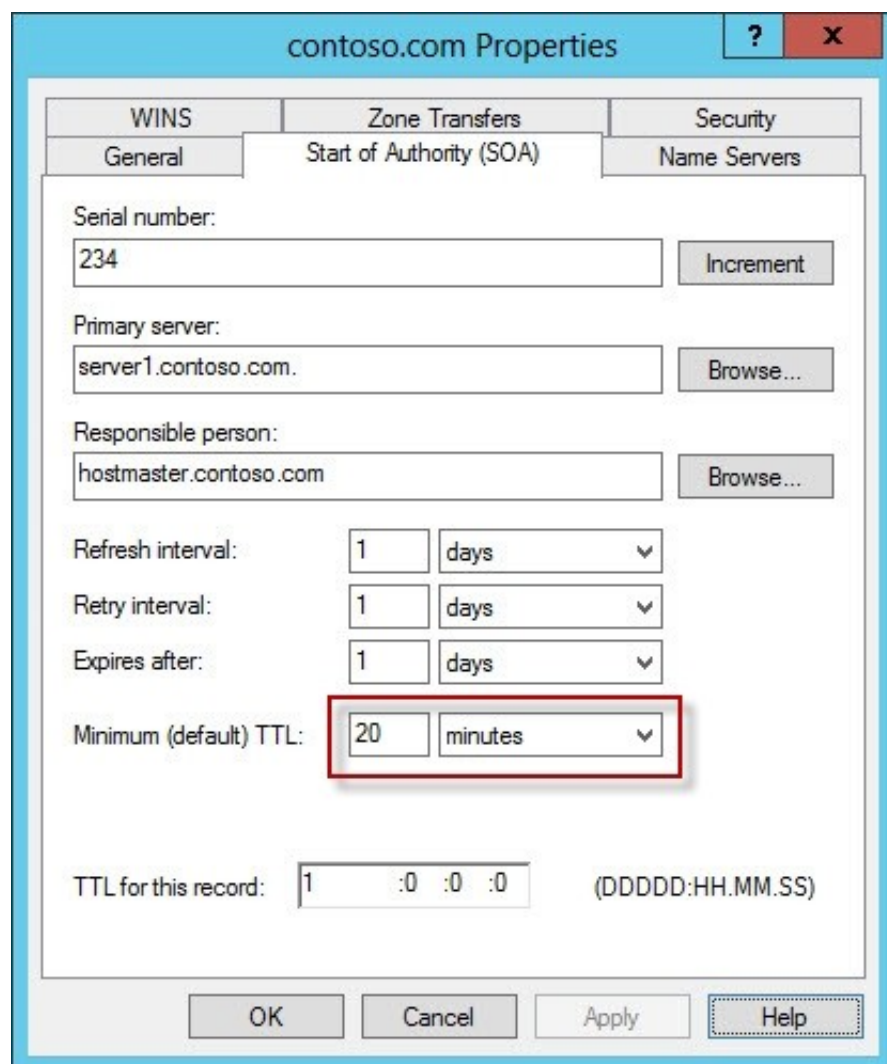
SOA Minimum Field: The SOA minimum field has been overloaded in the past to have three different meanings, the minimum TTL value of all RRs in a zone, the default TTL of RRs which did not contain a TTL value and the TTL of negative responses.

Despite being the original defined meaning, the first of these, the minimum TTL value of all RRs in a zone, has never in practice been used and is hereby deprecated. The second, the default TTL of RRs which contain no explicit TTL in the master zone file, is relevant only at the primary server. After a zone transfer all RRs have explicit TTLs and it is impossible to determine whether the TTL for a record was explicitly set or derived from the default after a zone transfer. Where a server does not require RRs to include the TTL value explicitly, it should provide a mechanism, not being the value of the MINIMUM field of the SOA record, from which the missing TTL values are obtained. How this is done is implementation dependent.

TTLs also occur in the Domain Name System (DNS), where they are set by an authoritative name server for a particular resource record. When a caching (recursive) nameserver queries the authoritative nameserver for a resource record, it will cache that record for the time (in seconds) specified by the TTL. If a stub resolver queries the caching nameserver for the same record before the TTL has expired, the caching server will simply reply with the already cached resource record rather than retrieve it from the authoritative nameserver again.

Shorter TTLs can cause heavier loads on an authoritative nameserver, but can be useful when changing the address of critical services like Web servers or MX records, and therefore are often lowered by the DNS administrator prior to a service being moved, in order to minimize disruptions.





contoso.com Properties

WINS Zone Transfers Security  
 General Start of Authority (SOA) Name Servers

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: 20 minutes

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

OK Cancel Apply Help

```
C:\Windows\system32>ipconfig /displaydns
```

Windows IP Configuration

dc1

```
Record Name . . . . . : dc1.home.local
Record Type . . . . . : 1
Time To Live . . . . . : 1196
Data Length . . . . . : 4
Section . . . . . : Answer
A <Host> Record . . . : 192.168.1.10
```

```
> set type=soa
```

```
> dc1
```

```
Server: dc1.home.local
Address: 192.168.1.10
```

home.local

```
primary name server = dc1.home.local
responsible mail addr = hostmaster.home.local
serial = 281
refresh = 900 (15 mins)
retry = 600 (10 mins)
expire = 300 (5 mins)
default TTL = 1200 (20 mins)
```

```
dc1.home.local internet address = 192.168.1.10
```

## NEW QUESTION 69

HOTSPOT - (Topic 2)

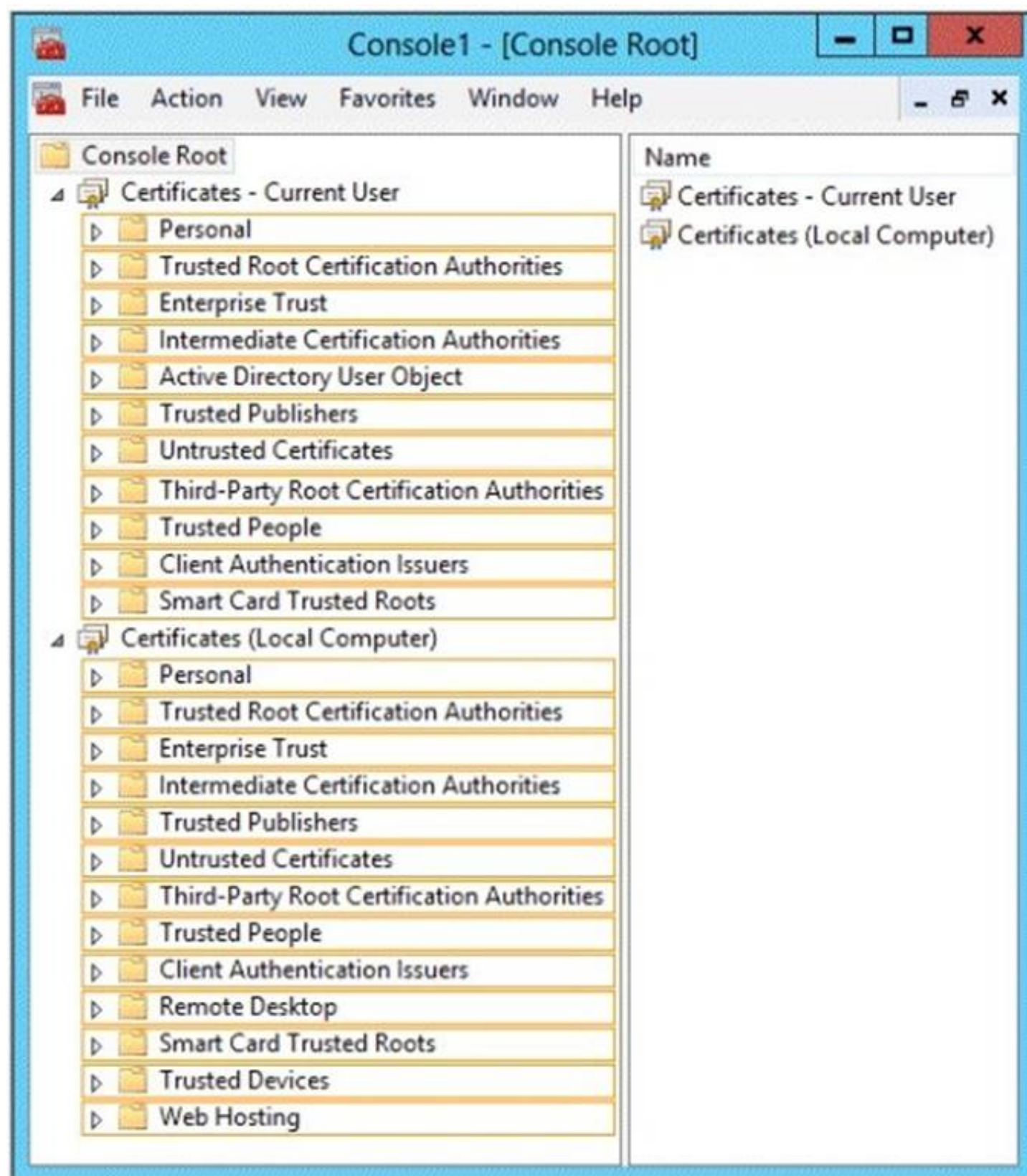
You have a server named Server1 that has the Network Policy and Access Services server role installed.

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.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

When organizations deploy their own public key infrastructure (PKI) and install a private trusted root CA, their 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 certificate store. After this occurs, the domain member computers trust certificates that are issued by the organization trusted root CA. For example, if you install AD CS, the CA sends its certificate to the domain member computers in your organization and they store the CA certificate in the Trusted Root Certification Authorities certificate store on the local computer. If you also configure and autoenroll a server certificate for your NPS servers and then deploy PEAP-MS-CHAP v2 for wireless connections, all domain member wireless client computers can successfully authenticate your NPS servers using the NPS server certificate because they trust the CA that issued the NPS server certificate. 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 that 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.

**References:**

<http://technet.microsoft.com/en-us/library/cc730811.aspx> <http://technet.microsoft.com/en-us/library/cc730811.aspx>  
<http://technet.microsoft.com/en-us/library/cc772401%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/ee407543%28v=ws.10%29.aspx>

**NEW QUESTION 74**

HOTSPOT - (Topic 2)

You have a server named LON-SVR1 that runs Windows Server 2012 R2. LON-SVR1 has the Remote Access server role installed. LON-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.)



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

Your company purchases an additional router named Router1. Router1 has an interface that connects to the perimeter network and an interface that connects to the Internet. The IP address of the interface that connects to the perimeter network is 172.16.0.2.

You need to ensure that LON-SVR1 will route traffic to the Internet by using Router1 if the current default gateway is unavailable.

How should you configure the static route on LON-SVR1? To answer, select the appropriate static route in the answer area.

IPv4 Static Route

Interface: Local Area Connection
Destination: 0 . 0 . 0 . 0
Network mask: 0 . 0 . 0 . 0
Gateway: 172 . 16 . 0 . 2
Metric: 300
☒ Use this route to initiate demand-dial connections
[For more information](#)

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Metric: Specifies an integer cost metric (ranging from 1 to 9999) for the route, which is used when choosing among multiple routes in the routing table that most closely match the destination address of a packet being forwarded. The route with the lowest metric is chosen. The metric can reflect the number of hops, the speed of the path, path reliability, path throughput, or administrative properties.

A metric is a value that is assigned to an IP route for a particular network interface that identifies the cost that is associated with using that route.

The metric that is assigned to specific default gateways can be configured independently for each gateway. This setup enables a further level of control over the metric that is used for the local routes.

#### NEW QUESTION 78

- (Topic 2)

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



are configured as shown in the following table.

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

All client computers run Windows 8 Enterprise.

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

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

You need to ensure that the client computers can discover HRA servers automatically. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

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

**Answer:** ABE

**Explanation:**

Requirements for HRA automatic discovery

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

Client computers must be running Windows Vista® with Service Pack 1 (SP1) or Windows XP with Service Pack 3 (SP3).

The HRA server must be configured with a Secure Sockets Layer (SSL) certificate. The EnableDiscovery registry key must be configured on NAP client computers. DNS SRV records must be configured.

The trusted server group configuration in either local policy or Group Policy must be cleared.

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

**NEW QUESTION 81**

- (Topic 2)

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.

**Answer:** B

**Explanation:**

PSOs cannot be applied to organizational units (OUs) directly. If your users are organized into OUs, consider creating global security groups that contain the users from these OUs and then applying the newly defined finegrained password and account lockout policies to them. If you move a user from one OU to another, you must update user memberships in

the corresponding global security groups.

Go ahead and hit "OK" and then close out of all open windows. Now that you have created a password policy, we need to apply it to a user/group. In order to do so, you must have "write" permissions on the PSO object. We're doing this in a lab, so I'm Domain Admin. Write permissions are not a problem

1. Open Active Directory Users and Computers (Start, point to Administrative Tools, and then click Active Directory Users and Computers).
2. On the View menu, ensure that Advanced Features is checked.
3. In the console tree, expand Active Directory Users and Computers\yourdomain\System\Password Settings Container
4. In the details pane, right-click the PSO, and then click Properties.
5. Click the Attribute Editor tab.
6. Select the msDS-PsoAppliesTo attribute, and then click Edit.

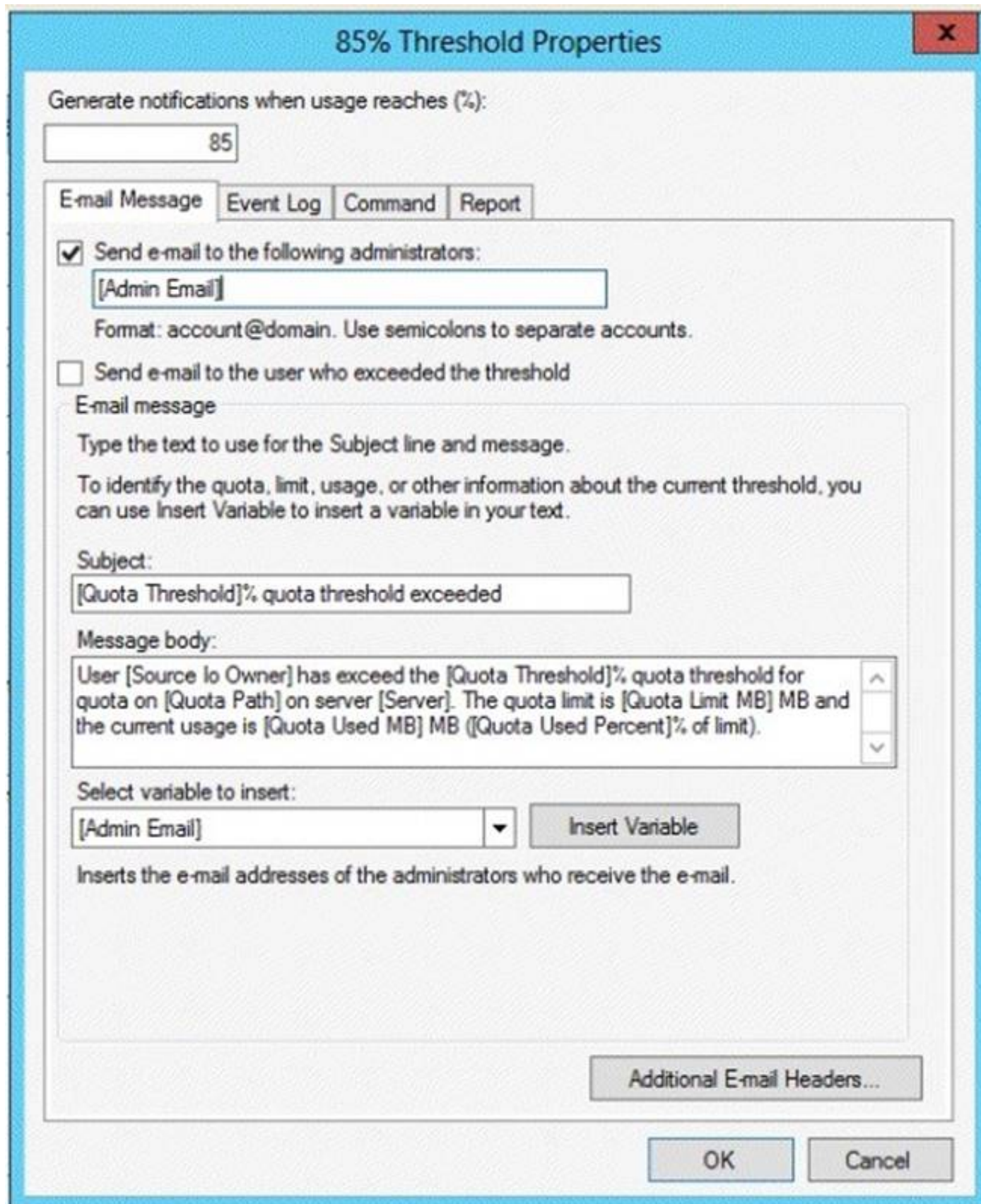
**NEW QUESTION 83**

- (Topic 2)

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

Server1 has the File Server Resource Manager role service installed.

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



**85% Threshold Properties**

Generate notifications when usage reaches (%):

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

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

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

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

**Subject:**

**Message body:**

**Select variable to insert:**  
   
 Inserts the e-mail addresses of the administrators who receive the e-mail.

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

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

**Answer: D**

**Explanation:**

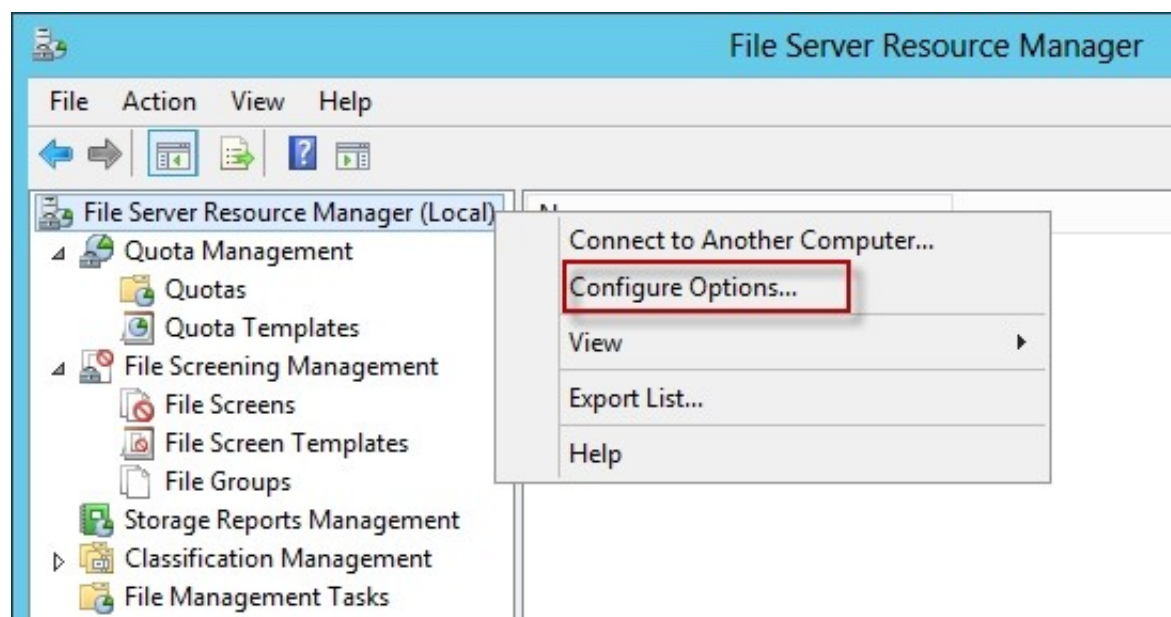
When you create quotas and file screens, you have the option of sending e-mail notifications to users when their quota limit is approaching or after they have attempted to save files that have been blocked. If you want to routinely notify certain administrators of quota and file screening events, you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

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

To configure e-mail options

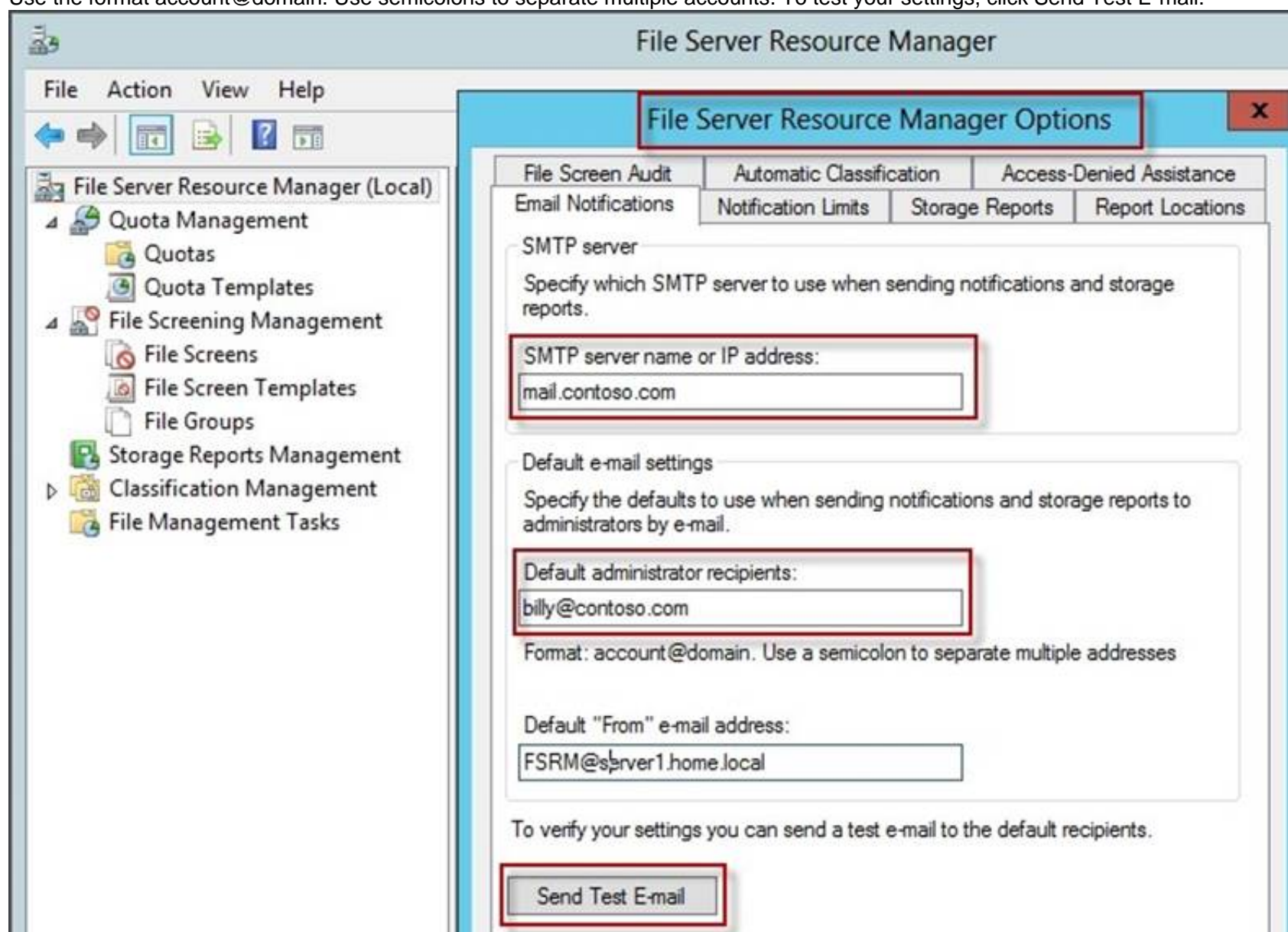
In the console tree, right-click File Server Resource Manager, and then click Configure options. The File Server Resource Manager Options dialog box opens.



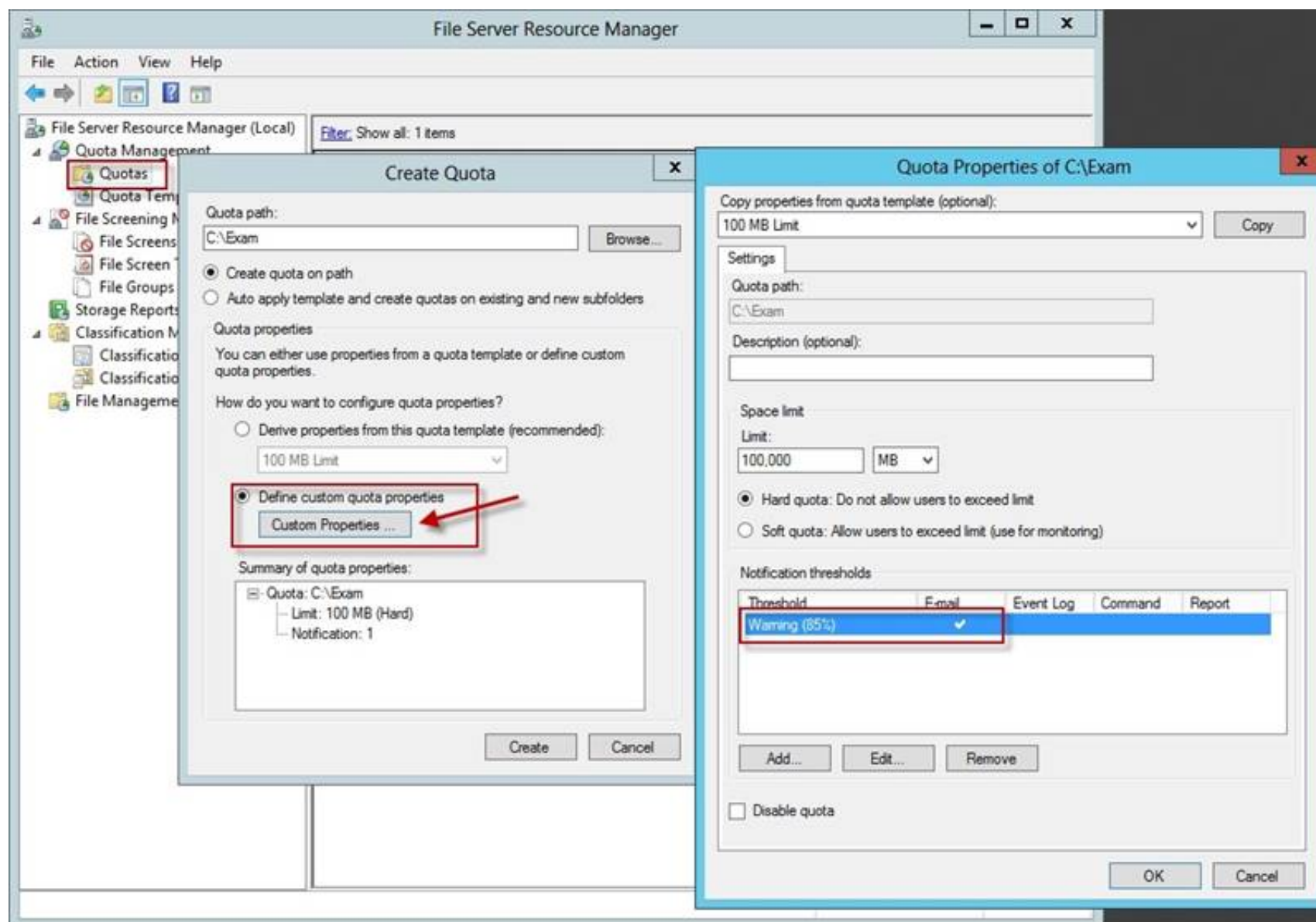


On the E-mail Notifications tab, under SMTP server name or IP address, type the host name or the IP address of the SMTP server that will forward e-mail notifications.

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







#### NEW QUESTION 85

- (Topic 3)

Your network contains one Active Directory domain. The domain contains a DirectAccess deployment.

You need to ensure that when the DirectAccess connection is active, the connection appears as "Contoso Internal Network -Authorized Users Only" on the DirectAccess clients.

What should you configure in the DirectAccess client Group Policy object (GPO)?

- A. Friendly Name
- B. Corporate Resources
- C. User Interface
- D. Prefer Local Names Allowed

**Answer: A**

#### NEW QUESTION 86

- (Topic 3)

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

You need to ensure that you can view update reports and computer reports on Server01.

Which two components should you install? Each correct answer presents part of the solution.

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

**Answer: BD**

#### NEW QUESTION 88

- (Topic 3)

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

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

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

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

What should you configure?

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

**Answer: D**

**Explanation:**

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

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

**NEW QUESTION 93**

- (Topic 3)

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.

**Answer:** C

**NEW QUESTION 97**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.

You need to identify whether the members of the Protected Users group will be prevented from authenticating by using NTLM.

Which cmdlet should you use?

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

**Answer:** D

**Explanation:**

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

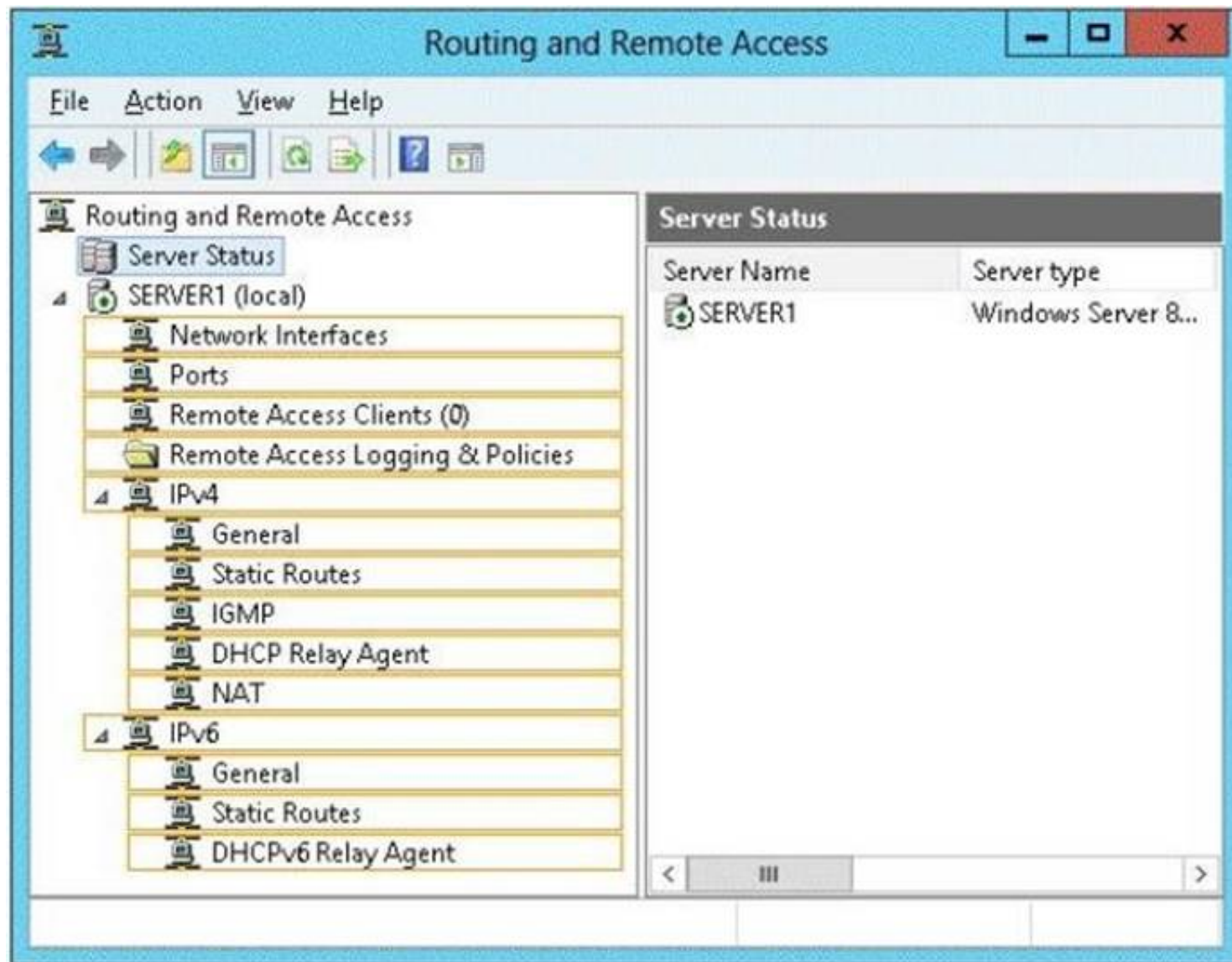
**NEW QUESTION 99**

HOTSPOT - (Topic 3)

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 configure Server1 as a network address translation (NAT) server. Which node should you use to add the NAT routing protocol?

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References: [https://technet.microsoft.com/en-us/library/dd469812\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dd469812(v=ws.11).aspx)

**NEW QUESTION 100**

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

References:

<https://technet.microsoft.com/en-GB/library/jj134239.aspx>

**NEW QUESTION 101**

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. You create a new user account named Admin5. You need to ensure that Admin5 can create Group Policy objects (GPOs) and link the GPOs to all of the organizational units (OUs) in the domain. Admin5 must be prevented from modifying GPOs created by other administrators. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

**Answer:** CD

**NEW QUESTION 106**



- (Topic 3)

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012 R2. The domain contains two domain controllers. The domain controllers are configured as shown in the following table.

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

Active Directory Recycle Bin is enabled.

You discover that a support technician accidentally removed 100 users from an Active Directory group named Group1 an hour ago.

You need to restore the membership of Group1. What should you do?

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

**Answer: D**

#### NEW QUESTION 110

HOTSPOT - (Topic 3)

Your network contains one Active directory forest named contoso.com. The forest contains

a single domain. All domain controllers are virtual machines that run Windows Server 2012 R2. The functional level of the domain and the forest is Windows Server 2012 R2.

The forest contains the domain controllers configured as shown in the following table.

Domain controller name	Configuration
DC01	Active Directory Lightweight Directory Services (AD LDS) Domain naming master Schema master Global catalog DNS server
DC02	Active Directory Certificate Services (AD CS) Relative identifier (ID) master Infrastructure master PDC emulator master DNS server
DC03	Global catalog DHCP server DNS server
DC04	Internet Information Services (IIS) Global catalog DNS server

In the table below, select the domain controller that can be cloned by using domain controller cloning and select the domain controller that must be online to perform domain controller cloning.

NOTE: Make only one selection in each column.

Domain controller	Can be cloned by using domain controller cloning	Must be online to perform domain controller cloning
DC01	<input type="radio"/>	<input type="radio"/>
DC02	<input type="radio"/>	<input type="radio"/>
DC03	<input type="radio"/>	<input type="radio"/>
DC04	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

References:

<http://blogs.technet.com/b/canitpro/archive/2013/06/12/step-by-step-domain-controller-cloning.aspx>

Domain controller	Can be cloned by using domain controller cloning	Must be online to perform domain controller cloning
DC01	<input type="radio"/>	<input type="radio"/>
DC02	<input type="radio"/>	<input checked="" type="radio"/>
DC03	<input type="radio"/>	<input type="radio"/>
DC04	<input checked="" type="radio"/>	<input type="radio"/>

PDC Emulator must be online to perform Domain Controller Cloning. The following server roles are not supported for cloning:

Dynamic Host Configuration Protocol (DHCP) Active Directory Certificate Services (AD CS)

Active Directory Lightweight Directory Services (AD LDS) [https://technet.microsoft.com/en-us/library/hh831734.aspx#virtualized\\_dc\\_cloning](https://technet.microsoft.com/en-us/library/hh831734.aspx#virtualized_dc_cloning)

<http://blogs.technet.com/b/canitpro/archive/2013/06/12/step-by-step-domain-controller-cloning.aspx>

**NEW QUESTION 112**

- (Topic 3)

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

DirectAccess is deployed to the network.

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

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

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

Which Group Policy setting should you configure?

- A. Configure Group Policy slow link detection.
- B. Configure Direct Access connections as a fast network connection.
- C. Configure wireless policy processing.
- D. Change Group Policy processing to run asynchronously when a slow network connection is detected.

**Answer: A**

**NEW QUESTION 115**

- (Topic 3)

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

**Answer: D**

**Explanation:**

[http://www.windowsnetworking.com/articles\\_tutorials/Configuring-DFS-Namespaces.html](http://www.windowsnetworking.com/articles_tutorials/Configuring-DFS-Namespaces.html)

**NEW QUESTION 117**

- (Topic 3)

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

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

All of the computer accounts for the human resources department are members of a group named HR Computers.

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

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

What should you configure?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 120**

- (Topic 3)

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

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

You deploy a new domain controller named DC3 that runs Windows Server 2012 R2. You discover that you cannot create Password Settings objects (PSOs) by using Active Directory Administrative Center.

You need to ensure that you can create PSOs from Active Directory Administrative Center. What should you do?

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

**Answer: C**

#### NEW QUESTION 125

HOTSPOT - (Topic 3)

Your network contains one Active Directory domain named contoso.com. The domain contains 10 file servers that run Windows Server 2012 R2.

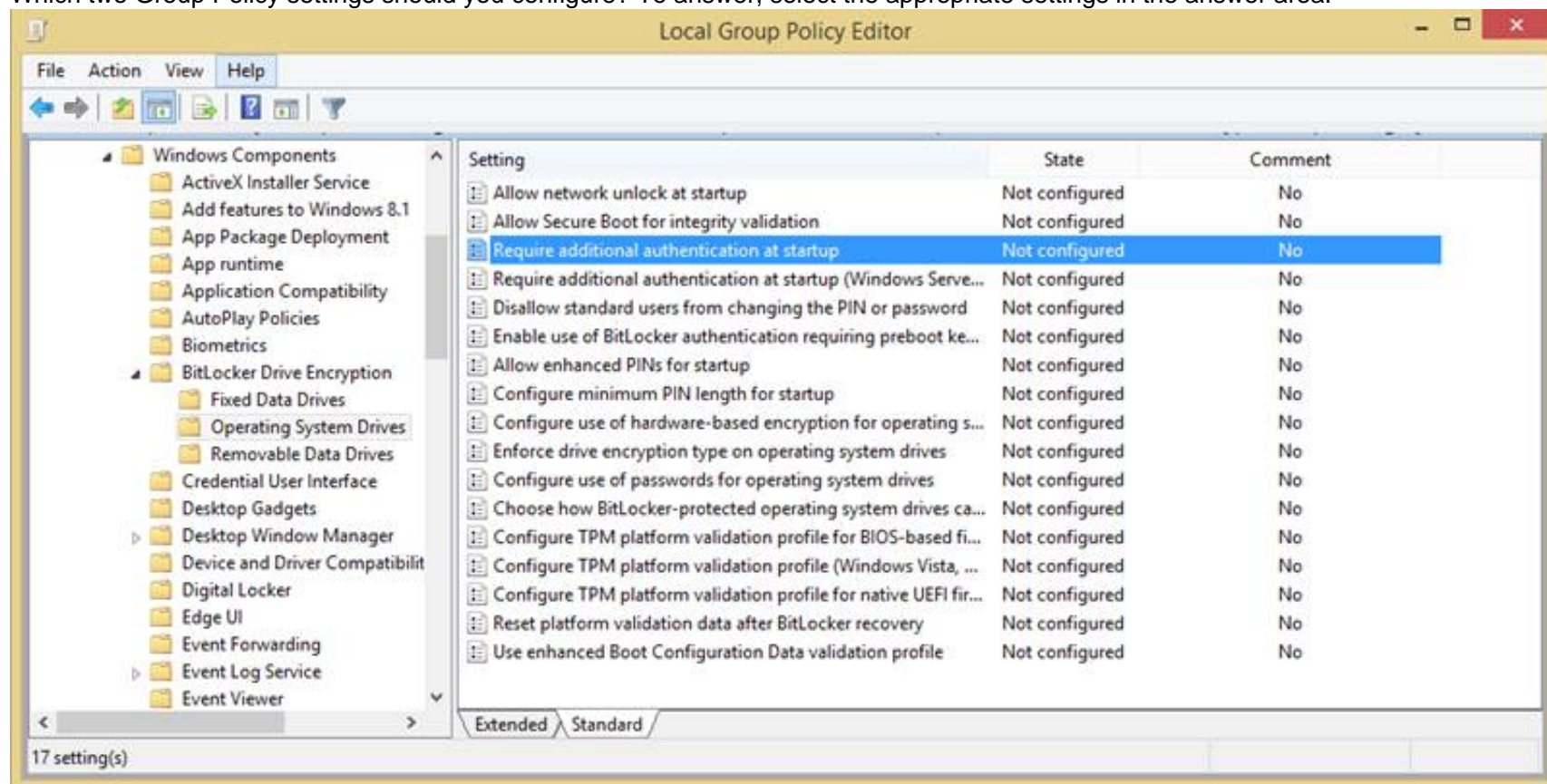
You plan to enable BitLocker Drive Encryption (BitLocker) for the operating system drives of the file servers.

You need to configure BitLocker policies for the file servers to meet the following requirements:

? Ensure that all of the servers use a startup PIN for operating system drives encrypted with BitLocker.

? Ensure that the BitLocker recovery key and recovery password are stored in Active Directory.

Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Choose how BitLocker-protected operating system drives can be recovered: With this policy setting, you can control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. In Save BitLocker recovery information to Active Directory Domain Services, choose which BitLocker recovery information to store in Active Directory Domain Services (AD DS) for operating system drives. If you select Store recovery password and key packages, the BitLocker recovery password and the key package are stored in AD DS. Storing the key package supports recovering data from a drive that is physically corrupted. If you select Store recovery password only, only the recovery password is stored in AD DS.

Require additional authentication at startup: With this policy setting, you can configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker. On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use:

- only the TPM for authentication
- insertion of a USB flash drive containing the startup key
- the entry of a 4-digit to 20-digit personal identification number (PIN)
- a combination of the PIN and the USB flash drive

There are four options for TPM-enabled computers or devices:

- Configure TPM startup
  - o Allow TPM
  - o Require TPM
  - o Do not allow TPM
- Configure TPM startup PIN
  - o Allow startup PIN with TPM
  - o Require startup PIN with TPM
  - o Do not allow startup PIN with TPM
- Configure TPM startup key
  - o Allow startup key with TPM



- o Require startup key with TPM
  - o Do not allow startup key with TPM Configure TPM startup key and PIN
  - o Allow TPM startup key with PIN
  - o Require startup key and PIN with TPM
  - o Do not allow TPM startup key with PIN
- <https://technet.microsoft.com/en-us/library/jj679890.aspx>

**NEW QUESTION 127**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.

You need to identify whether deleted objects can be recovered from the Active Directory Recycle Bin.

Which cmdlet should you use?

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

**Answer:** E

**Explanation:**

The Get-ADOptionalFeature cmdlet gets an optional feature or performs a search to retrieve multiple optional features from an Active Directory.

Example: Get-ADOptionalFeature 'Recycle Bin Feature'

Get the optional feature with the name 'Recycle Bin Feature'.

Reference: Get-ADOptionalFeature <https://technet.microsoft.com/en-us/library/ee617218.aspx>

**NEW QUESTION 130**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.

You need to identify which security principals are authorized to have their password cached on RODC1.

Which cmdlet should you use?

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

**Answer:** B

**NEW QUESTION 132**

DRAG DROP - (Topic 3)

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.

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.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Start Server2 by using PXE. Box 2: Add a capture image to Server1. Box 3: Add an install image to Server1. Note:

\* Capture images are Windows Preinstallation Environment (Windows PE) images that allow you to easily capture the install images that you prepare using Sysprep.exe. Instead of using complex command-line tools, once you have run Sysprep.exe on your reference computer, you can boot to the Windows Deployment Services client computer using PXE and select the capture image. When the capture image boots, it starts the Capture Image Wizard, which will guide you through the capture process and optionally upload the new install image to a Windows Deployment Services server.

Steps

/ create a capture image.

/ Create an install image.

/ Add the install image to the Windows Deployment Services server.

**NEW QUESTION 135**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The forest functional level is Windows Server 2012. All servers run Windows Server 2012 R2. All client computers run Windows 8.1.

The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that

runs Windows Server 2012 R2.

You need to identify which domain controller must be online when cloning a domain controller.

Which cmdlet should you use?

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

**Answer:** D

**Explanation:**

One requirement for cloning a domain controller is an existing Windows Server 2012 DC that hosts the PDC emulator role. You can run the Get-ADDomain and retrieve which server has the PDC emulator role.

Example: Command Prompt: C:\PS> Get-ADDomain

Output would include a line such as: PDCEmulator : Fabrikam-DC1.Fabrikam.com

Incorrect:

Not A: The Get-ADGroupMember cmdlet gets the members of an Active Directory group. Members can be users, groups, and computers.

Not E: The Get-ADOptionalFeature cmdlet gets an optional feature or performs a search to retrieve multiple optional features from an Active Directory.

Not F: The Get-ADAuthorizationGroup cmdlet gets the security groups from the specified user, computer or service accounts token.

Reference: Step-by-Step: Domain Controller Cloning <http://blogs.technet.com/b/canitpro/archive/2013/06/12/step-by-step-domain-controller-cloning.aspx>

Reference: Get-ADDomain <https://technet.microsoft.com/en-us/library/ee617224.aspx>

**NEW QUESTION 138**

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. The domain contains a server named Server01 that runs Windows Server 2012 R2.

Server01 does not have a Trusted Platform Module (TPM).

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

Which Group policy setting should you configure?

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

**Answer:** A

**NEW QUESTION 141**

- (Topic 3)

You have a DNS server that runs Windows Server 2012 R2. The server hosts the zone for contoso.com and is accessible from the Internet.

You need to create a DNS record for the Sender Policy Framework (SPF) to list the hosts that are authorized to send email for contoso.com.

Which type of record should you create?

- A. mail exchanger (MX)
- B. resource record signature (RRSIG)
- C. text (TXT)
- D. name server (NS)

**Answer:** C

**NEW QUESTION 145**

- (Topic 3)

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 148**

.....



## Relate Links

**100% Pass Your 70-411 Exam with ExamBible Prep Materials**

<https://www.exambible.com/70-411-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>