

70-411 Dumps

Administering Windows Server 2012

<https://www.certleader.com/70-411-dumps.html>



NEW QUESTION 1

- (Topic 1)

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

Hyperv1 hosts four virtual machines named VM1, VM2, VM3, and VM4. All of the virtual machines run Windows Server 2008 R2.

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

Which tool should you use on Hyperv1?

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

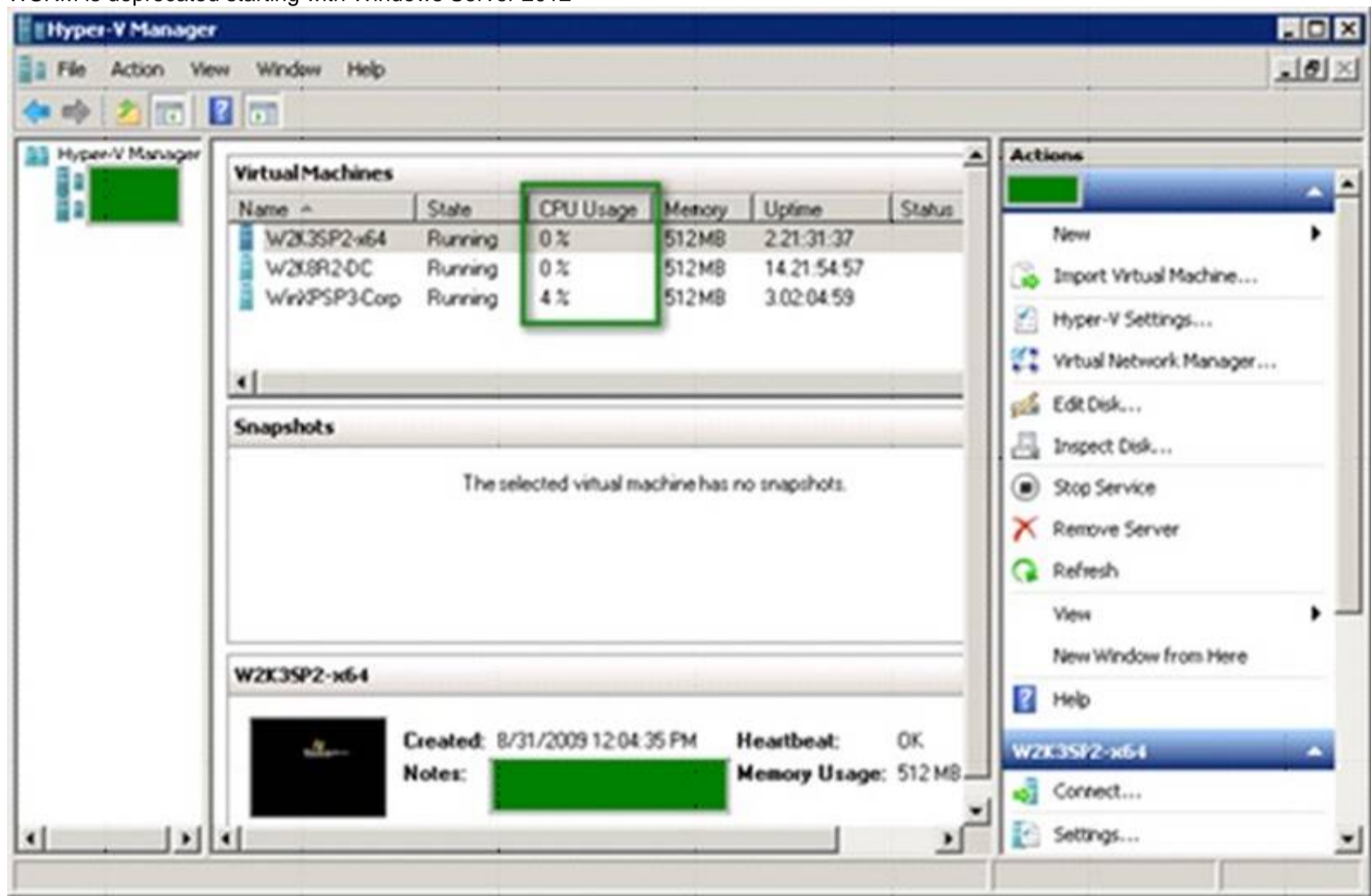
Answer: C

Explanation:

Hyper-V Performance Monitoring Tool

Know which resource is consuming more CPU. Find out if CPUs are running at full capacity or if they are being underutilized. Metrics tracked include Total CPU utilization, Guest CPU utilization, Hypervisor CPU utilization, idle CPU utilization, etc.

WSRM is deprecated starting with Windows Server 2012



NEW QUESTION 2

HOTSPOT - (Topic 1)

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

Server1 has the File Server Resource Manager role service installed.

You need to configure Server1 to meet the following requirements:

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

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

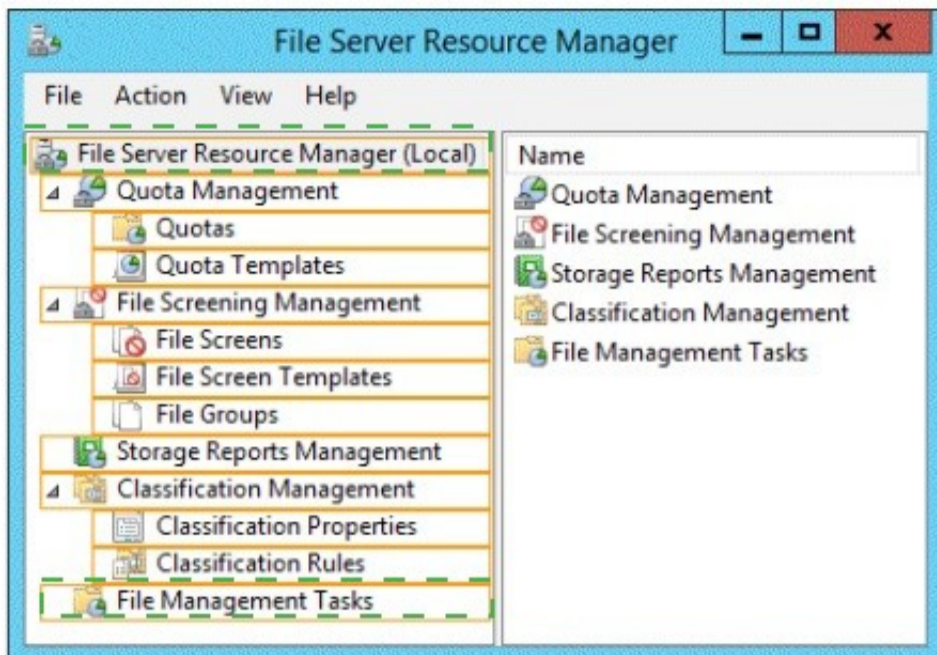
Which two nodes should you configure? To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 3

HOTSPOT - (Topic 1)

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

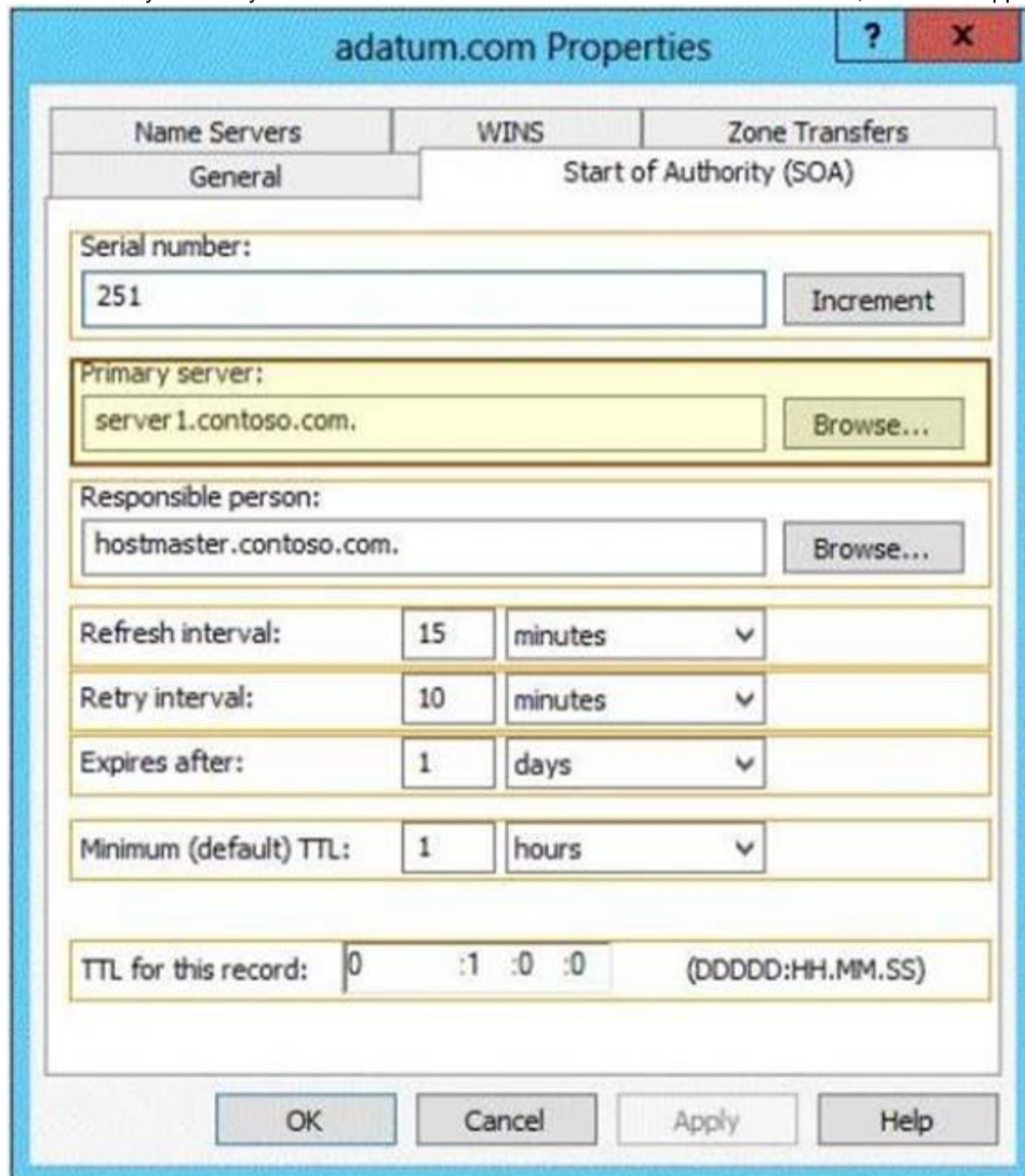
All DNS servers host a DNS zone named adatum.com. The adatum.com zone is not Active Directory-integrated.

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

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

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

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

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

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

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

NEW QUESTION 4

- (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.

You have two GPOs linked to an organizational unit (OU) named OU1. You need to change the precedence order of the GPOs.

What should you use?

- A. Dcgpofix
- B. Get-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: I

Explanation:

The Set-GPLinkcmdlet sets the properties of a GPO link. You can set the following properties:

? Enabled. If the GPO link is enabled, the settings of the GPO are applied when

Group Policy is processed for the site, domain or OU.

? Enforced. If the GPO link is enforced, it cannot be blocked at a lower-level (in the Group Policy processing hierarchy) container.

? Order. The order specifies the precedence that the settings of the GPO take over conflicting settings in other GPOs that are linked (and enabled) to the same site, domain, or OU.

Reference: <http://technet.microsoft.com/en-us/library/ee461022.aspx>

NEW QUESTION 5

- (Topic 1)

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

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

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

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

Answer: C

Explanation:

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

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

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

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

auditpol /resourceSACL

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

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

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

References:

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

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

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

NEW QUESTION 6

- (Topic 1)

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

You implement DirectAccess by using the default configuration.

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

DirectAccess to access other resources in contoso.com.
Which settings should you configure in a Group Policy object (GPO)?

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 7

- (Topic 1)

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

Server1 has the following role services installed:

? DirectAccess and VPN (RRAS)

? Network Policy Server

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

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

What should you configure on Server1?

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

Answer: A

Explanation:

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

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

NEW QUESTION 8

- (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 9

HOTSPOT - (Topic 1)

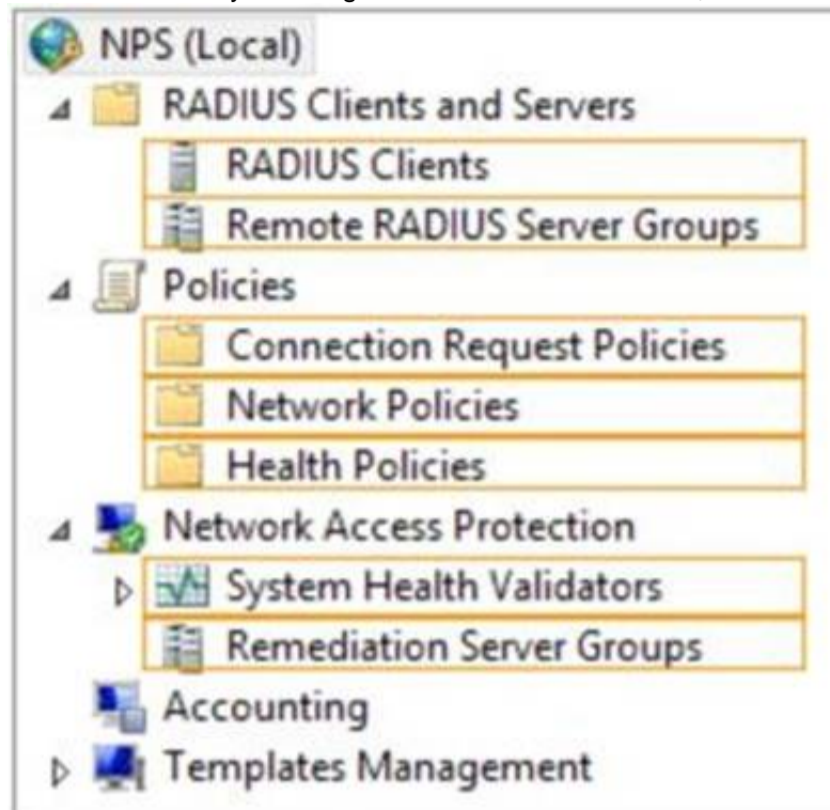
Your network contains a RADIUS server named Server1.

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

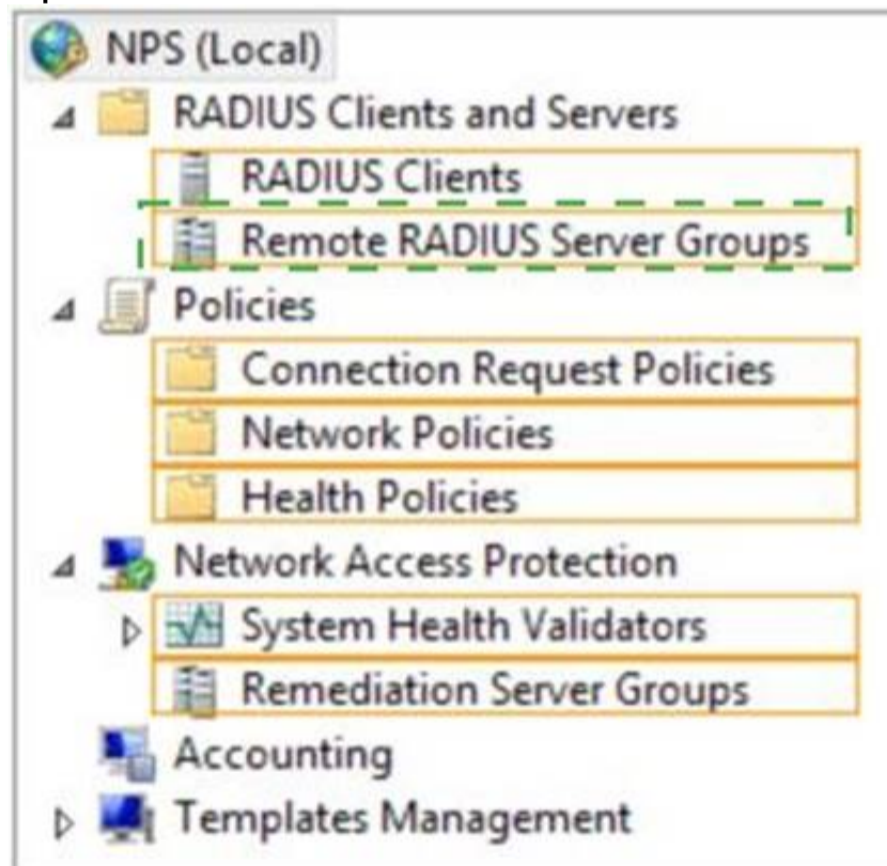
You need to ensure that all accounting requests for Server2 are forwarded to Server1.

On Server2, you configure a Connection Request Policy.

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



- A. Mastered
- B. Not Mastered

Answer: A**Explanation:****NEW QUESTION 10**

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains six domain controllers named DC1, DC2, DC3, DC4, DC5, and DC6.

Each domain controller has the DNS Server server role installed and hosts an Active Directory-integrated zone for contoso.com.

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

You need to ensure that the new zone will be available only on DC5 and DCG. What should you do first?

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

Answer: D**Explanation:**

You can store Domain Name System (DNS) zones in the domain or application directory partitions of Active Directory Domain Services (AD DS). A partition is a

data structure in AD DS that distinguishes data for different replication purposes. When you create an application directory partition for DNS, you can control the scope of replication for the zone that is stored in that partition.

NEW QUESTION 10

- (Topic 1)

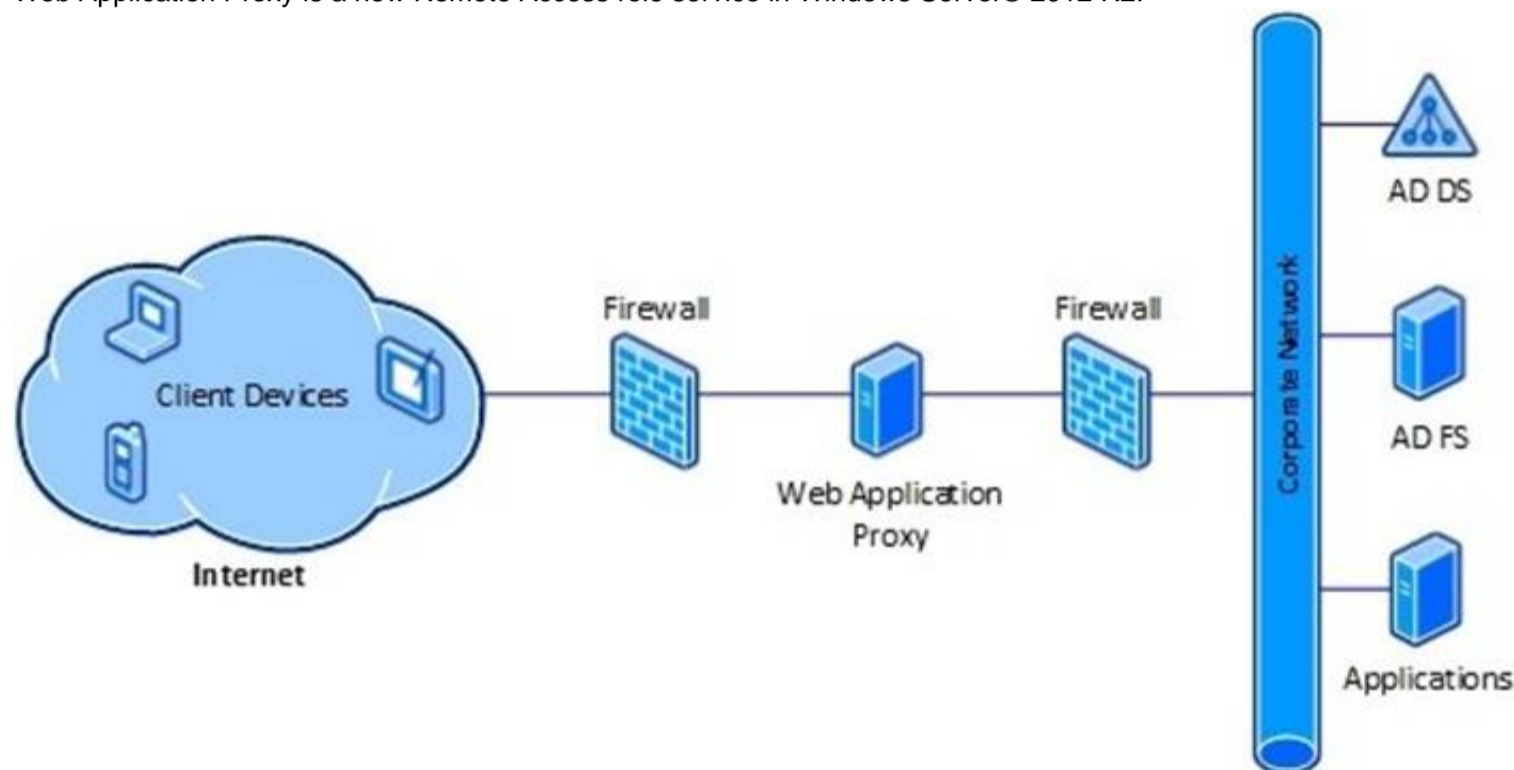
Your network contains an Active Directory domain named contoso.com. You need to install and configure the Web Application Proxy role service. What should you do?

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

Answer: A

Explanation:

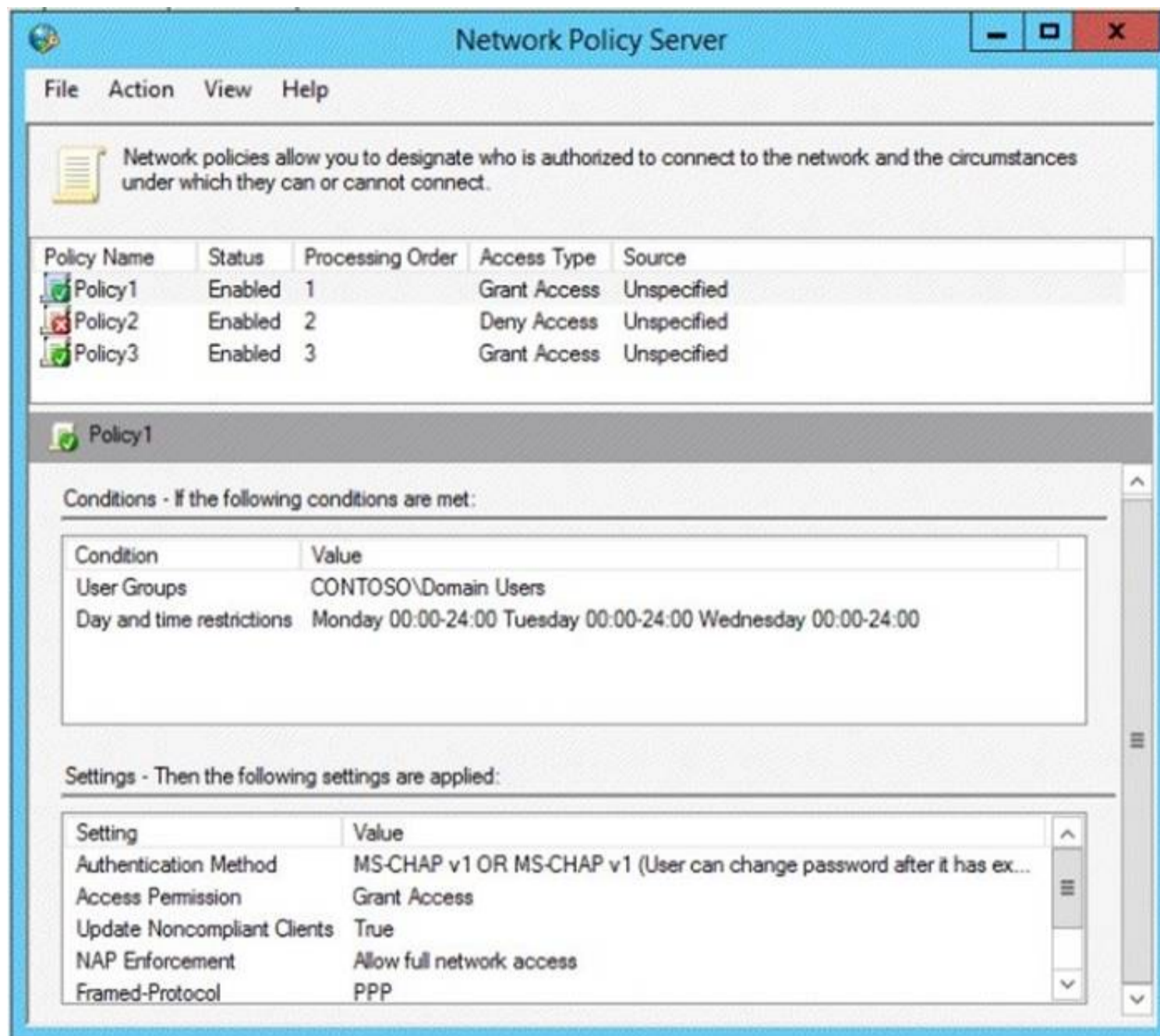
Web Application Proxy is a new Remote Access role service in Windows Server® 2012 R2.

**NEW QUESTION 14**

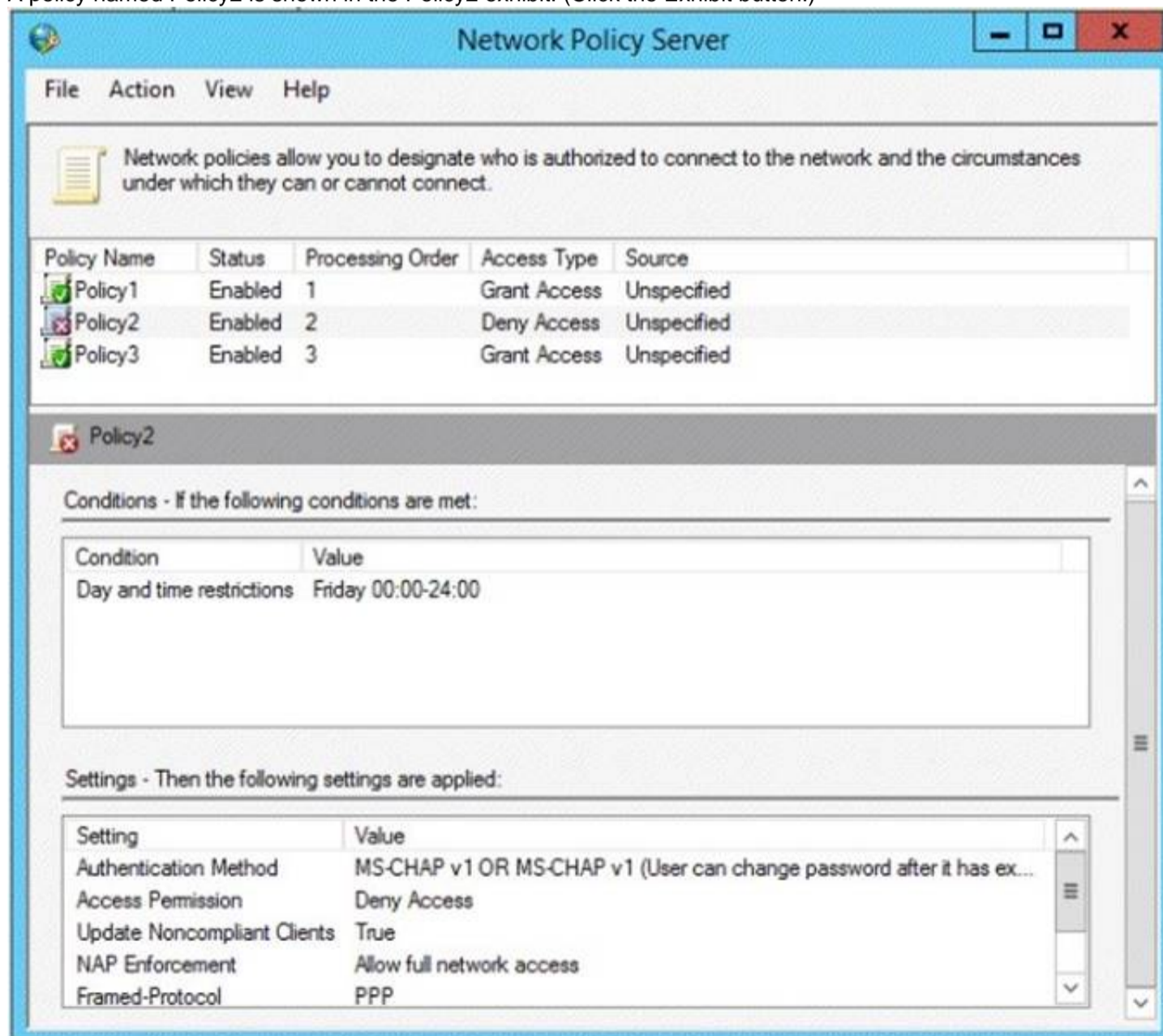
HOTSPOT - (Topic 1)

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

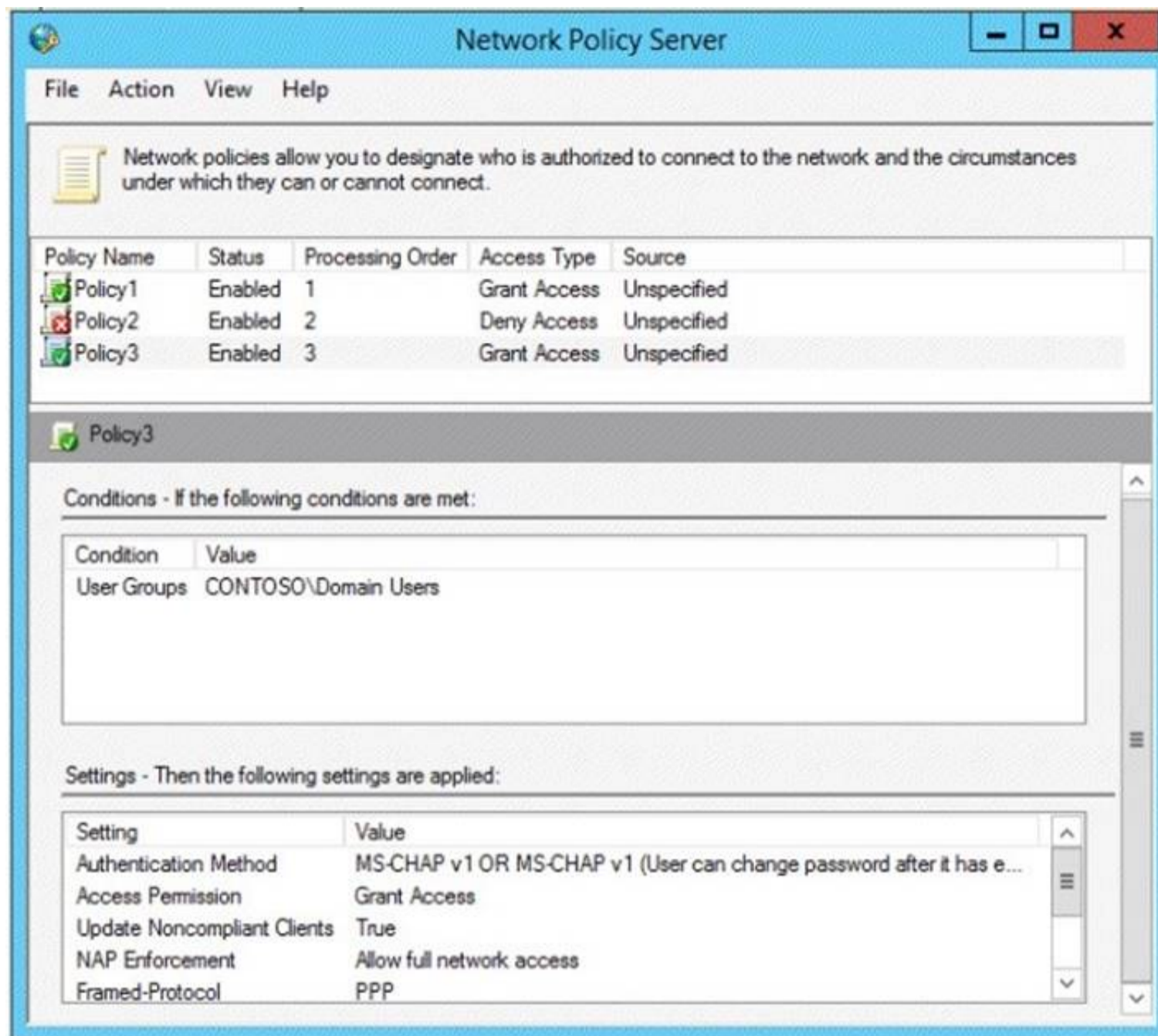
The Network Access Permission for User1 is set to Control access through NPS Network Policy. The Network Access Permission for User2 is set to Allow access. A policy named Policy1 is shown in the Policy1 exhibit. (Click the Exhibit button.)



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 19

- (Topic 1)

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

What should you do?

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

Answer: A

Explanation:

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

References:

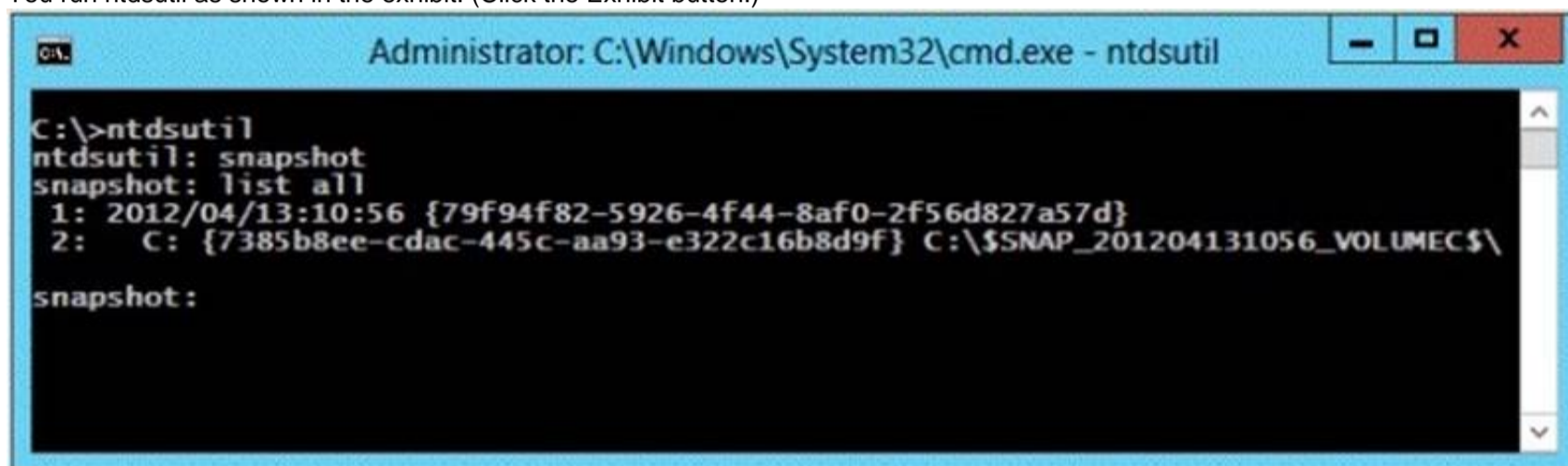
[http://technet.microsoft.com/en-us/library/cc749447\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc749447(v=ws.10).aspx) [http://technet.microsoft.com/en-us/library/dd744382\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd744382(v=ws.10).aspx) <http://technet.microsoft.com/en-us/library/hh825224.aspx>

NEW QUESTION 21

- (Topic 1)

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

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



You need to ensure that you can access the contents of the mounted snapshot. What should you do?

- A. From the snapshot context of ntdsutil, run activate instance "NTDS".
- B. From a command prompt, run dsamain.exe -dbpath c:\\$snap_201204131056_volume c:\windows\ntds\ntd
- C. dit -ldapport 389.
- D. From the snapshot context of ntdsutil, run mount {79f94f82-5926-4f44-8af0-2f56d827a57d}.
- E. From a command prompt, run dsamain.exe -dbpath c:\\$snap_201204131056_volume c:\windows\ntds\ntd
- F. dit -ldapport 33389.

Answer: D

Explanation:

By default, only members of the Domain Admins group and the Enterprise Admins group are allowed to view the snapshots because they contain sensitive AD DS data. If you want to access snapshot data from an old domain or forest that has been deleted, you can allow nonadministrators to access the data when you run Dsamain.exe.

If you plan to view the snapshot data on a domain controller, specify ports that are different from the ports that the domain controller will use.

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP port and UDP [7] port 389. The client then sends

an operation request to the server, and the server sends responses in return. With some exceptions, the client does not need to wait for a response before sending the next request, and the server may send the responses in any order. All information is transmitted using Basic Encoding Rules (BER).

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

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

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

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

snapshot: mount {062d937f-9cdd-4286-8938-9c29ce83c8a6}
Snapshot {d41683c7-ae91-48fc-a639-1e9b82138bf4} mounted as C:\$SNAP_201212101208_UOLUMECS\
snapshot: quit
ntdsutil: quit

C:\Windows\system32>dsamain -dbpath c:\$SNAP_201212101208_UOLUMECS\windows\ntds\
ntds.dit -ldapport 5000
EVENTLOG <Informational>: NTDS General / Internal Configuration : 2168
The DC is running on a supported hypervisor. VM Generation ID is detected.

Current value of VM Generation ID: 6680128214492828164

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

msDS-GenerationId attribute value:
6680128214492828164

EVENTLOG <Informational>: NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete, version 6.2.9200.16384
```

References:

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

NEW QUESTION 26

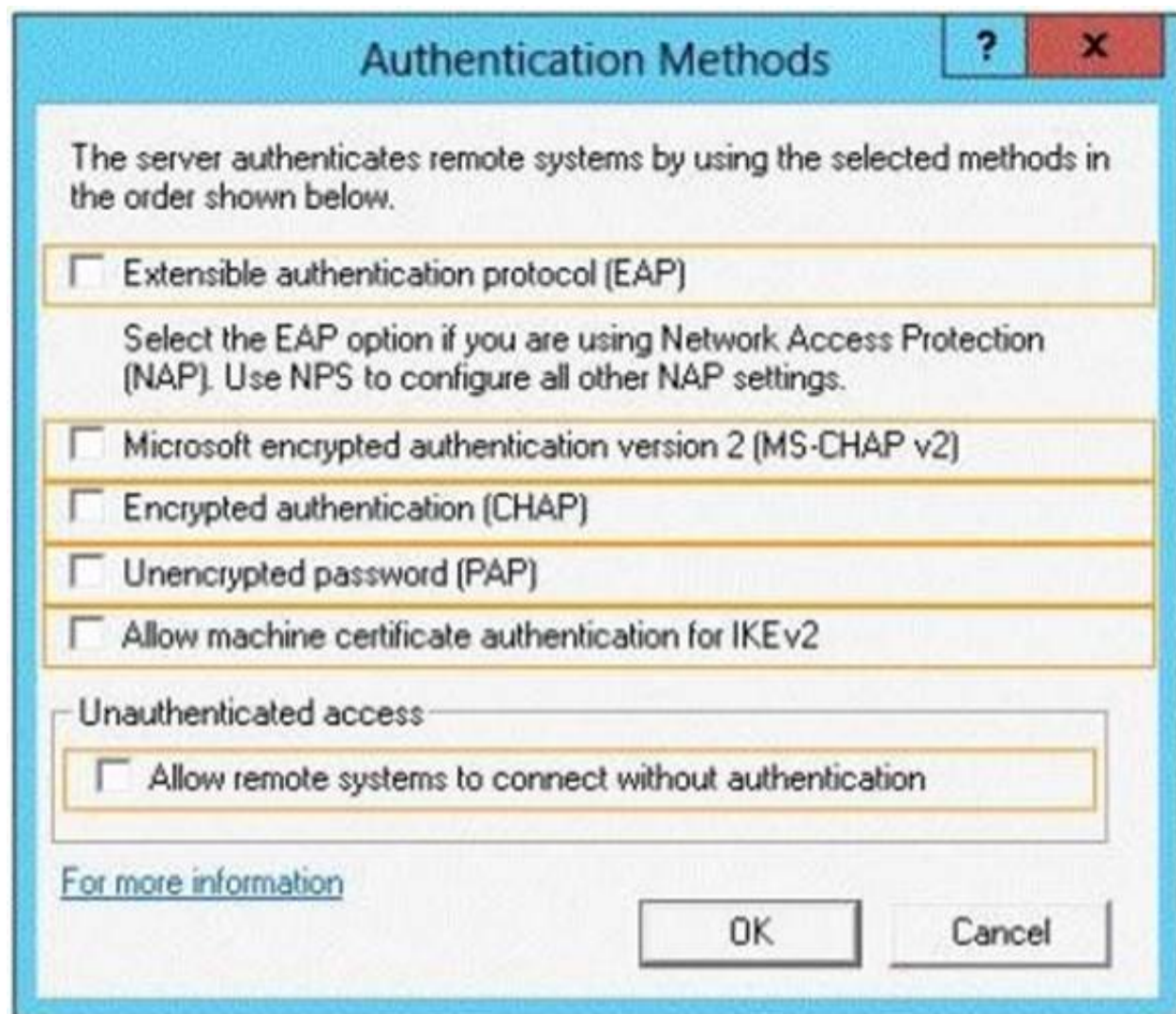
HOTSPOT - (Topic 1)

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

You have a client named Client1 that is configured as an 802.1X supplicant.

You need to configure Server1 to handle authentication requests from Client1. The solution must minimize the number of authentication methods enabled on Server1.

Which authentication method should you enable? To answer, select the appropriate authentication method in the answer area.



- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Microsoft® Windows® uses EAP to authenticate network access for Point-to-Point Protocol (PPP) connections (dial-up and virtual private network) and for IEEE 802.1X-based network access to authenticating Ethernet switches and wireless access points (APs).

NEW QUESTION 28

- (Topic 1)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed. Server1 has a folder named Folder1 that is used by the human resources department. You need to ensure that an email notification is sent immediately to the human resources manager when a user copies an audio file or a video file to Folder1. What should you configure on Server1?

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

Answer: C

Explanation:

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

With File Server Resource Manager (FSRM) you can create file screens that prevent users from saving unauthorized files on volumes or folders. File Screen Enforcement:

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

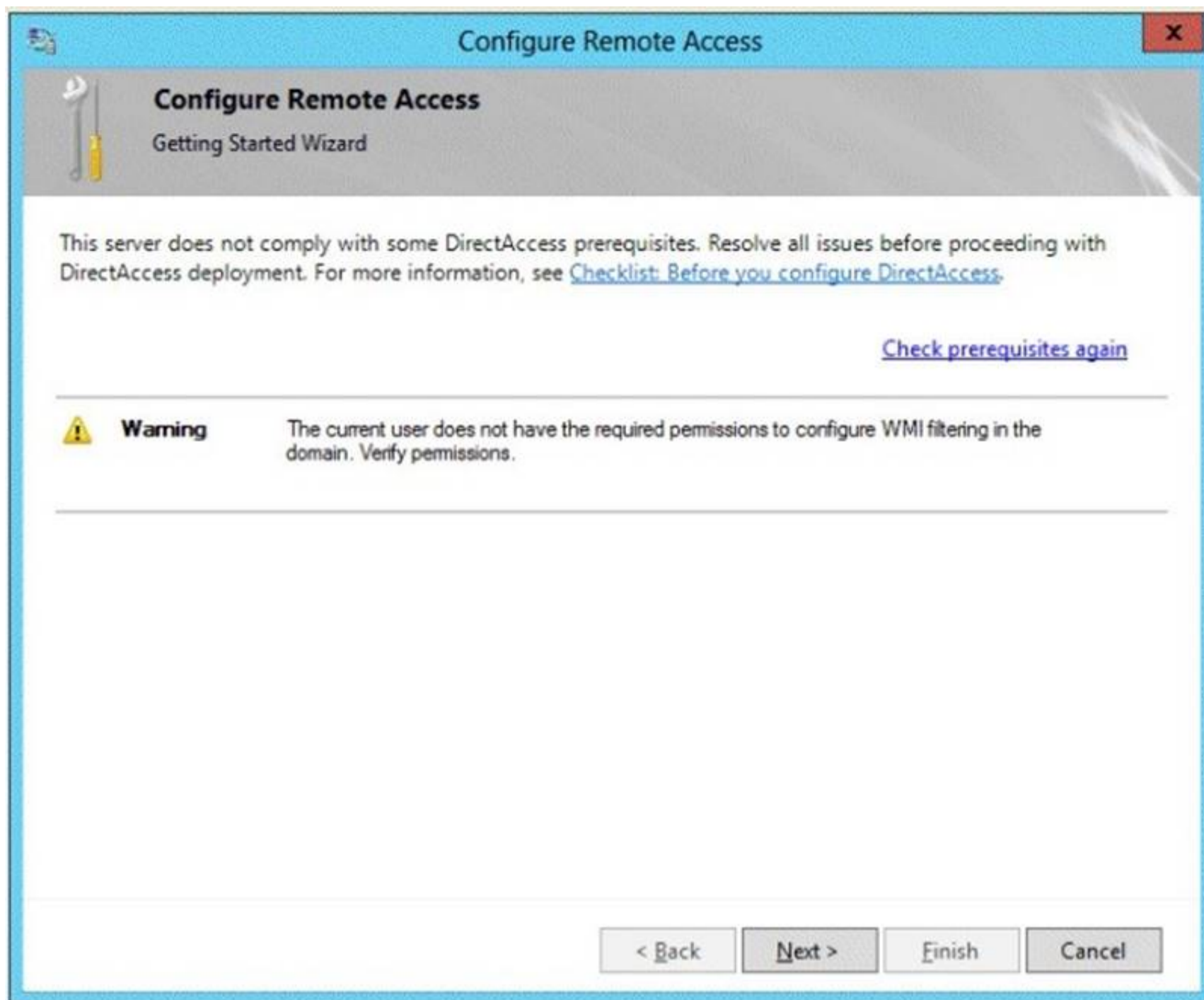
NEW QUESTION 33

- (Topic 1)

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

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

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



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

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

Answer: B

Explanation:

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

Administrators (A built-in group)

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

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

References:

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

NEW QUESTION 36

- (Topic 1)

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

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

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

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

What should you do?

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

Answer: A

Explanation:

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

The owner distribution list is configured by using the SMB Share – Advanced file share profile in the New Share Wizard in Server Manager.

NEW QUESTION 40

DRAG DROP - (Topic 1)

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

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

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

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

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

Network policy Properties

Overview | Conditions | Constraints | Settings

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

Settings:

RADIUS Attributes

- Standard
- Vendor Specific

Network Access Protection

- NAP Enforcement**
- Extended State

Routing and Remote Access

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

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

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

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

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

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

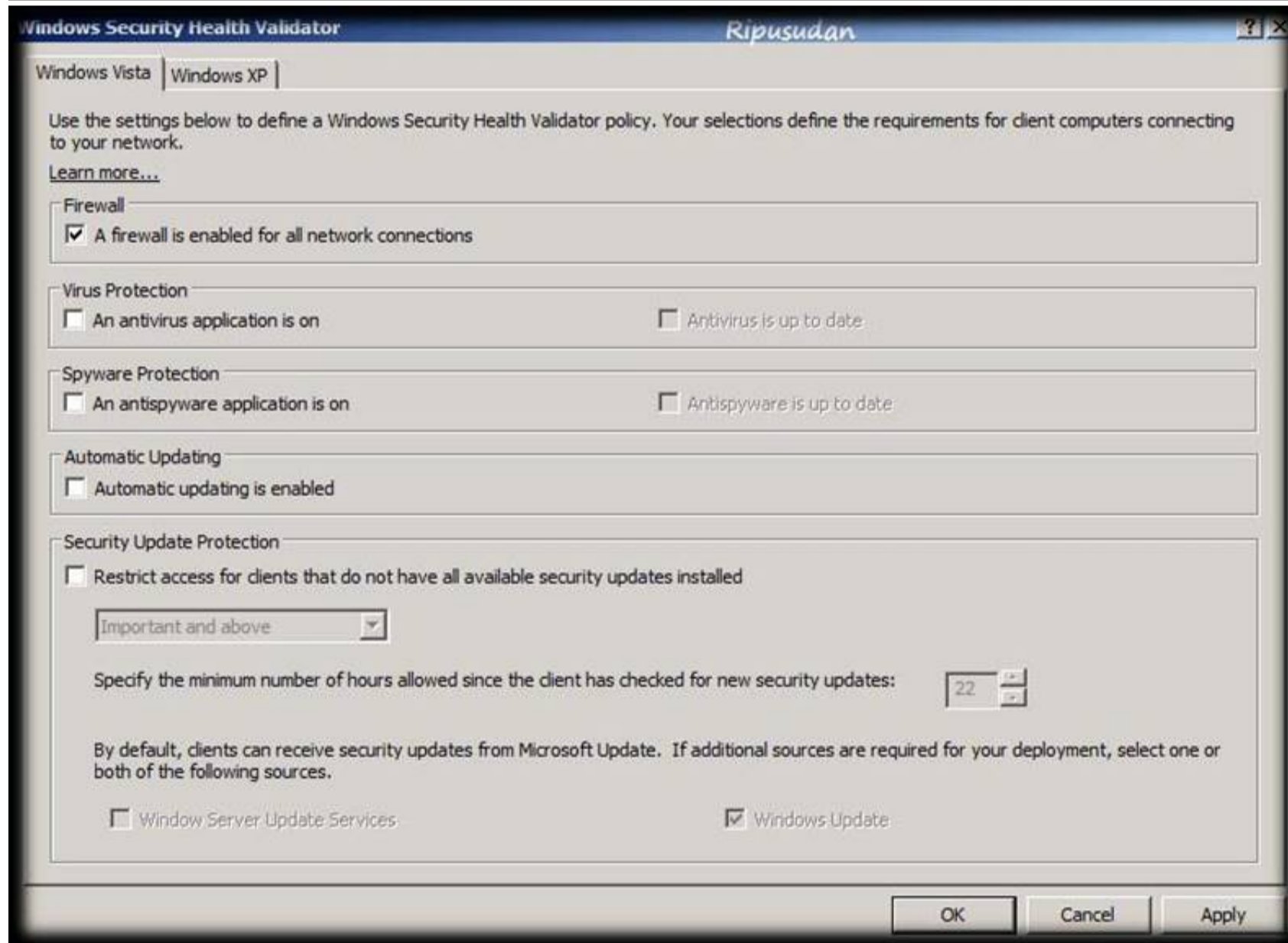
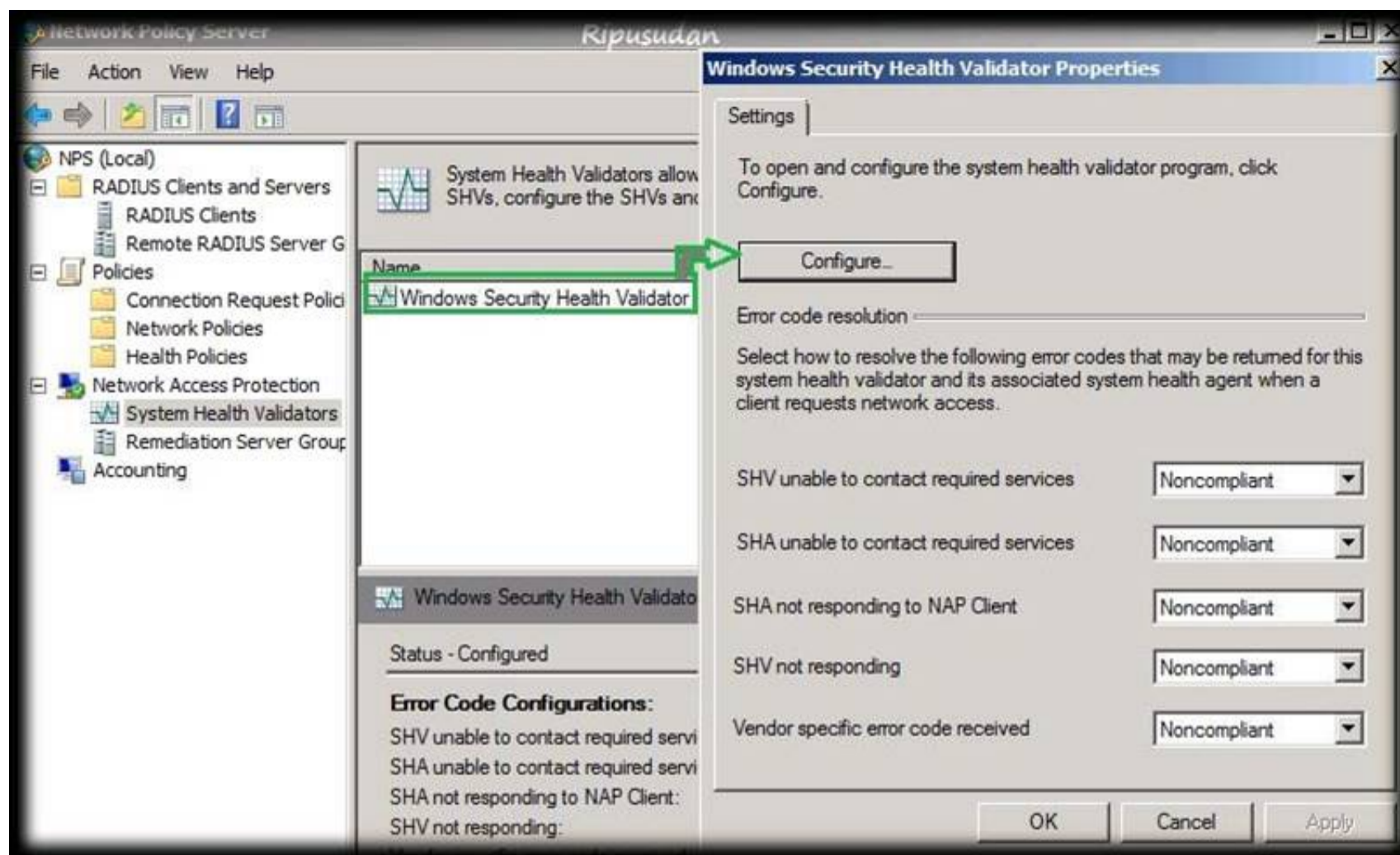
Remediation Server Group and Troubleshooting URL
To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

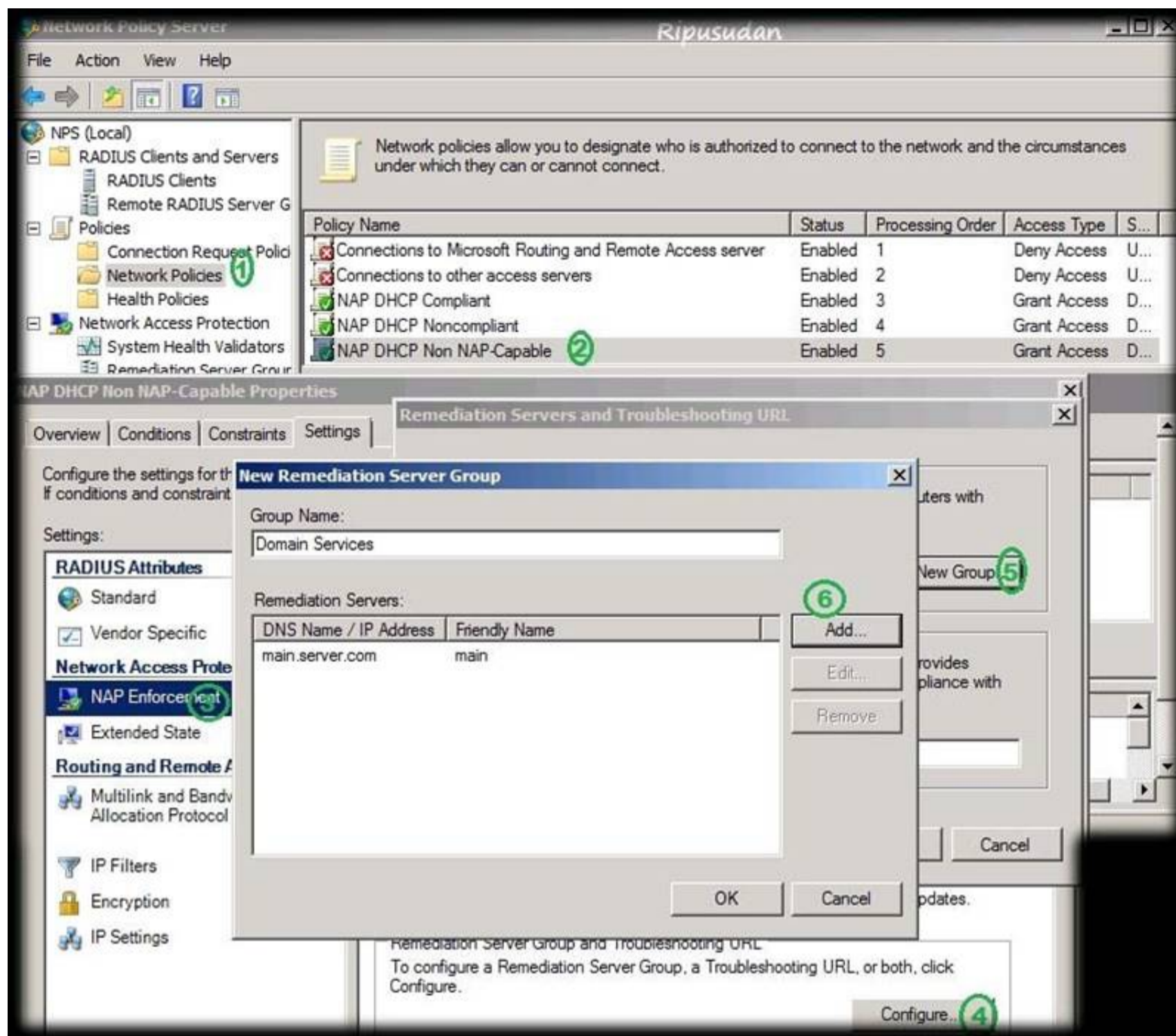
Configure...

Auto remediation

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

OK Cancel Apply





* 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 41

- (Topic 1)

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

You install the Remote Access server role on 10 servers.

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

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

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

Answer: CD

Explanation:

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

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

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

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

NEW QUESTION 45

- (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 49

DRAG DROP - (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 Web Server (IIS) server role installed.

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

You need to identify the setspn.exe command that you must run to configure the appropriate Service Principal Name (SPN) for the web site.

What should you run?

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

The screenshot shows a drag-and-drop interface. On the left, under the 'Objects' header, there is a list of items: '-r', '-s', 'AppPool1', 'http/contoso', 'https/contoso', 'http/secure.contoso.com', and 'https/secure.contoso.com'. On the right, under the 'Answer Area' header, there is a text input field containing 'setspn.exe' followed by three empty boxes, each labeled 'Object'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Note:

* -s <SPN>

Adds the specified SPN for the computer, after verifying that no duplicates exist. Usage: setspn -s SPN accountname

For example, to register SPN "http/daserver" for computer "daserver1": setspn -S http/daserver daserver1

[http://technet.microsoft.com/en-us/library/cc731241\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731241(v=ws.10).aspx)

Attn: with Windows 2008 option is -a but with Windows 2012 it started to show -s Definition of an SPN

An SPN is the name by which a client uniquely identifies an instance of a service. If you install multiple instances of a service on computers throughout a forest, each service instance must have its own SPN. A particular service instance can have multiple SPNs if there are multiple names that clients might use for authentication. For example, an SPN always includes the name of the host computer on which the service instance is running. Therefore, a service instance might register an SPN for each name or alias of its host.

Adding SPNs

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

The HTTP service class

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

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

References:

<http://support.microsoft.com/kb/929650/en-us>

<http://technet.microsoft.com/en-us/library/cc731241%28v=ws.10%29.aspx>

NEW QUESTION 51

- (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

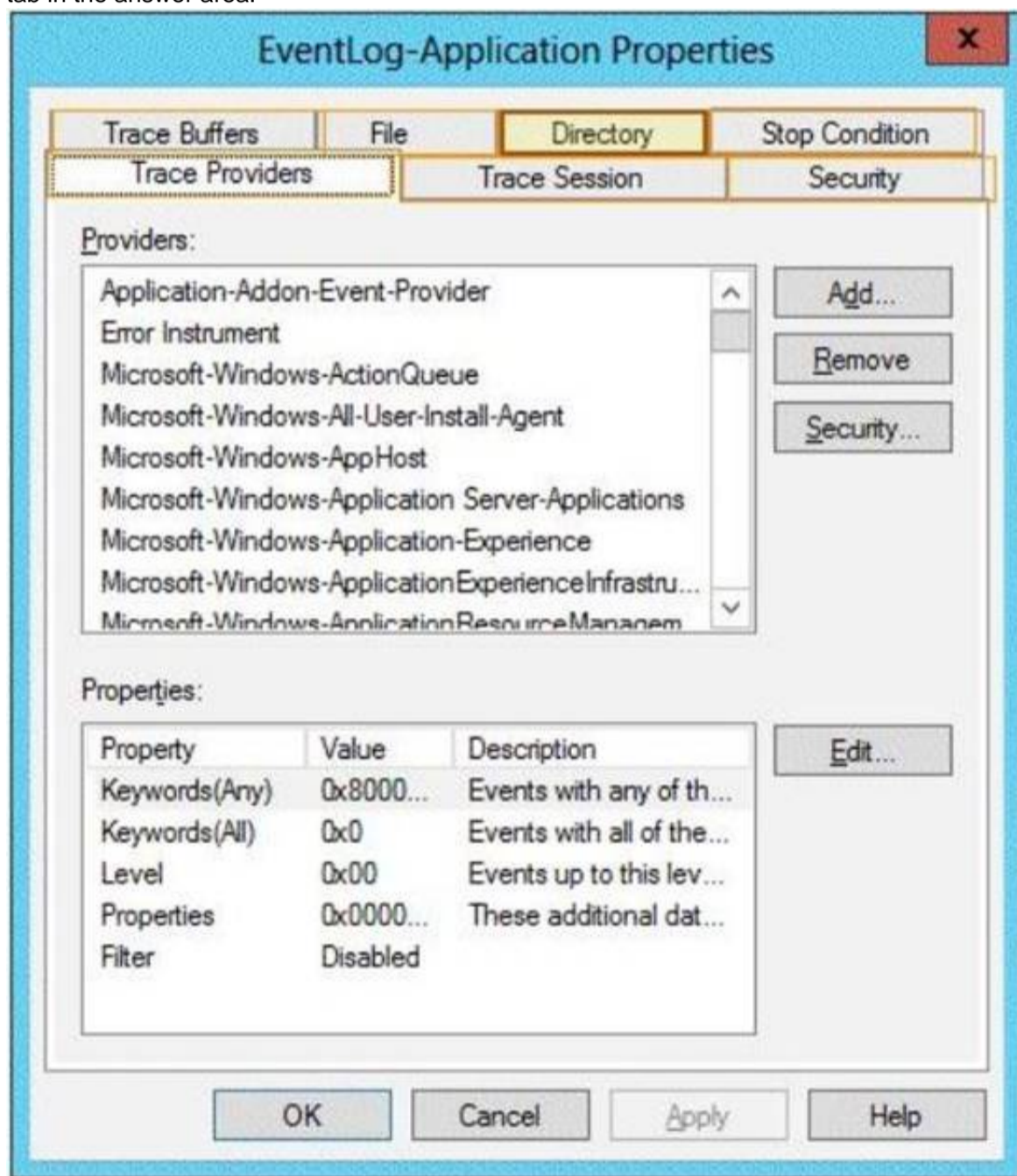
NEW QUESTION 53

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).

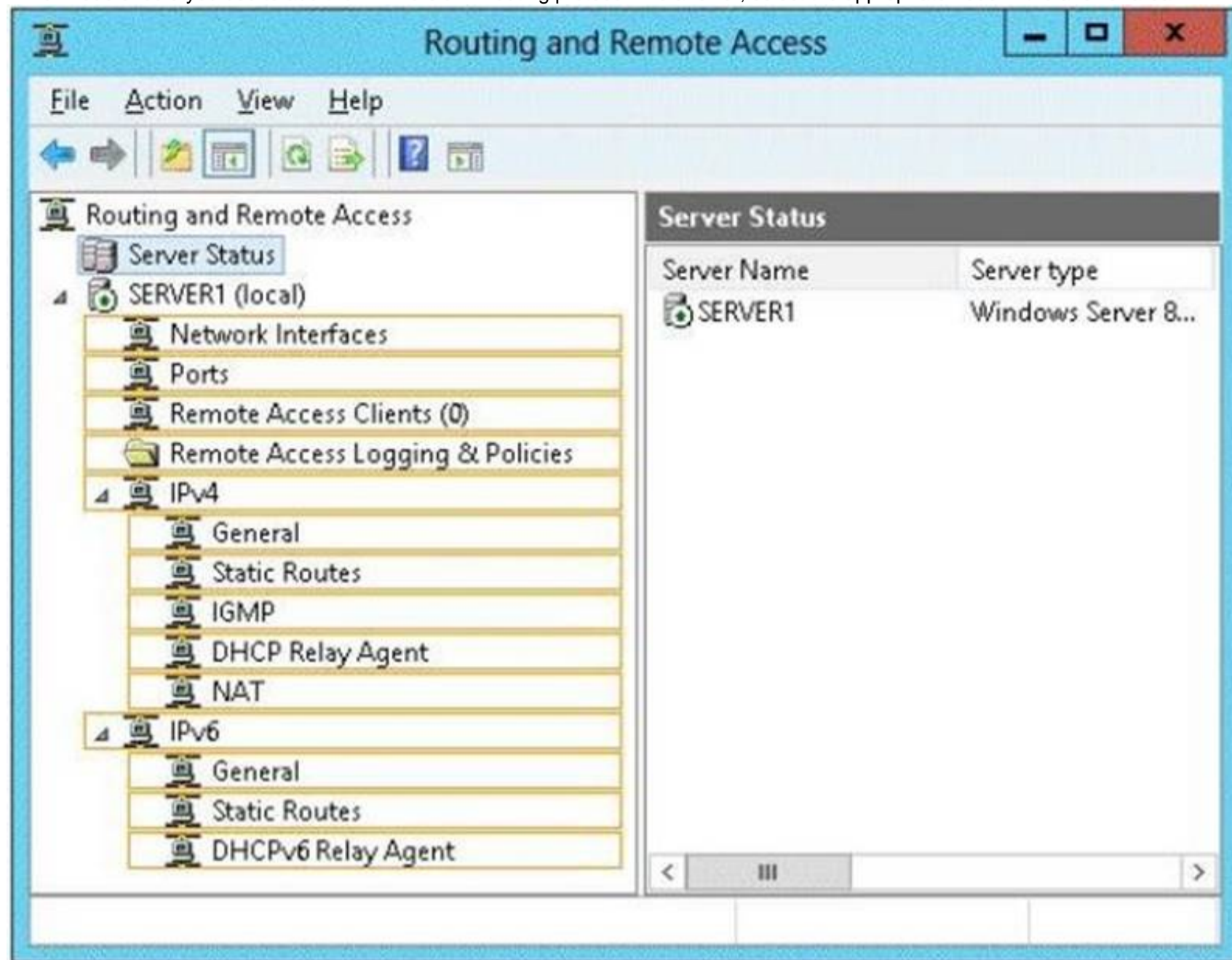
NEW QUESTION 55

HOTSPOT - (Topic 1)

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

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

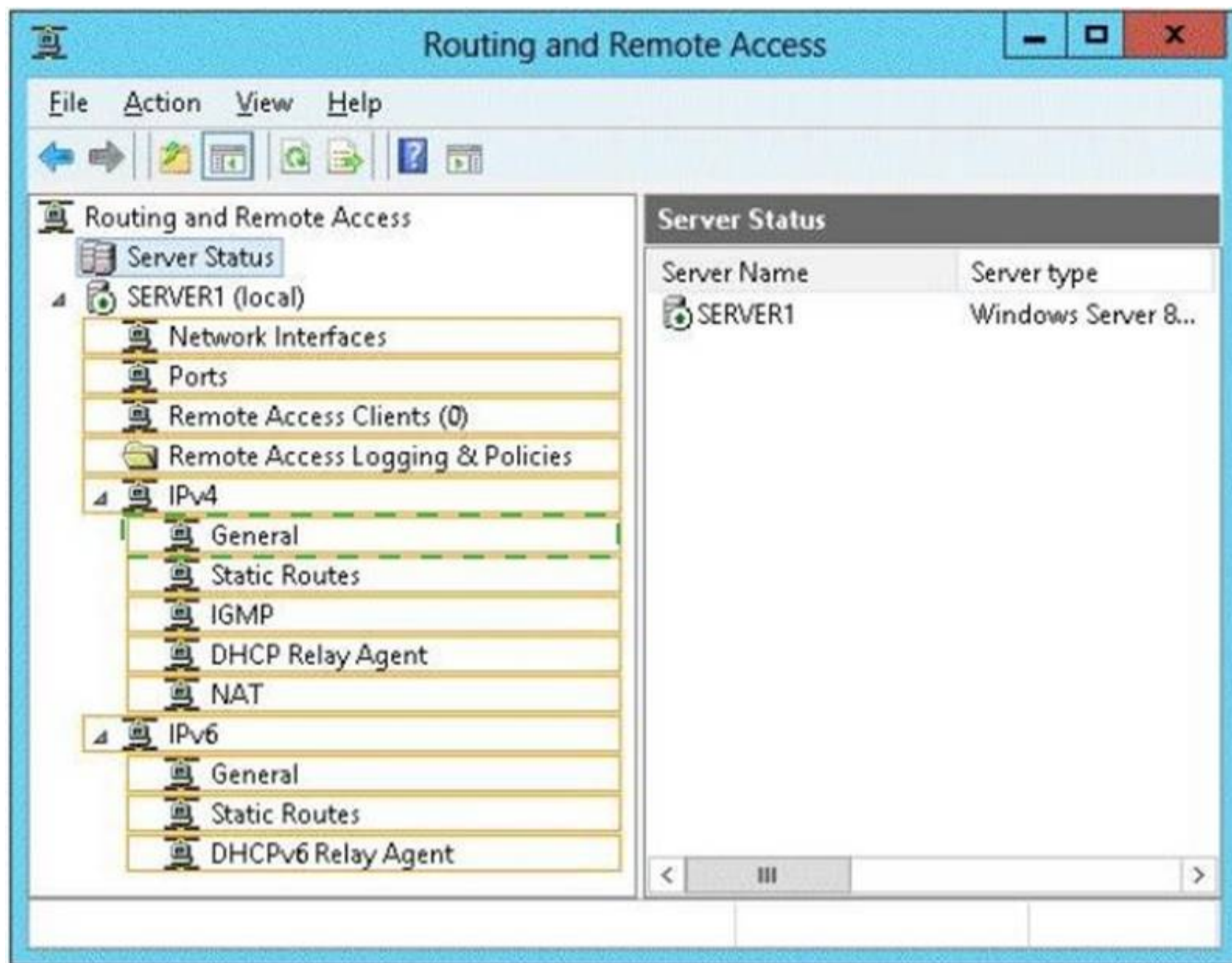
Which node should you use to add the RIP version 2 routing protocol? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 56

- (Topic 1)

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

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

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

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

Which type of zone should you create?

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

Answer: B

Explanation:

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

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



You can use stub zones to:

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

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

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

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

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

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

References:

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

NEW QUESTION 58

- (Topic 1)

You have a server named Server 1.

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

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 59

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 dism.exe and specify the <i>/Capture-Image</i> parameter.	
Run dism.exe and specify the <i>/Apply-Image</i> parameter.	
Run wusa.exe and specify the <i>/uninstall</i> parameter.	
Run dism.exe and specify the <i>/RemovePackage</i> parameter.	
Run dism.exe 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 62

- (Topic 1)

Your network contains four Network Policy Server (NPS) servers named Server1, Server2, Servers, and Server4.

Server1 is configured as a RADIUS proxy that forwards connection requests to a remote RADIUS server group named Group1.

You need to ensure that Server2 and Server3 receive connection requests. Server4 must only receive connection requests if both Server2 and Server3 are unavailable.

How should you configure Group1?

- A. Change the Weight of Server4 to 10.
- B. Change the Weight of Server2 and Server3 to 10.
- C. Change the Priority of Server2 and Server3 to 10.
- D. Change the Priority of Server4 to 10.

Answer: D

Explanation:

During the NPS proxy configuration process, you can create remote RADIUS server groups and then add RADIUS servers to each group. To configure load balancing, you must have

more than one RADIUS server per remote RADIUS server group. While adding group members, or after creating a RADIUS server as a group member, you can access the Add RADIUS server dialog box to configure the following items on the Load Balancing tab:

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

Weight. NPS uses this Weight setting to determine how many connection requests to send to each group member when the group members have the same priority level. Weight setting must be assigned a value between 1 and 100, and the value represents a percentage of 100 percent. For example, if the remote RADIUS server group contains two members that both have a priority level of 1 and a weight rating of 50, the NPS proxy forwards 50 percent of the connection requests to each RADIUS server.

Advanced settings. These failover settings provide a way for NPS to determine whether the remote RADIUS server is unavailable. If NPS determines that a RADIUS server is unavailable, it can start sending connection requests to other group members. With these settings you can configure the number of seconds that the NPS proxy waits for a response from the RADIUS server before it considers the request dropped; the maximum number of dropped requests before the NPS proxy identifies the RADIUS server as unavailable; and the number of seconds that can elapse between requests before the NPS proxy identifies the RADIUS server as unavailable.

The default priority is 1 and can be changed from 1 to 65535. So changing server 2 and 3 to priority 10 is not the way to go.

Edit RADIUS Server

Address Authentication/Accounting Load Balancing

The priority of ranking indicates the status of a server. A primary server has a priority of 1.

Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority.

Priority: 1 Weight: 50

Advanced settings

Number of seconds without response before request is considered dropped: 3

Maximum number of dropped requests before server is identified as unavailable: 5

Number of seconds between requests when server is identified as unavailable: 30

OK Cancel Apply

Reference: [http://technet.microsoft.com/en-us/library/dd197433\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd197433(WS.10).aspx)

NEW QUESTION 66

- (Topic 1)

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

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

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 68

- (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.

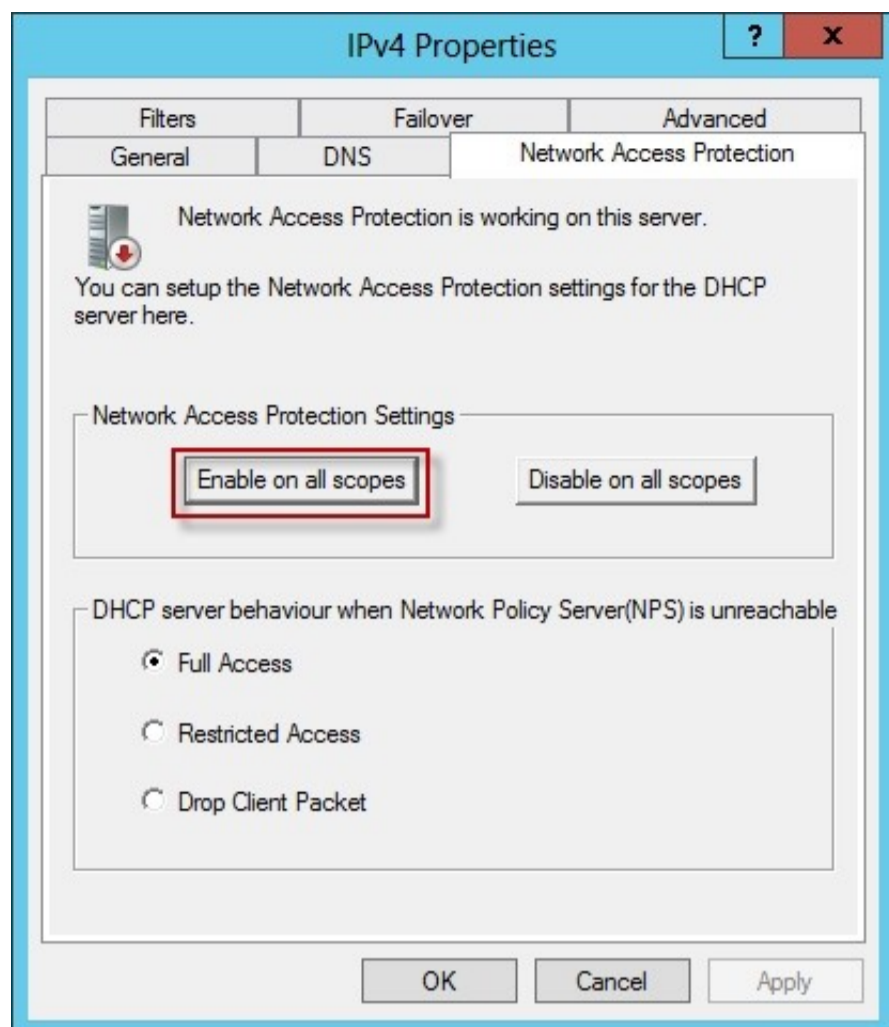
You enable Network Access Protection (NAP) on all of the DHCP scopes on Server1. You need to create a DHCP policy that will apply to all of the NAP non-compliant DHCP clients.

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 73

- (Topic 1)

Your network contains an Active Directory domain named `adatum.com`. A network administrator creates a Group Policy central store.

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

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

What should you do?

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

Answer: C

Explanation:

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

NEW QUESTION 77

DRAG DROP - (Topic 1)

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

The schema is upgraded to Windows Server 2012 R2.

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

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

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Note: Box 1:

Group Managed Service Accounts Requirements:

At least one Windows Server 2012 Domain Controller

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

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

To create a new managed service account

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

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

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

Box 3:

Configure a service account for Internet Information Services

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

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

? Click Start, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.

? Double-click <Computer name>, double-click Application Pools, right-click <Pool Name>, and click Advanced Settings.

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

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

NEW QUESTION 79

- (Topic 1)

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

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

What should you do?

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

Answer: A

Explanation:

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

To view or modify the properties of a Data Collector Set after it has been created, you can:

* Select the Open properties for this data collector set check box at the end of the Data Collector Set Creation Wizard.

* Right-click the name of a Data Collector Set, either in the MMC scope tree or in the console window, and click Properties in the context menu.

Directory tab:

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

NEW QUESTION 81

- (Topic 1)

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

You have a desktop computer that has the following configuration:

? Computer name: Computer1

? Operating system: Windows 8

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

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

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

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

A. 20CF3065D08700000000000000000000

B. 979708BFC04B45259FE0C4150BB6C618

C. 979708BF-C04B-452S-9FE0-C4150BB6C618

D. 00000000000000000000000020CF306SD087

E. 00000000-0000-0000-0000-C41S0BB6C618

Answer: CD

Explanation:

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

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

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

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

Windows PowerShell

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

```
-DomainName "TSQA.contoso.com"
```

NEW QUESTION 85

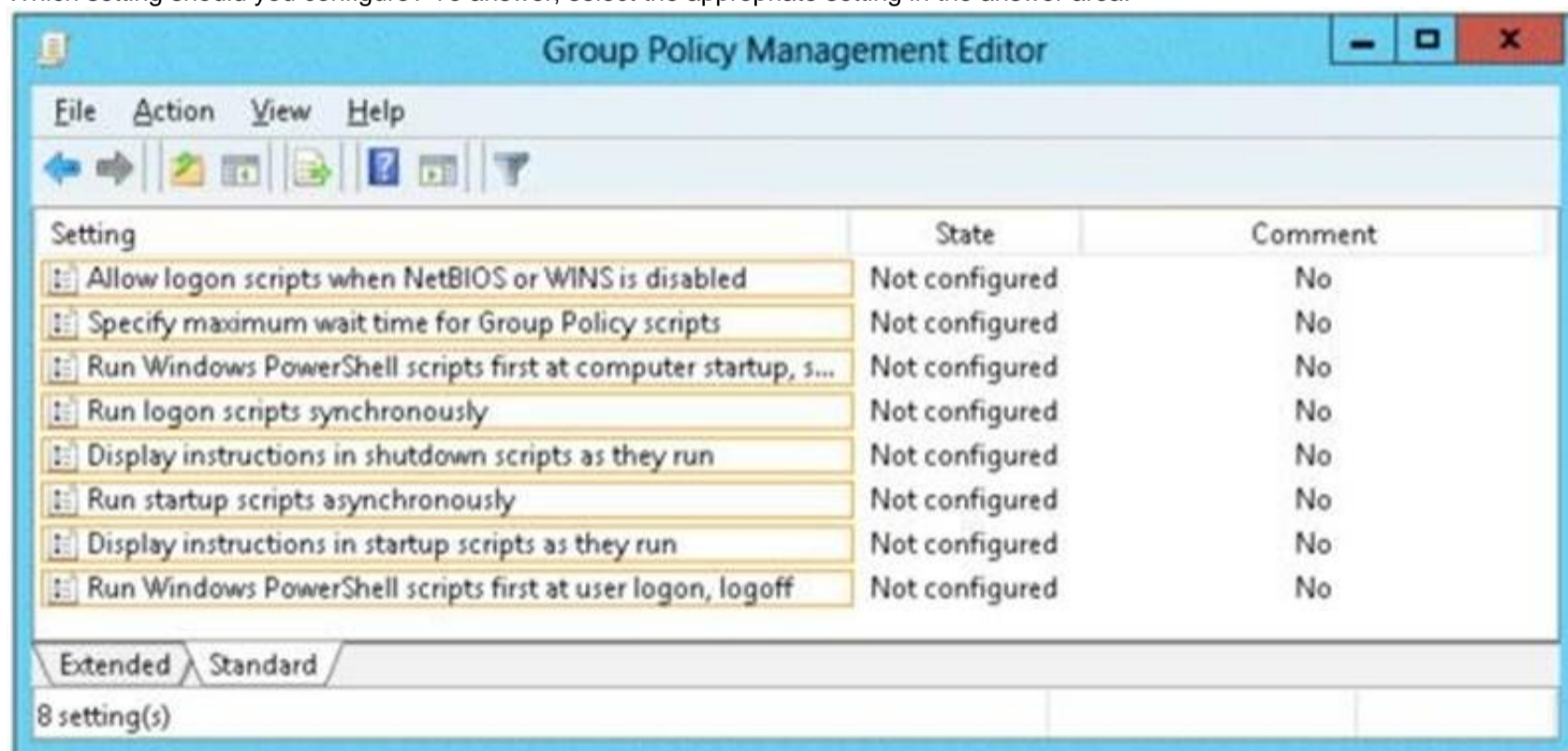
HOTSPOT - (Topic 1)

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

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

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

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



A. Mastered

B. Not Mastered

Answer: A

Explanation:

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

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

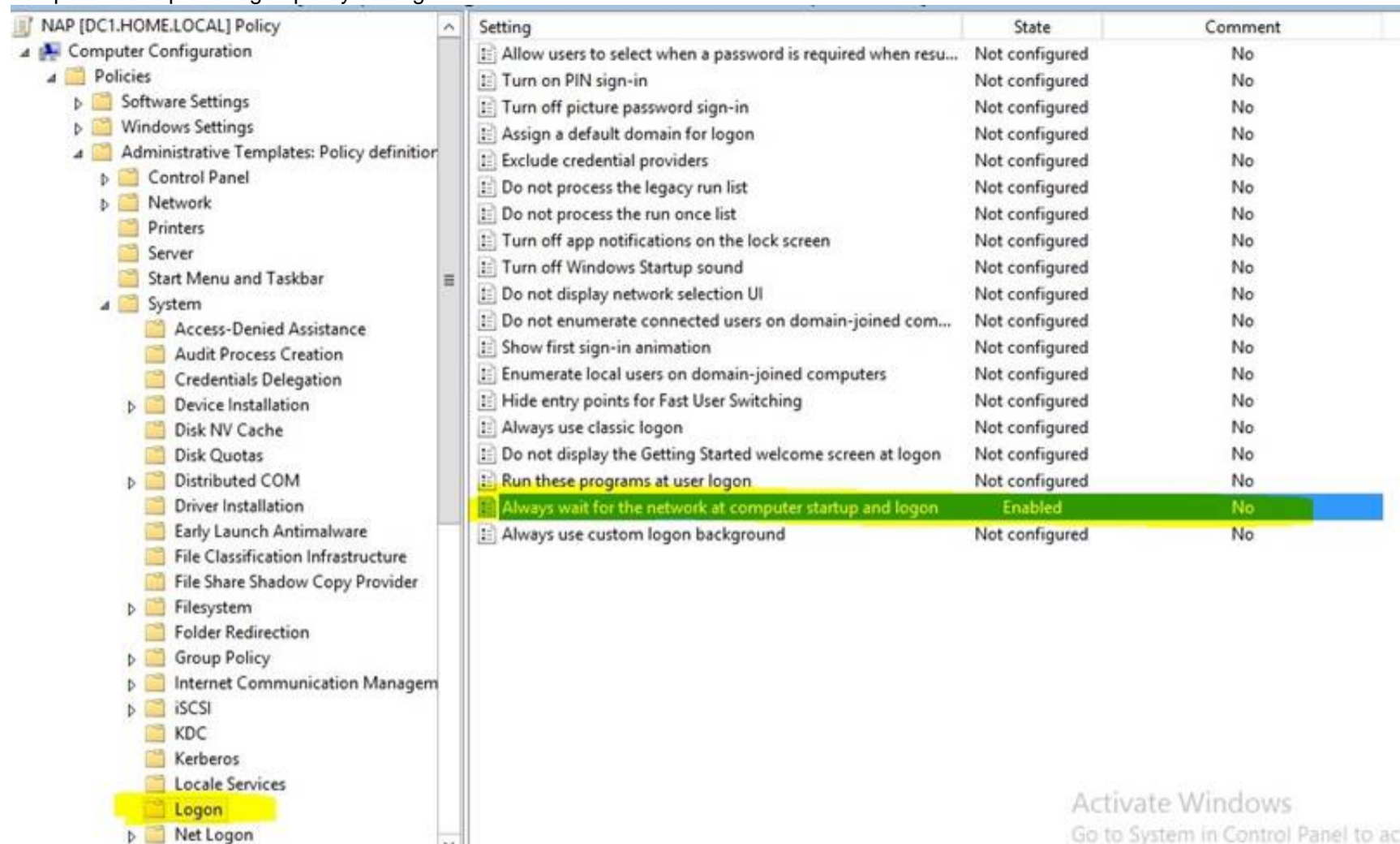
If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.

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

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

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

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



References:

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

NEW QUESTION 87

HOTSPOT - (Topic 1)

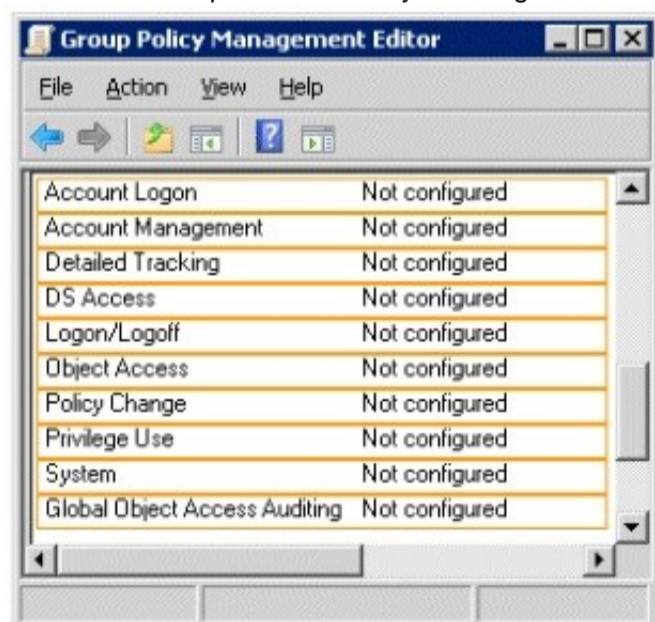
Your network contains an Active Directory domain named contoso.com.

You create an organizational unit (OU) named OU1 and a Group Policy object (GPO) named GPO1. You link GPO1 to OU1.

You move several file servers that store sensitive company documents to OU1. Each file server contains more than 40 shared folders.

You need to audit all of the failed attempts to access the files on the file servers in OU1. The solution must minimize administrative effort.

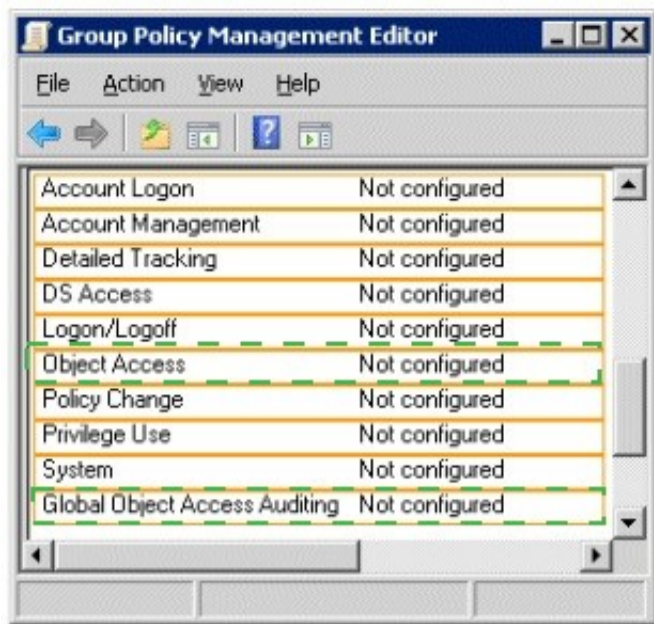
Which two audit policies should you configure in GPO1? To answer, select the appropriate two objects in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 90

- (Topic 1)

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

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

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

What should you do?

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

Answer: A

Explanation:

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

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

2. Start group policy by running the following command:

%SYSTEMROOT%\System32\gpedit. msc.

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

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

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

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

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

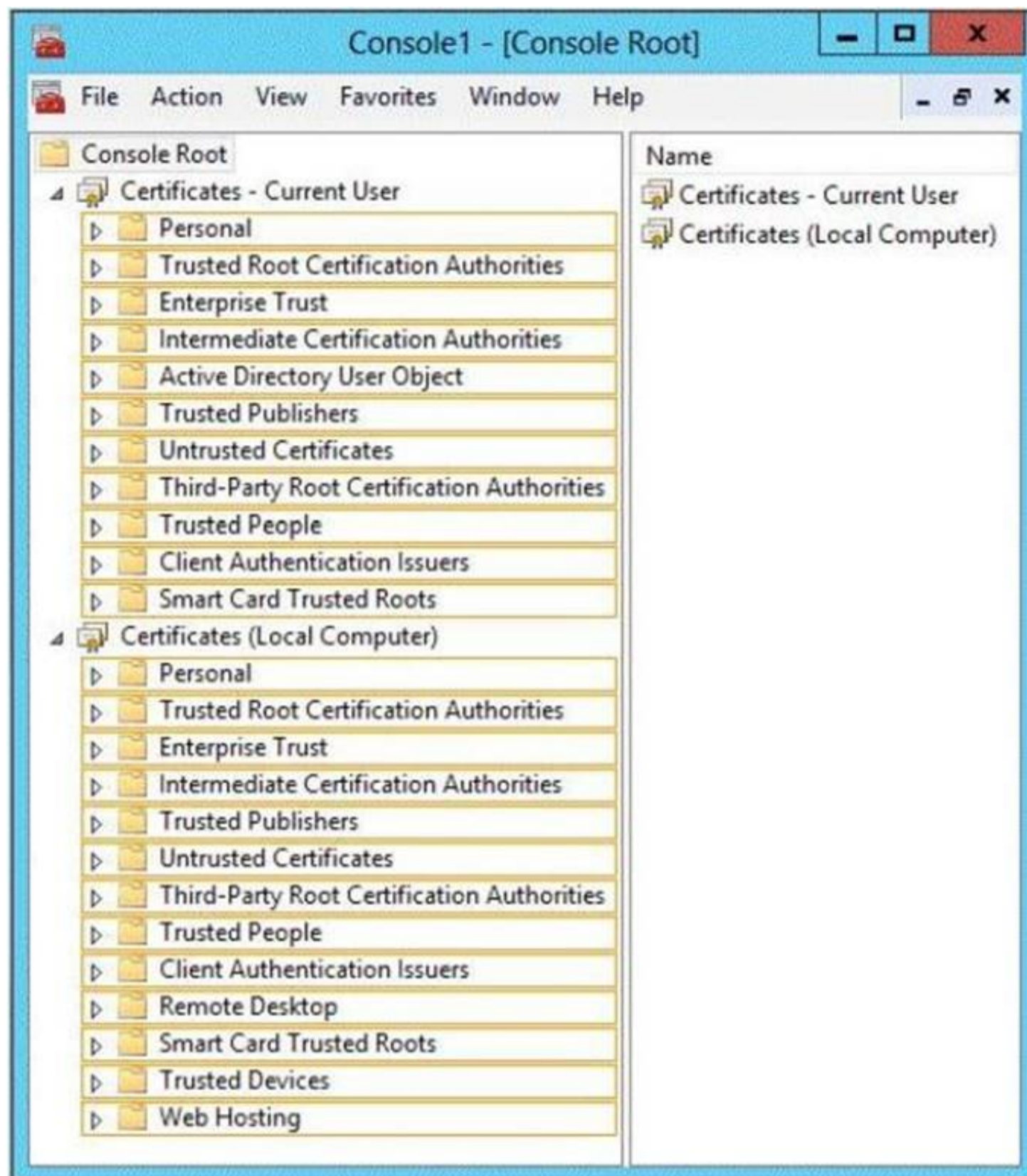
NEW QUESTION 93

HOTSPOT - (Topic 1)

You have a server named Server1 that has the Web Server (IIS) server role installed. You obtain a Web Server certificate.

You need to configure a website on Server1 to use Secure Sockets Layer (SSL).

To which store should you import the certificate? To answer, select the appropriate store in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

[http://technet.microsoft.com/en-us/library/cc740068\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc740068(v=ws.10).aspx)

When you enable secure communications (SSL and TLS) on an Internet Information Services (IIS) computer, you must first obtain a server certificate.

If it is a Self-Signed certificate, it only can be used on the local server machine.

If it is a public certificate, you'll need to download the CA root certificate of the certificate and install the CA root certificate into the Trusted Root Certificate Authorities store.

Root certificates provide a level of trust that certificates that are lower in the hierarchy can inherit. Each certificate is inspected for a parent certificate until the search reaches the root certificate.

For more information about certificate, please refer to: References:

<http://technet.microsoft.com/en-us/library/cc700805.aspx> <http://support.microsoft.com/kb/232137/en-us>

http://www.sqlservermart.com/HowTo/Windows_Import_Certificate.aspx

<http://msdn.microsoft.com/en-us/library/windows/hardware/ff553506%28v=vs.85%29.aspx>

<http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis>

<http://support.microsoft.com/kb/299875/en-us>

<http://technet.microsoft.com/en-us/library/dd163531.aspx>

<http://blogs.msdn.com/b/mosharaf/archive/2006/10/30/using-test-certificate-with-reporting-services-2005-to-establish-ssl-connection.aspx>

NEW QUESTION 95

- (Topic 2)

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

You enable and configure Routing and Remote Access (RRAS) on Server1. You create a user account named User1.

You need to ensure that User1 can establish VPN connections to Server1. What should you do?

- A. Create a network policy.
- B. Create a connection request policy.
- C. Add a RADIUS client.

D. Modify the members of the Remote Management Users group.

Answer: A

Explanation:

Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

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



References:

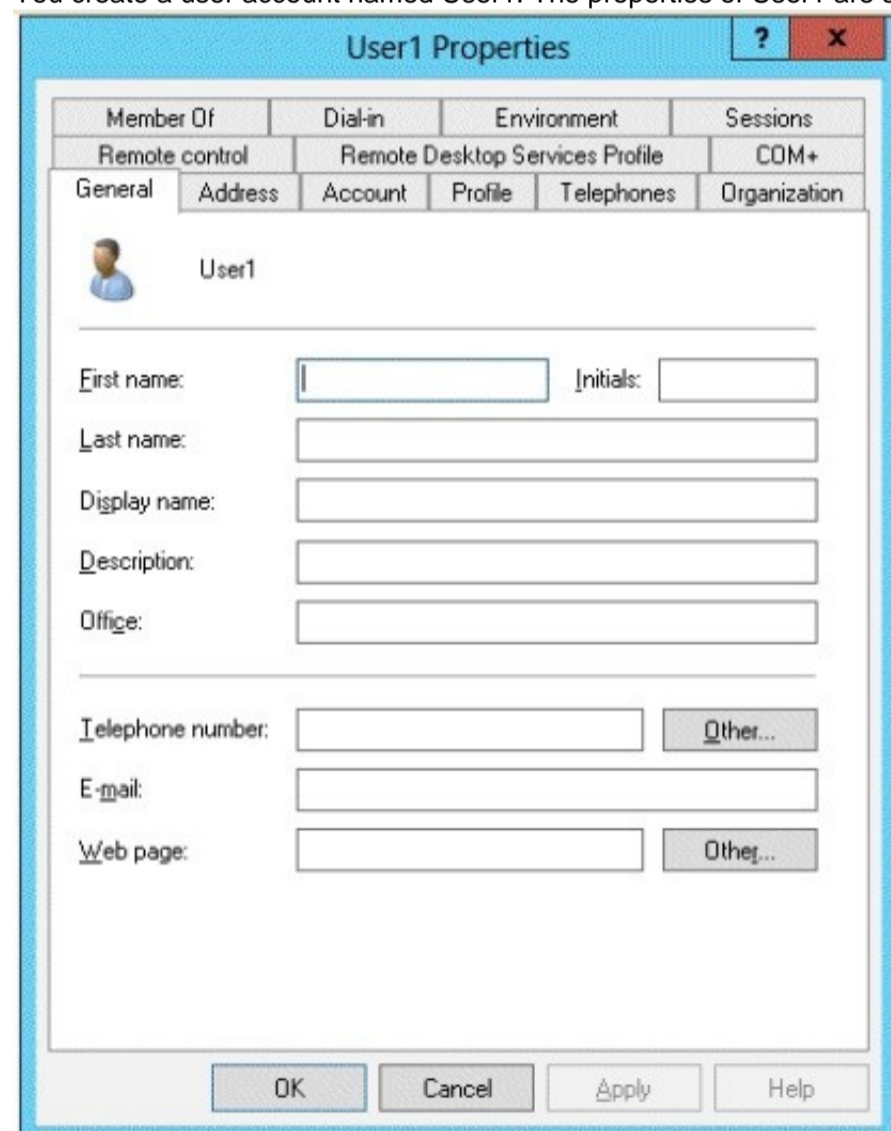
<http://technet.microsoft.com/en-us/library/hh831683.aspx>
<http://technet.microsoft.com/en-us/library/cc754107.aspx>
<http://technet.microsoft.com/en-us/library/dd314165%28v=ws.10%29.aspx>
<http://technet.microsoft.com/en-us/windowsserver/dd448603.aspx>
[http://technet.microsoft.com/en-us/library/dd314165\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/libr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

NEW QUESTION 99

- (Topic 2)

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

You create a user account named User1. The properties of User1 are shown in the exhibit. (Click the Exhibit button.)



You plan to use the User1 account as a service account. The service will forward authentication requests to other servers.

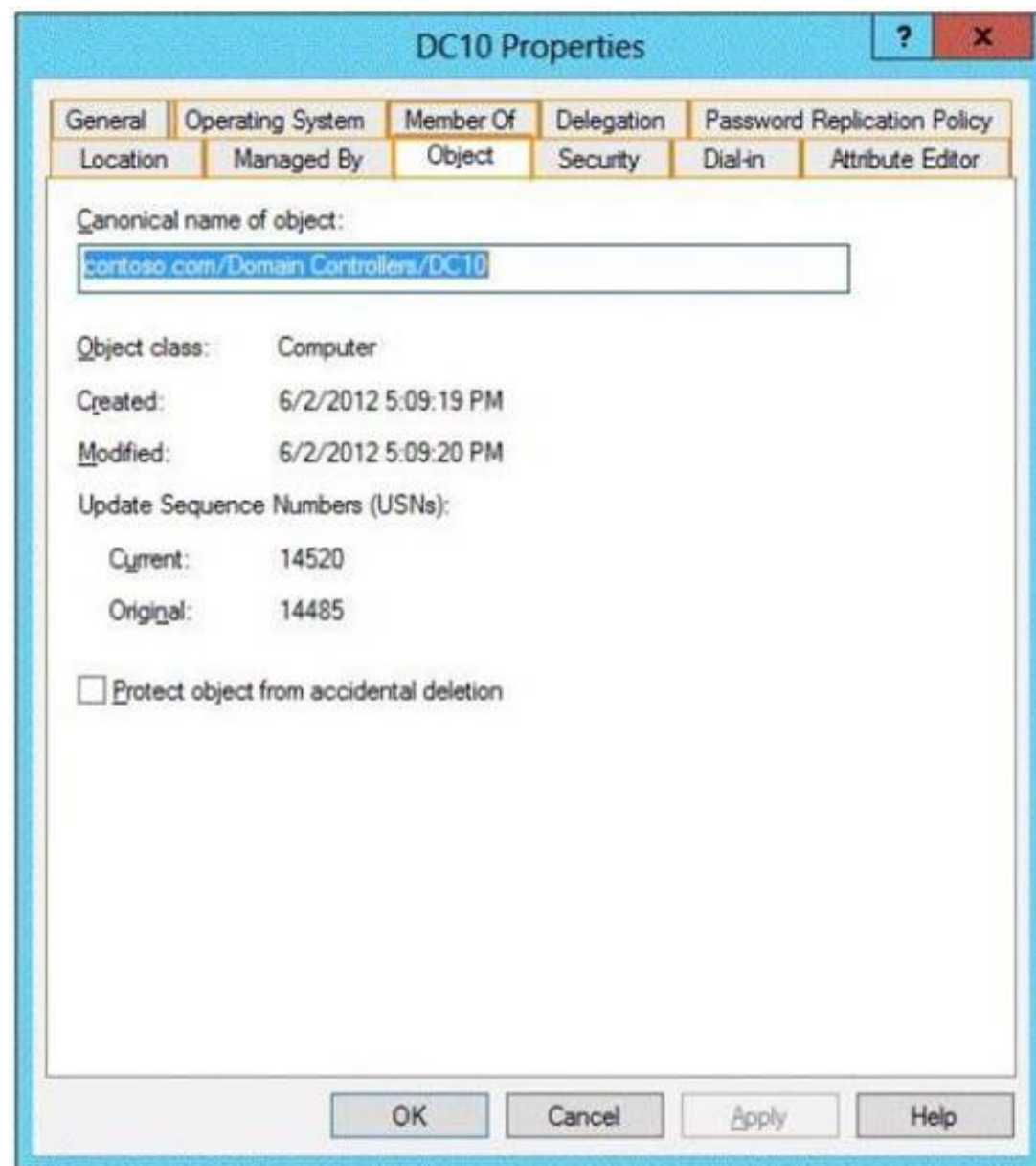
You need to ensure that you can view the Delegation tab from the properties of the User1 account.

What should you do first?

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

Answer: C

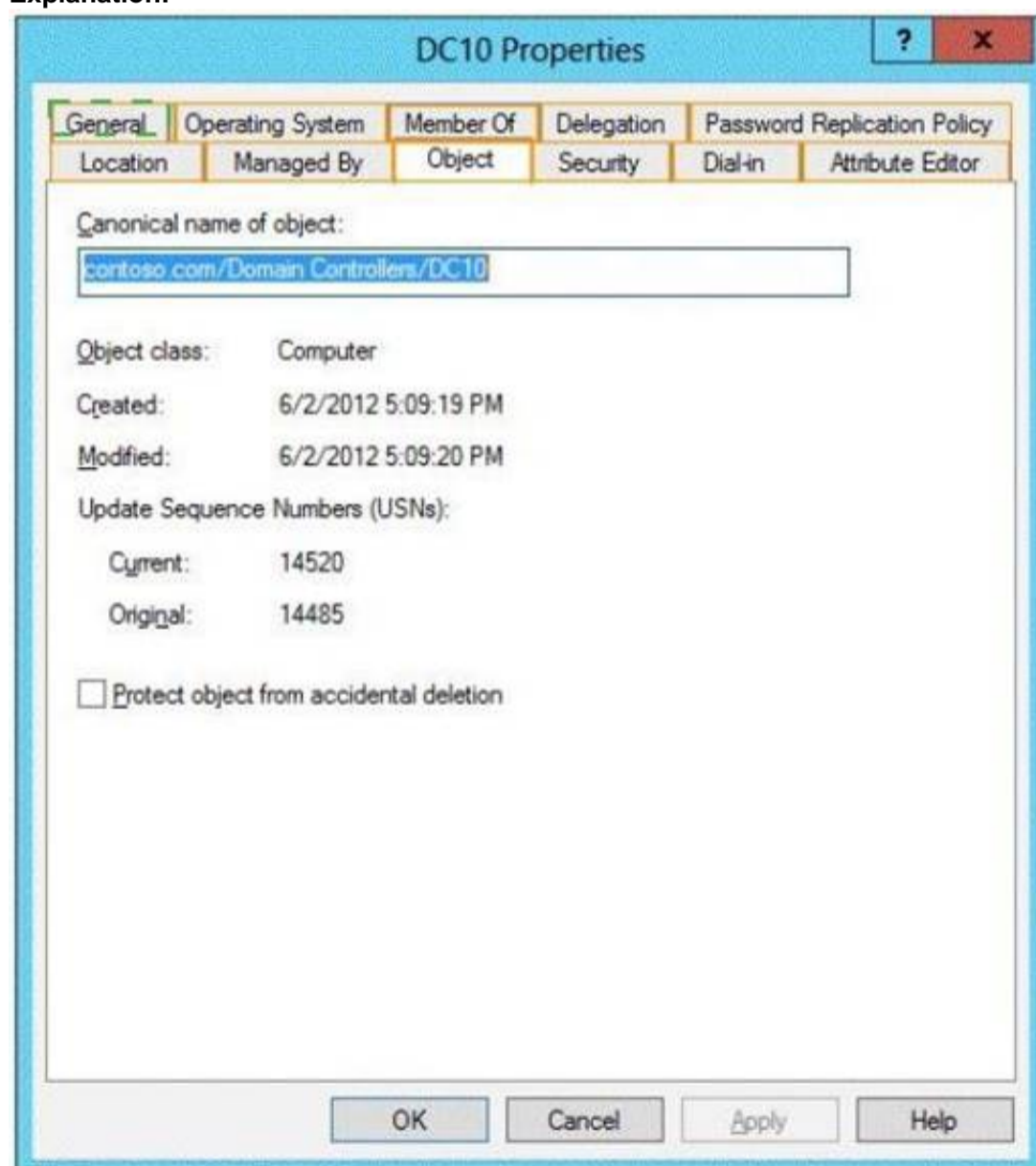
Explanation:



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 102

- (Topic 2)

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

A domain controller named DC1 runs Windows Server 2012 R2. DC1 is backed up daily. During routine maintenance, you delete a group named Group1. You need to recover Group1 and identify the names of the users who were members of Group1 prior to its deletion. You want to achieve this goal by using the minimum amount of administrative effort. What should you do first?

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 106

- (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.)

The screenshot shows the 'Remote Access Setup' wizard, 'Infrastructure Server Setup' step, 'DNS' configuration page. The page title is 'Remote Access Setup' and the subtitle is 'Infrastructure Server Setup'. The main instruction is 'Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.' The left sidebar shows 'Network Location Server', 'DNS' (selected), 'DNS Suffix Search List', and 'Management'. The main content area has a text box explaining DNS suffixes and a table with columns 'Name Suffix' and 'DNS Server Address'. The table contains two entries: 'contoso.com' with '2002:c1a8:6a:3333::1' and 'server5.contoso.com' with a blank address. Below the table is a section 'Select a local name resolution option:' with three radio buttons: '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)' (selected), and 'Use local name resolution for any kind of DNS resolution error (least restrictive)'. At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

Name Suffix	DNS Server Address
contoso.com	2002:c1a8:6a:3333::1
server5.contoso.com	
*	

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

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:

//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](http://www.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 111

- (Topic 2)

Your network contains an Active Directory domain named [contoso.com](http://www.contoso.com). The domain contains a server named Server1 that runs Windows Server 2012 R2 and has the Network Policy Server role service installed.

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

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

Answer: D

Explanation:

NPS trace logging files

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

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

The following log files contain helpful information about NAP:

IASNAP. LOG: Contains detailed information about NAP processes, NPS authentication, and NPS authorization.

IASSAM. LOG: Contains detailed information about user authentication and authorization.

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

To create tracing log files on a server running NPS

? Open a command line as an administrator.

? Type `netshras set tr * en`.

? Reproduce the scenario that you are troubleshooting.

? Type `netshras set tr * dis`.

? Close the command prompt window.

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

NEW QUESTION 113

- (Topic 2)

Your network contains an Active Directory domain named [contoso.com](http://www.contoso.com). Domain controllers run either Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 R2.

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 117

- (Topic 2)

Your network contains an Active Directory domain named [contoso.com](http://www.contoso.com). All domain controllers run Windows Server 2012 R2.

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

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

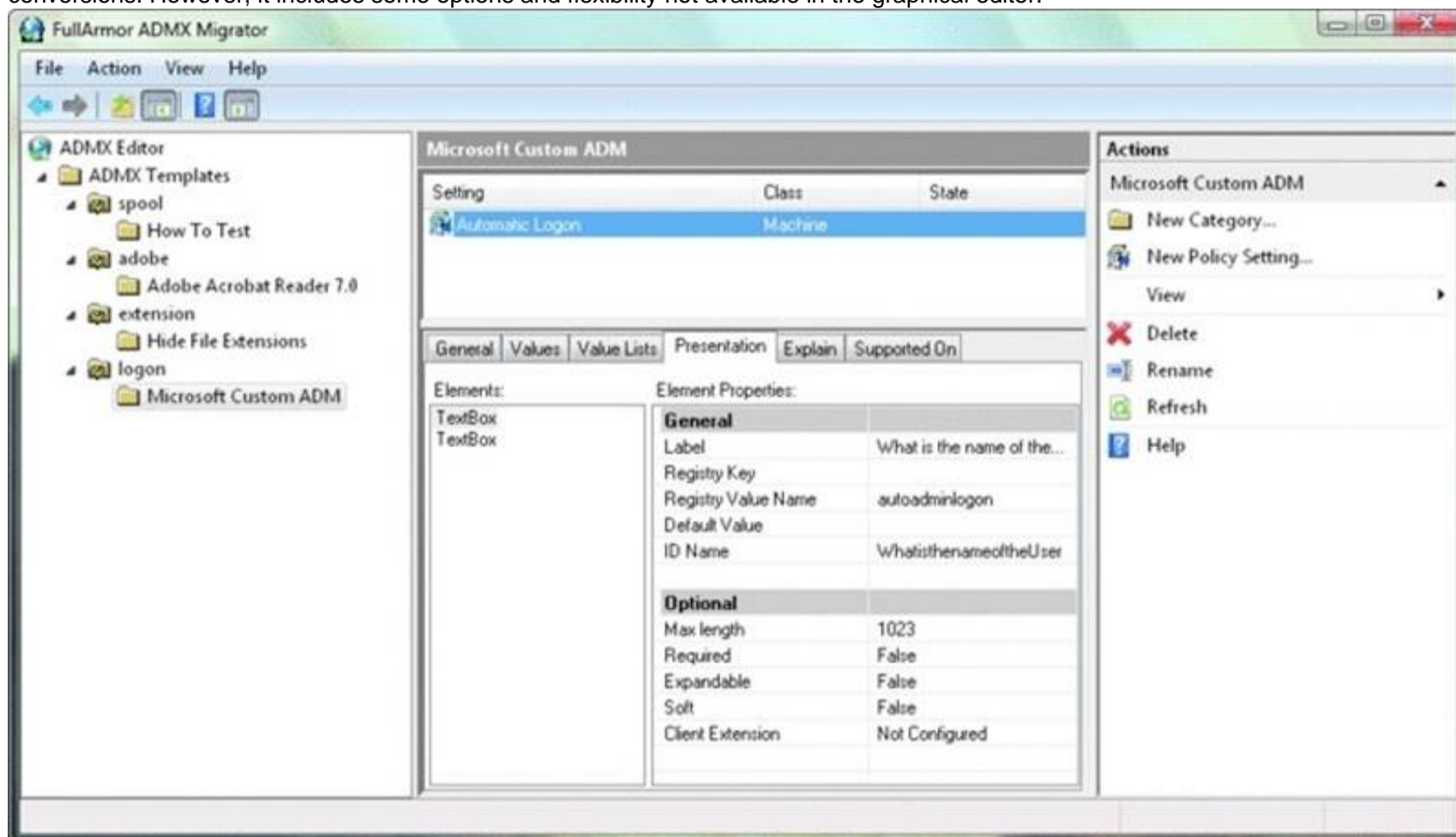
Which action should you run first?

- A. Load Template
- B. New Policy Setting
- C. Generate ADMX from ADM
- D. New Category

Answer: C

Explanation:

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



References:

<http://technet.microsoft.com/pt-pt/magazine/2008.02.utilityspotlight%28en-us%29.aspx> <http://technet.microsoft.com/pt-pt/magazine/2008.02.utilityspotlight%28en-us%29.aspx>

NEW QUESTION 120

- (Topic 2)

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

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

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

What should you do from the Update Services console?

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

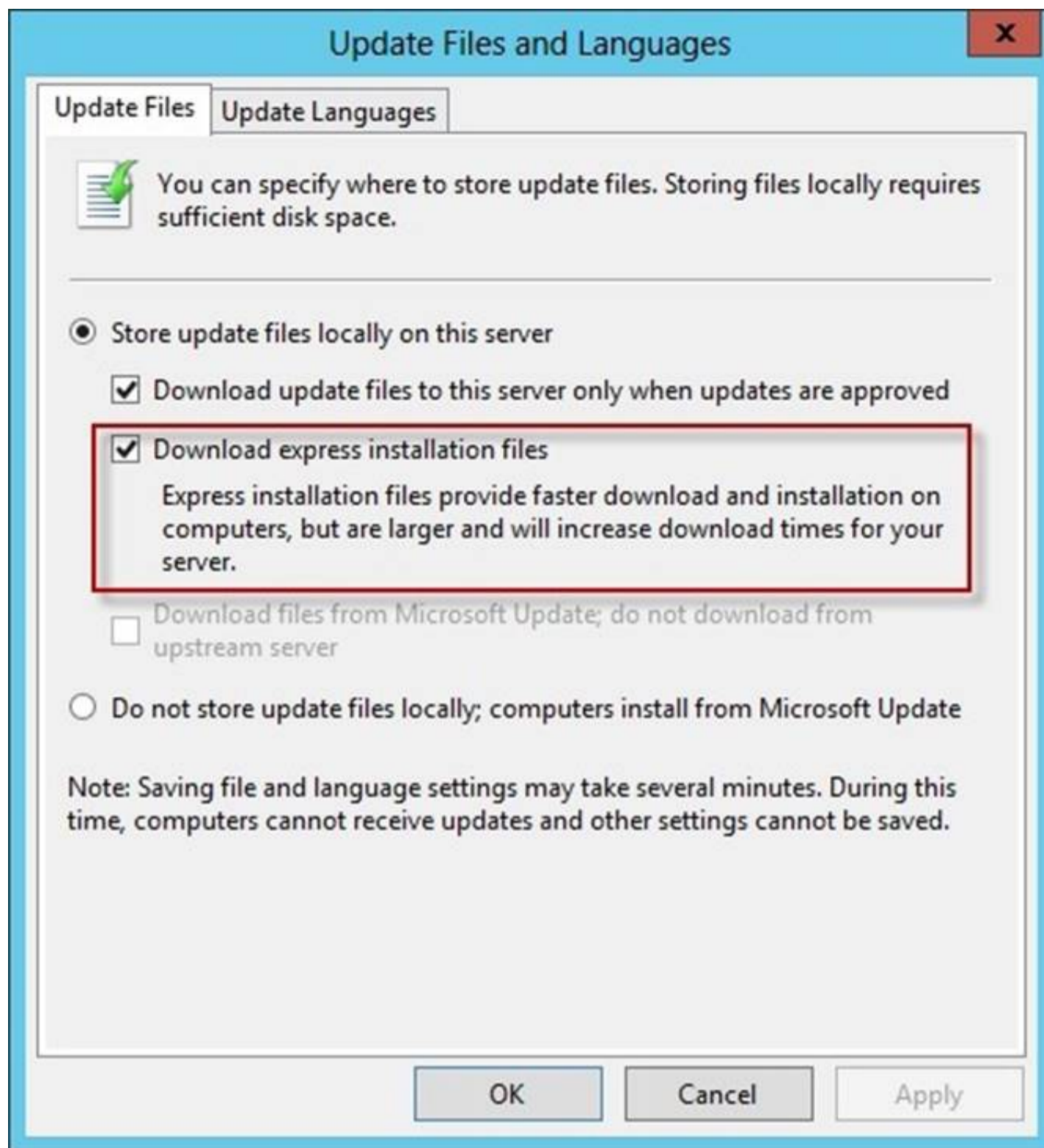
Answer: A

Explanation:

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

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

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



Reference:

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

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

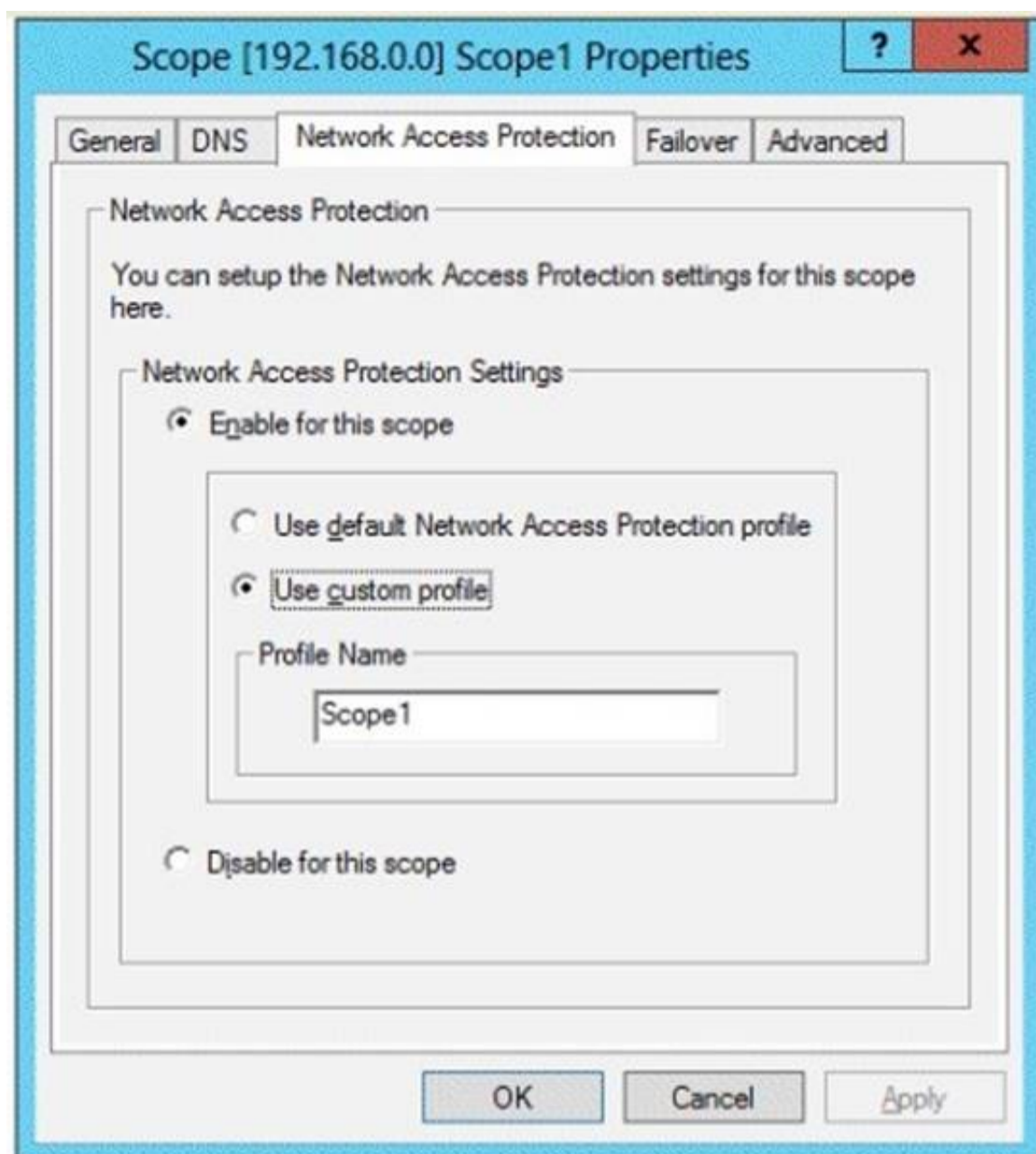
NEW QUESTION 124

- (Topic 2)

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

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

You modify the settings of Scope1 as shown in the exhibit. (Click the Exhibit button.)



You need to configure Server1 to provide unique NAP enforcement settings to the NAP non-compliant DHCP clients from Scope1. What should you create?

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

Answer: D

Explanation:

MS-Service Class

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

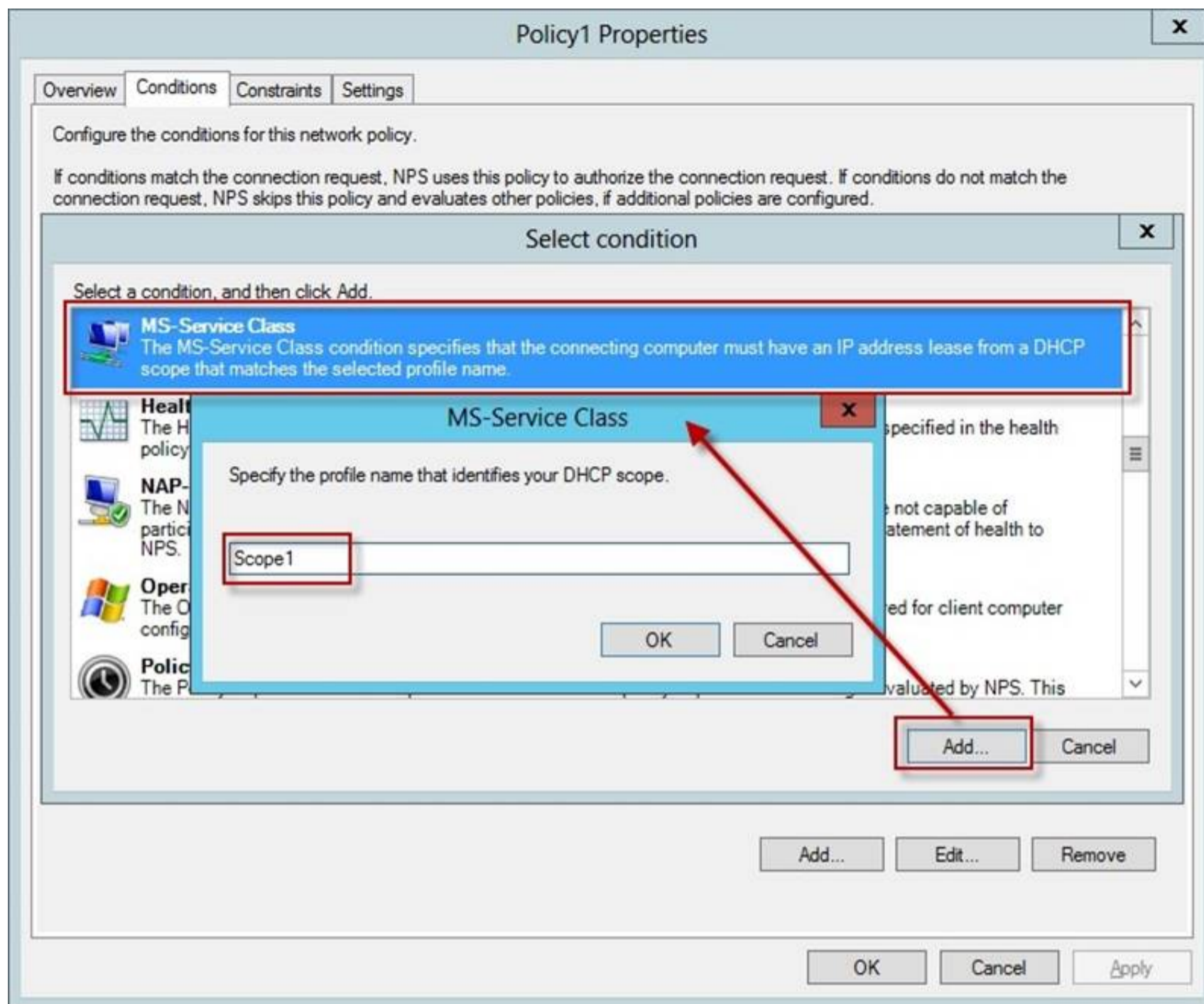
Open the NPS console, double-click Policies, click Network Policies, and then double-click the policy you want to configure.

In policy Properties, click the Conditions tab, and then click Add. In Select condition, scroll to the Network Access Protection group of conditions.

If you want to configure the Identity Type condition, click Identity Type, and then click Add. In Specify the method in which clients are identified in this policy, select the items appropriate for your deployment, and then click OK.

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

If you want to configure the MS-Service Class condition, click MS-Service Class, and then click Add. In Specify the profile name that identifies your DHCP scope, type the name of an existing DHCP profile, and then click Add.



The MS-Service Class condition restricts the policy to clients that have received an IP address from a DHCP scope that matches the specified DHCP profile name. This condition is used only when you are deploying NAP with the DHCP enforcement method.

References:

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

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

NEW QUESTION 128

- (Topic 2)

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

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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 132

HOTSPOT - (Topic 2)

Your network contains an Active Directory domain named contoso.com. All client computers are configured as DHCP clients.

You link a Group Policy object (GPO) named GPO1 to an organizational unit (OU) that contains all of the client computer accounts.

You need to ensure that Network Access Protection (NAP) compliance is evaluated on all of the client computers.

Which two settings should you configure in GPO1?

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 133

- (Topic 2)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 136

- (Topic 2)

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

You mount an Active Directory snapshot on DC1.

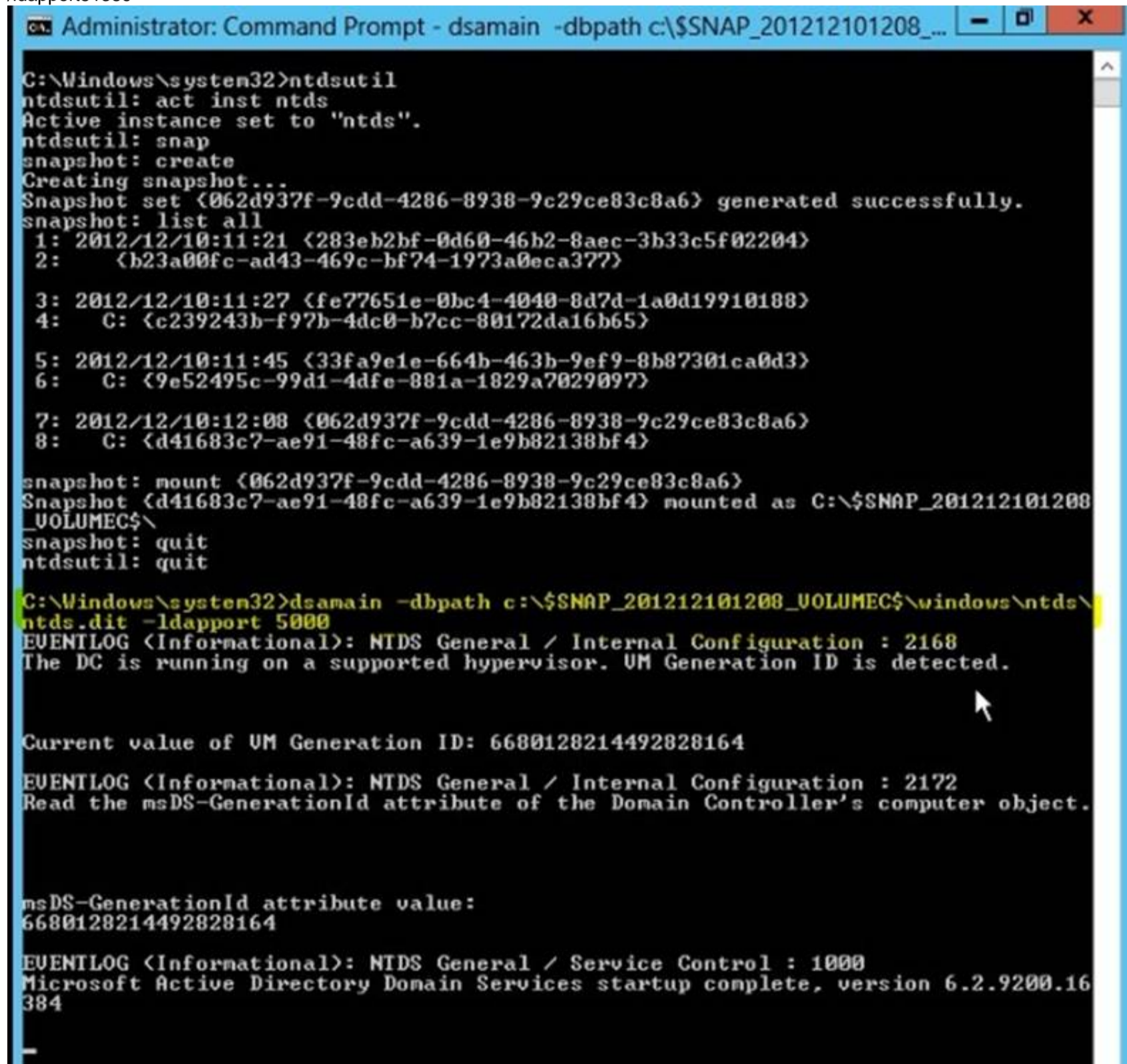
You need to expose the snapshot as an LDAP server. Which tool should you use?

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

Answer: C

Explanation:

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



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

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

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

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

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

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

Current value of VM Generation ID: 6680128214492828164

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

msDS-GenerationId attribute value:
6680128214492828164

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

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

NEW QUESTION 138

- (Topic 2)

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

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

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

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

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

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

- A. Create a replication connection.
- B. Create a namespace.

- C. Share and publish the replicated folder.
- D. Create a new topology.
- E. Modify the Referrals settings.

Answer: BCE

Explanation:

To share a replicated folder and publish it to a DFS namespace Click Start, point to Administrative Tools, and then click DFS Management. In the console tree, under the Replication node, click the replication group that contains the replicated folder you want to share. In the details pane, on the Replicated Folders tab, right-click the replicated folder that you want to share, and then click Share and Publish in Namespace. In the Share and Publish Replicated Folder Wizard, click Share and publish the replicated folder in a namespace, and then follow the steps in the wizard. Note that: If you do not have an existing namespace, you can create one in the Namespace Path page in the Share and Publish Replicated Folder Wizard. To create the namespace, in the Namespace Path page, click Browse, and then click New Namespace.

To create a namespace

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

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

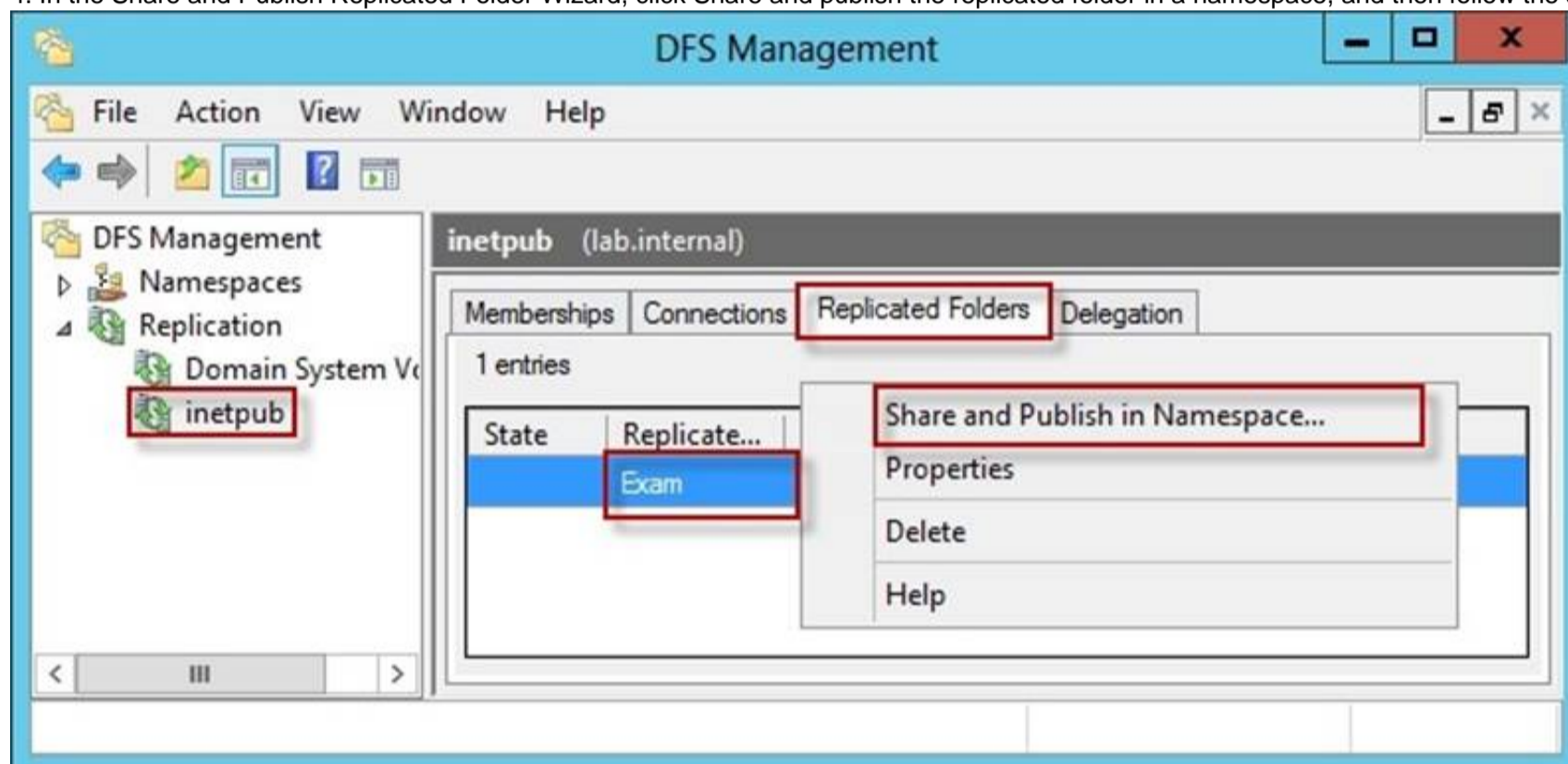
To create a stand-alone namespace on a failover cluster, specify the name of a clustered file server instance on the Namespace Server page of the New Namespace Wizard.

Important

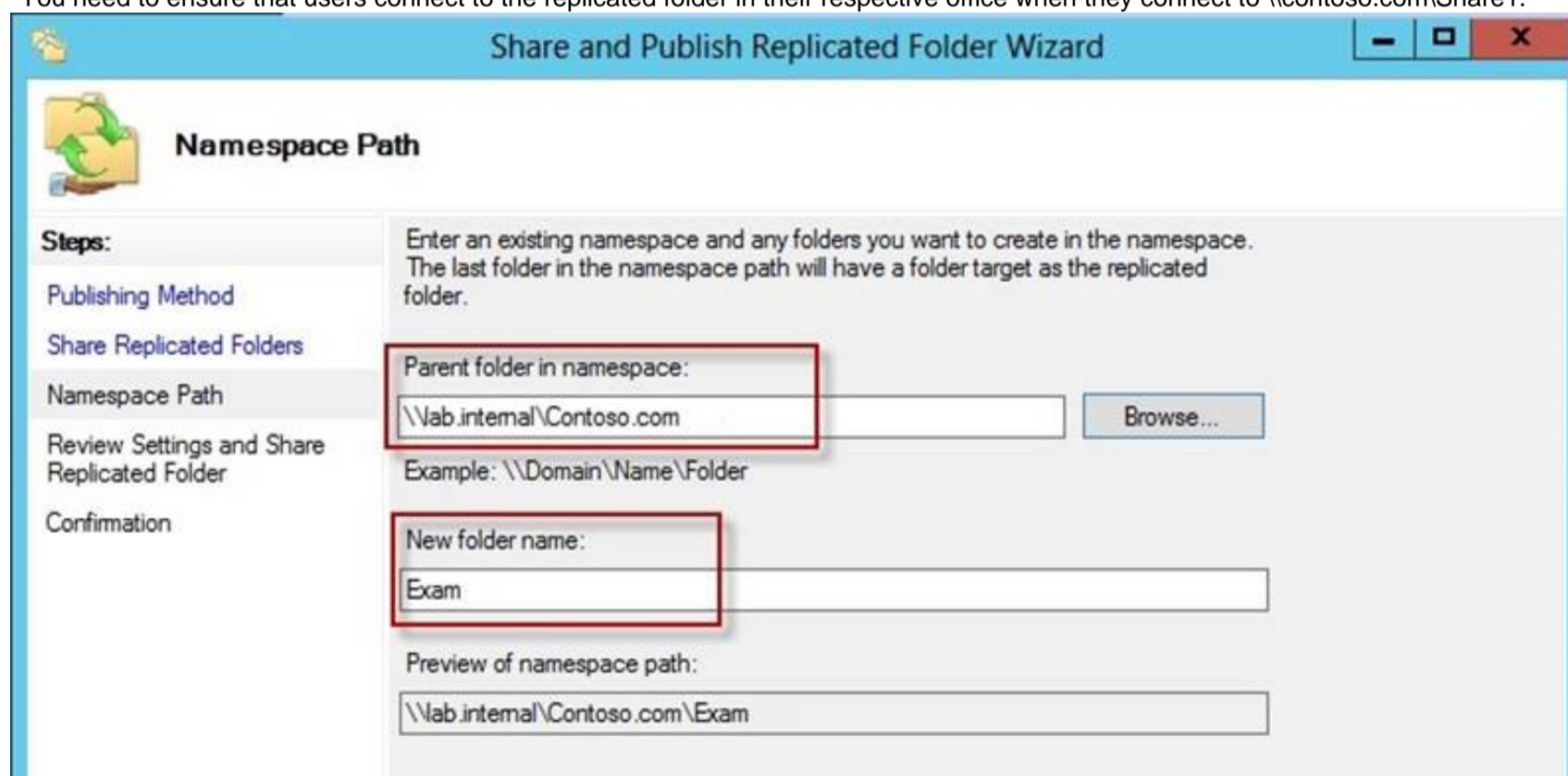
Do not attempt to create a domain-based namespace using the Windows Server 2008 mode unless the forest functional level is Windows Server 2003 or higher. Doing so can result in a namespace for which you cannot delete DFS folders, yielding the following error message: "The folder cannot be deleted. Cannot complete this function."

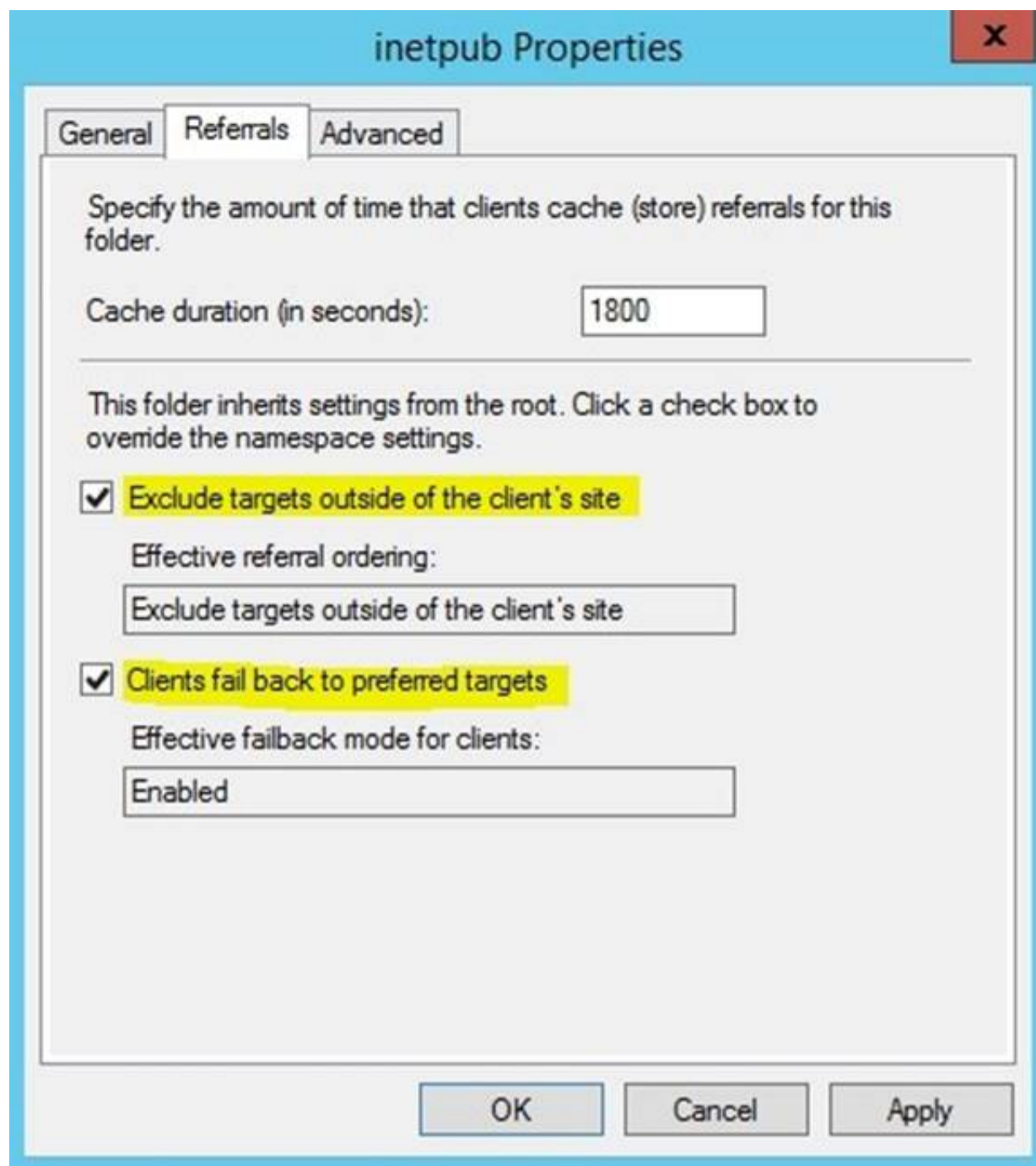
To share a replicated folder and publish it to a DFS namespace

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



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





Reference:

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

NEW QUESTION 141

- (Topic 2)

Your network contains three Network Policy Server (NPS) servers named NPS1, NPS2, and NPS3. NP51 is configured as a RADIUS proxy that forwards connection requests to a remote RADIUS server group named Group1. You need to ensure that NPS2 receives connection requests. NPS3 must only receive connection requests if NPS2 is unavailable. How should you configure Group1?

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

Answer: A

Explanation:

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

NEW QUESTION 146

HOTSPOT - (Topic 2)

Your network contains 25 Web servers that run Windows Server 2012 R2. You need to configure auditing policies that meet the following requirements:

- ? Generate an event each time a new process is created.
- ? Generate an event each time a user attempts to access a file share.

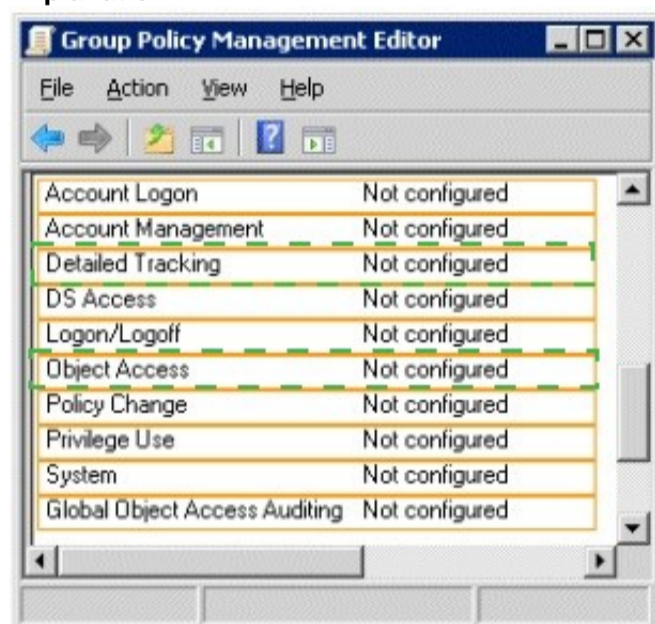
Which two auditing policies should you configure? To answer, select the appropriate two auditing policies in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

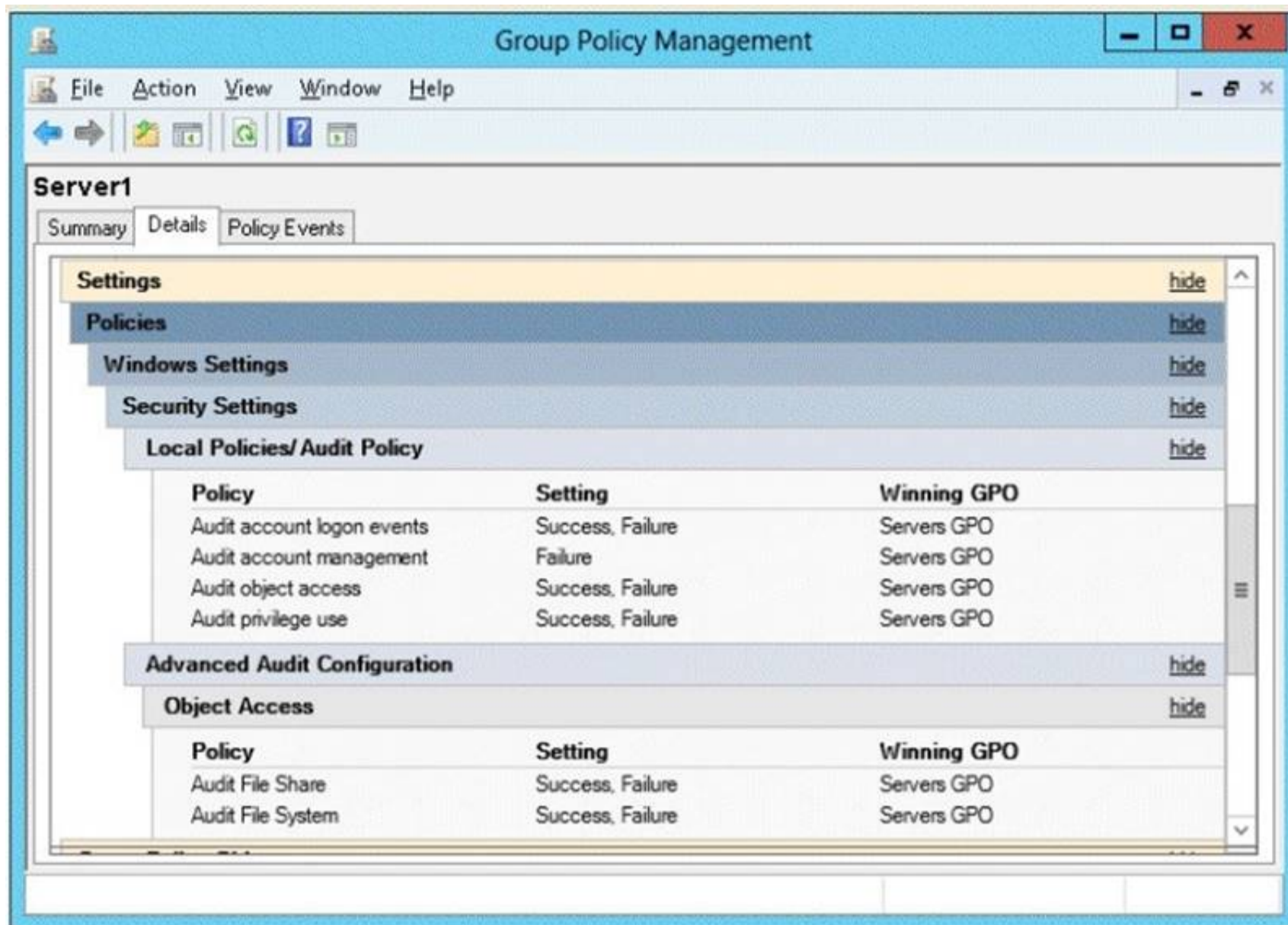
Explanation:



NEW QUESTION 149

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2012 R2. You view the effective policy settings of Server1 as shown in the exhibit. (Click the Exhibit button.)



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

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

Answer: A

Explanation:

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

Enabling Advanced Audit Policy Configuration

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

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

Audit Policy settings

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

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

Advanced Audit Configuration Settings

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

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

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

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

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

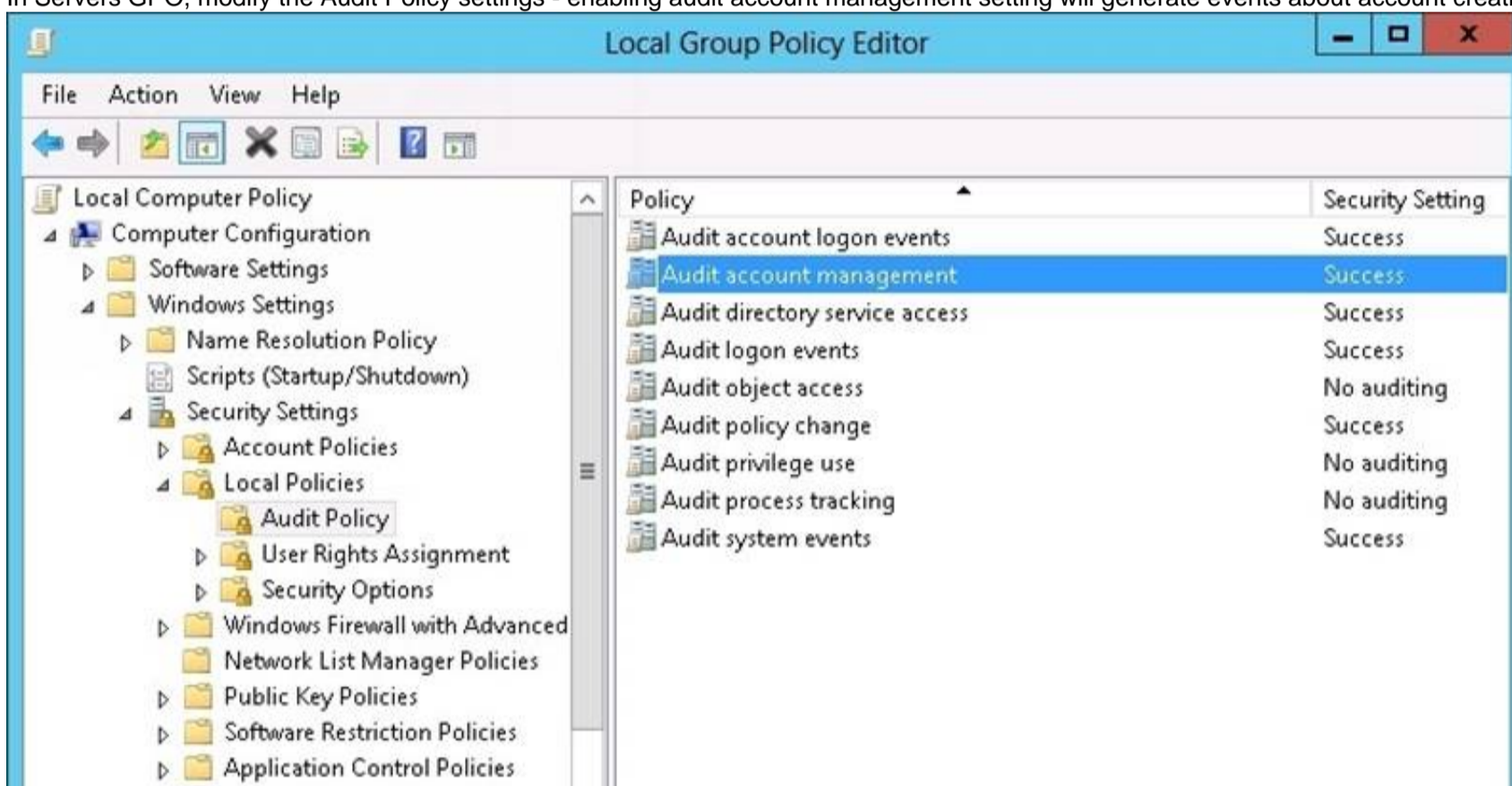
Advanced Audit Configuration Settings

Advanced Audit Configuration Settings -> Audit Policy

-> Account Management -> Audit User Account Management



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



ence:

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

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

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

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

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

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

NEW QUESTION 151

HOTSPOT - (Topic 2)

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

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

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

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

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

Answer Area

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

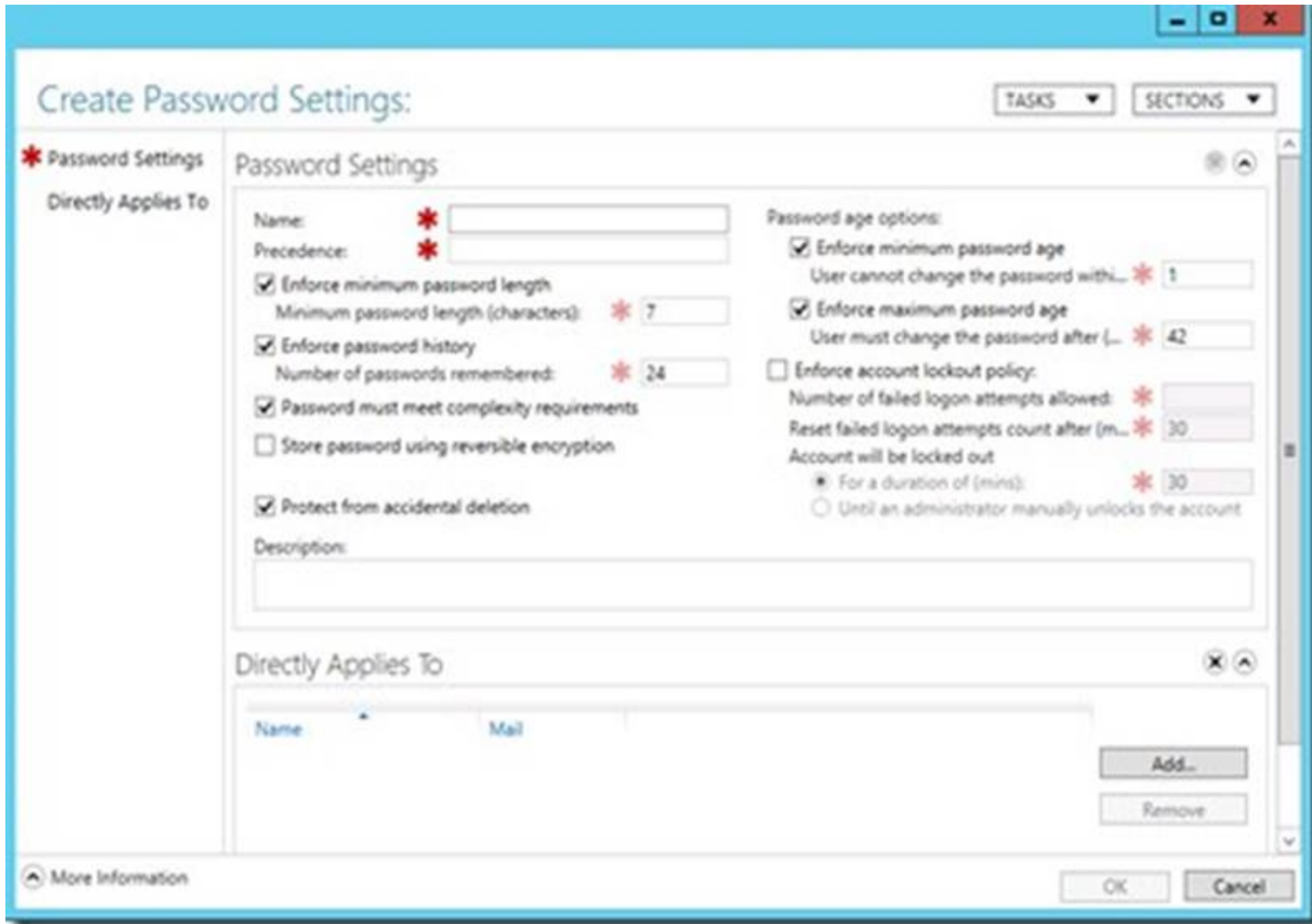
Box 1: PSO

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

Note:

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

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



NEW QUESTION 155

- (Topic 2)

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

You update several records on Server1.

You need to force the replication of the contoso.com zone records from Server1 to Server2. What should you do from Server2?

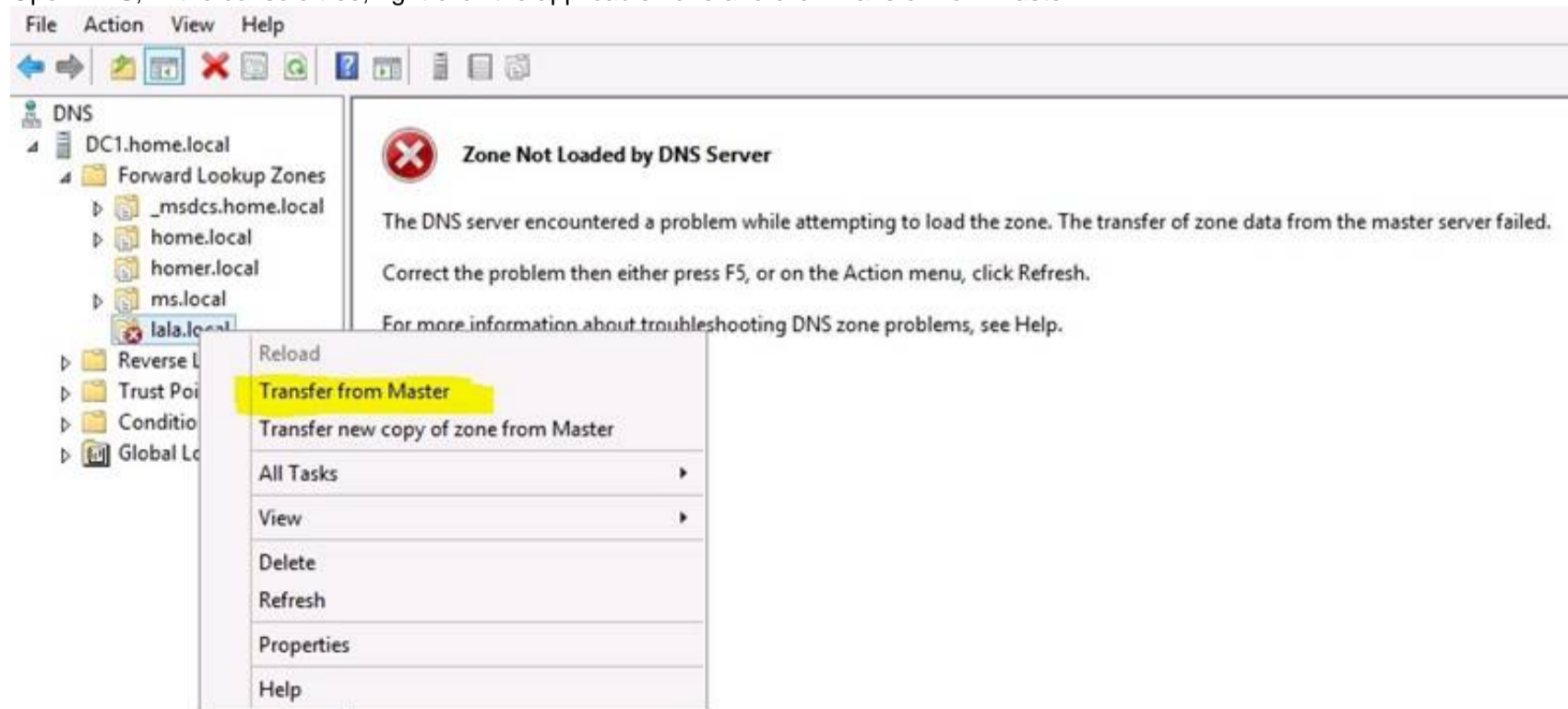
- A. Right-click the contoso.com zone and click Reload.
- B. Right-click the contoso.com zone and click Transfer from Master.
- C. Right-click Server2 and click Update Server Data Files.
- D. Right-click Server2 and click Refresh.

Answer: B

Explanation:

Initiates zone transfer from secondary server

Open DNS; In the console tree, right-click the applicable zone and click Transfer from master.



References:

- <http://technet.microsoft.com/en-us/library/cc779391%28v=ws.10%29.aspx>
- <http://technet.microsoft.com/en-us/library/cc779391%28v=ws.10%29.aspx>
- [http://technet.microsoft.com/en-us/library/cc786985\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc786985(v=ws.10).aspx)
- [http://technet.microsoft.com/en-us/library/cc779391\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc779391(v=ws.10).aspx)

NEW QUESTION 160

DRAG DROP - (Topic 2)

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

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

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

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

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

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

To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 162

- (Topic 2)

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

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

The network contains a server named Server1 that has the Hyper-V server role installed. DC6 is a virtual machine that is hosted on Server1. You need to ensure that you can clone DC6. What should you do?

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

Answer: D

Explanation:

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

```
Get-ADComputer (Get-ADDomainController –Discover –Service "PrimaryDC").name  
–Propertyoperatingsystemversion|fl
```

Reference: http://technet.microsoft.com/en-us/library/hh831734.aspx#steps_deploy_vdc

NEW QUESTION 166

- (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 Network Policy Server role service installed.

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

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

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

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

Answer: C

Explanation:

Configure NAP enforcement for VPN

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

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

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

NEW QUESTION 171

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. Network Access Protection (NAP) is deployed to the domain. You need to create NAP event trace log files on a client computer. What should you run?

- A. logman
- B. Register-ObjectEvent
- C. tracert
- D. Register-EngineEvent

Answer: A

Explanation:

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

To create NAP event trace log files on a client computer

? Open a command line as an administrator.

? Type

```
logman start QAgentRt -p {b0278a28-76f1-4e15-b1df-14b209a12613} 0xFFFFFFFF 9 -o
```

```
%systemroot%\tracing\nap\QAgentRt. etl –ets.
```

Note: To troubleshoot problems with WSHA, use the following GUID: 789e8f15-0cbf-4402- b0ed-0e22f90fdc8d.

? Reproduce the scenario that you are troubleshooting.

? Type logman stop QAgentRt -ets.

? Close the command prompt window.

References:

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

NEW QUESTION 176

- (Topic 2)

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.

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

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

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

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

Answer: BD

Explanation:

PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server.

When you use EAP with a strong EAP type, such as TLS with smart cards or TLS with certificates, both the client and the server use certificates to verify their identities to each other.

NEW QUESTION 177

HOTSPOT - (Topic 2)

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

You have two user accounts named User1 and User2. User1 and User2 are the members of a group named Group1. User1 has the Department value set to Accounting, user2 has the Department value set to Marketing. Both users have the Employee Type value set to Contract Employee.

You create the auditing entry as shown in the exhibit. (Click the Exhibit button.)

Auditing Entry for Global File SACL

Principal: Authenticated Users [Select a principal](#)

Type: All

Permissions:

- ☐ Full control
- ☐ Traverse folder / execute file
- ☒ List folder / read data
- ☐ Read attributes
- ☒ Read extended attributes
- ☐ Create files / write data
- ☐ Create folders / append data
- ☐ Write attributes
- ☐ Write extended attributes
- ☒ Delete subfolders and files
- ☒ Delete
- ☒ Read permissions
- ☒ Change permissions
- ☒ Take ownership
- ☐ Read
- ☐ Write
- ☐ Execute

[Clear all](#)

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

[Manage grouping](#)

User Department Not equals Value Accounting [Remove](#)

And

User Employee Type Equals Value Contract Employee [Remove](#)

[Add a condition](#)

[OK](#) [Cancel](#)

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

Answer Area

To ensure that an audit event is logged when User1 deletes files on Server1, you must ...

You must ... to ensure that an audit event is logged when User2 opens files on Server1.

Answer Area

To ensure that an audit event is logged when User1 deletes files on Server1, you must ...

- modify the Principal setting.
- modify the Permissions settings.
- modify the Employee Type setting.
- modify the condition for the Department va

You must ... to ensure that an audit event is logged when User2 opens files on Server1.

- add a condition
- modify the Principal setting
- modify the Permissions settings
- modify the condition for the Department va

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To ensure that an audit event is logged when User1 deletes files on Server1, you must ...

- modify the Principal setting.
- modify the Permissions settings.
- modify the Employee Type setting.
- modify the condition for the Department va

You must ... to ensure that an audit event is logged when User2 opens files on Server1.

- add a condition
- modify the Principal setting
- modify the Permissions settings
- modify the condition for the Department va

NEW QUESTION 179

- (Topic 2)

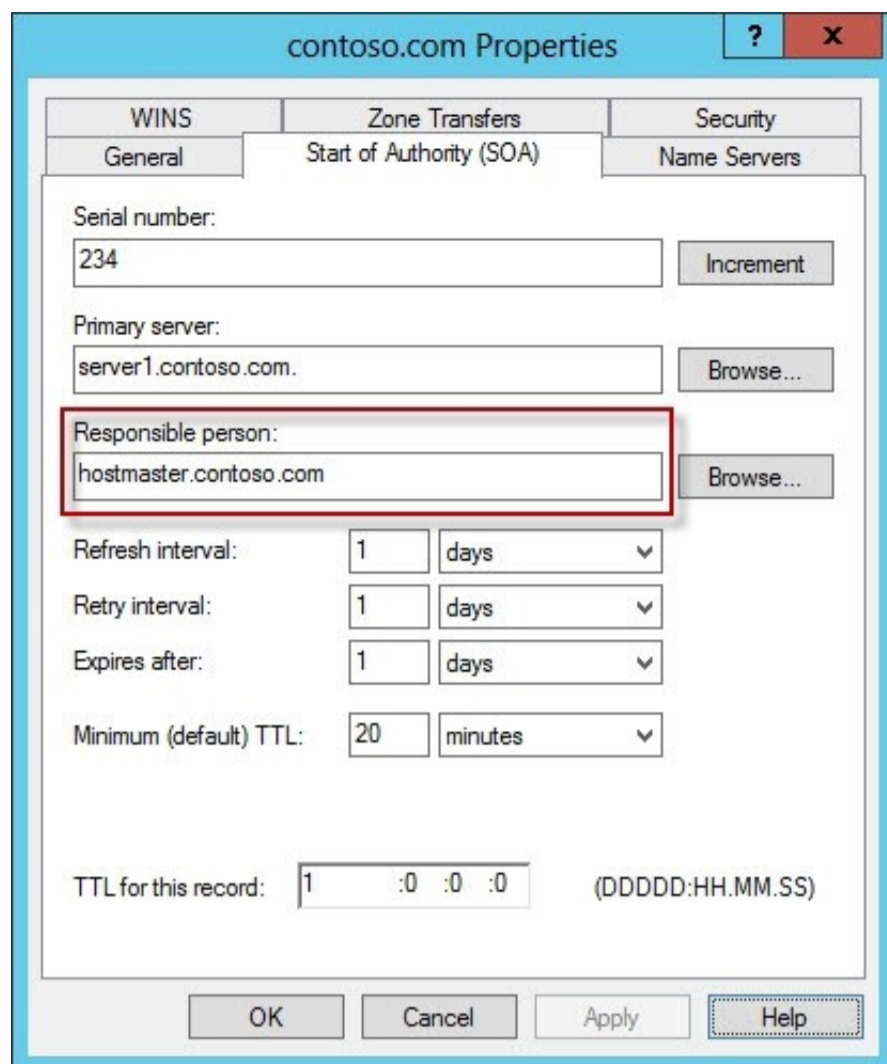
You have a DNS server named Server1 that runs Windows Server 2012 R2. On Server1, you create a DNS zone named contoso.com. You need to specify the email address of the person responsible for the zone. Which type of DNS record should you configure?

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

Answer: A

Explanation:

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



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

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

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

NEW QUESTION 184

- (Topic 2)

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

DirectAccess is implemented on Server1 by using the default configuration.

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

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

What should you do?

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

Answer: B

Explanation:

With IPv6 and the Name Resolution Policy Table (NRPT), by default, DirectAccess clients separate their intranet and Internet traffic as follows:

? DNS name queries for intranet fully qualified domain names (FQDNs) and all

intranet traffic is exchanged over the tunnels that are created with the DirectAccess server or directly with intranet servers. Intranet traffic from DirectAccess clients is IPv6 traffic.

? DNS name queries for FQDNs that correspond to exemption rules or do not match

the intranet namespace, and all traffic to Internet servers, is exchanged over the physical interface that is connected to the Internet. Internet traffic from DirectAccess clients is typically IPv4 traffic.

In contrast, by default, some remote access virtual private network (VPN) implementations, including the VPN client, send all intranet and Internet traffic over the remote access VPN

connection. Internet-bound traffic is routed by the VPN server to intranet IPv4 web proxy servers for access to IPv4 Internet resources. It is possible to separate the intranet and Internet traffic for remote access VPN clients by using split tunneling. This involves configuring the Internet Protocol (IP) routing table on VPN clients so that traffic to intranet locations is sent over the VPN connection, and traffic to all other locations is sent by using the physical interface that is connected to the Internet.

You can configure DirectAccess clients to send all of their traffic through the tunnels to the DirectAccess server with force tunneling. When force tunneling is

configured, DirectAccess clients detect that they are on the Internet, and they remove their IPv4 default route. With the exception of local subnet traffic, all traffic sent by the DirectAccess client is IPv6 traffic that goes through tunnels to the DirectAccess server.

NEW QUESTION 189

- (Topic 2)

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

All client computers run Windows 8 Enterprise.

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

You need to update the PATH variable on all of the client computers. Which Group Policy preference should you configure?

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

Answer: D

Explanation:

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

NEW QUESTION 193

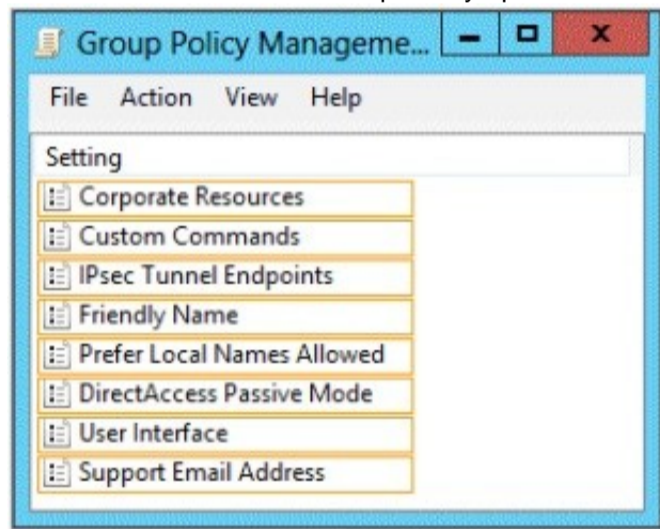
HOTSPOT - (Topic 2)

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1.

Your company implements DirectAccess.

A user named User1 works at a customer's office. The customer's office contains a server named Server1.

When User1 attempts to connect to Server1, User1 connects to Server1 in adatum.com. You need to provide User1 with the ability to connect to Server1 in the customer's office. Which Group Policy option should you configure? To answer, select the appropriate option in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Specifies whether the user has Connect and Disconnect options for the DirectAccess entry when the user clicks the Networking notification area icon.

If the user clicks the Disconnect option, NCA removes the DirectAccess rules from the Name Resolution Policy Table (NRPT) and the DirectAccess client computer uses whatever normal name resolution is available to the client computer in its current network configuration, including sending all DNS queries to the local intranet or Internet DNS servers. Note that NCA does not remove the existing IPsec tunnels and users can still access intranet resources across the DirectAccess server by specifying IPv6 addresses rather than names.

The ability to disconnect allows users to specify single-label, unqualified names (such as "PRINTSVR") for local resources when connected to a different intranet and for temporary access to intranet resources when network location detection has not correctly determined that the DirectAccess client computer is connected to its own intranet.

To restore the DirectAccess rules to the NRPT and resume normal DirectAccess functionality, the user clicks Connect.

Note: If the DirectAccess client computer is on the intranet and has correctly determined its network location, the Disconnect option has no effect because the rules for DirectAccess are already removed from the NRPT.

If this setting is not configured, users do not have Connect or Disconnect options.

NEW QUESTION 196

- (Topic 2)

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

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

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

What should you modify?

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

Answer: D

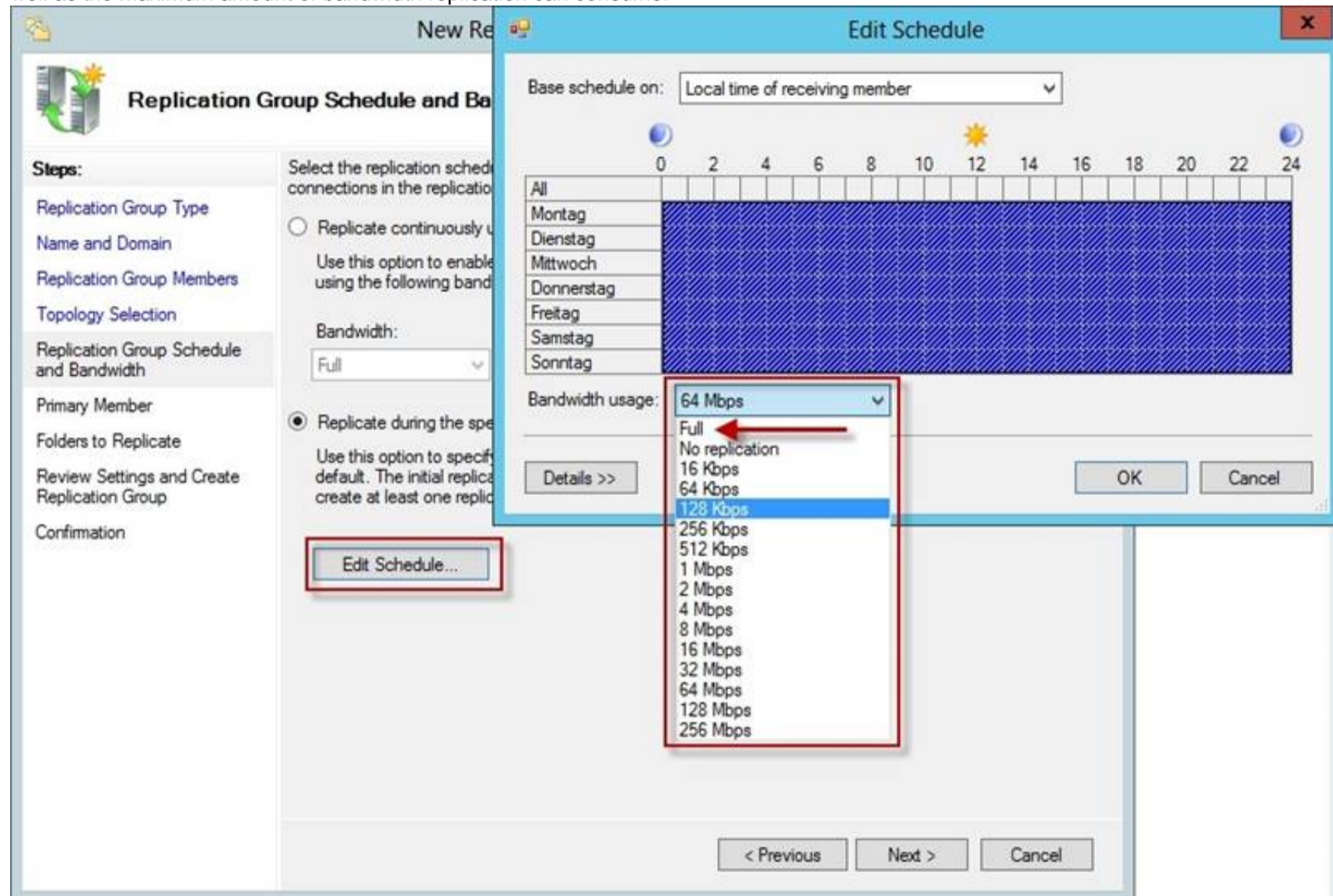
Explanation:

Scheduling allows less bandwidth the by limiting the time interval of the replication Does DFS Replication throttle bandwidth per schedule, per server, or per connection?

If you configure bandwidth throttling when specifying the schedule, all connections for that replication group will use that setting for bandwidth throttling. Bandwidth throttling can be also set as a connection-level setting using DFS Management.

To edit the schedule and bandwidth for a specific connection, use the following steps: In the console tree under the Replication node, select the appropriate replication group. Click the Connections tab, right-click the connection that you want to edit, and then click Properties.

Click the Schedule tab, select Custom connection schedule and then click Edit Schedule. Use the Edit Schedule dialog box to control when replication occurs, as well as the maximum amount of bandwidth replication can consume.



NEW QUESTION 198

- (Topic 2)

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

Administrators use client computers that run Windows 8 to perform all management tasks. A central store is configured on a domain controller named DC1.

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

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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 202

- (Topic 2)

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

Server1 has a dynamically expanding virtual hard disk that is mounted to drive E.

You need to ensure that you can enable BitLocker Drive Encryption (BitLocker) on drive E. Which command should you run?

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

Answer: D

Explanation:

Manage-bde: on

Encrypts the drive and turns on BitLocker. Example:

The following example illustrates using the -on command to turn on BitLocker for drive C and add a recovery password to the drive.

manage-bde -on C: -recoverypassword

NEW QUESTION 206

- (Topic 2)

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

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

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

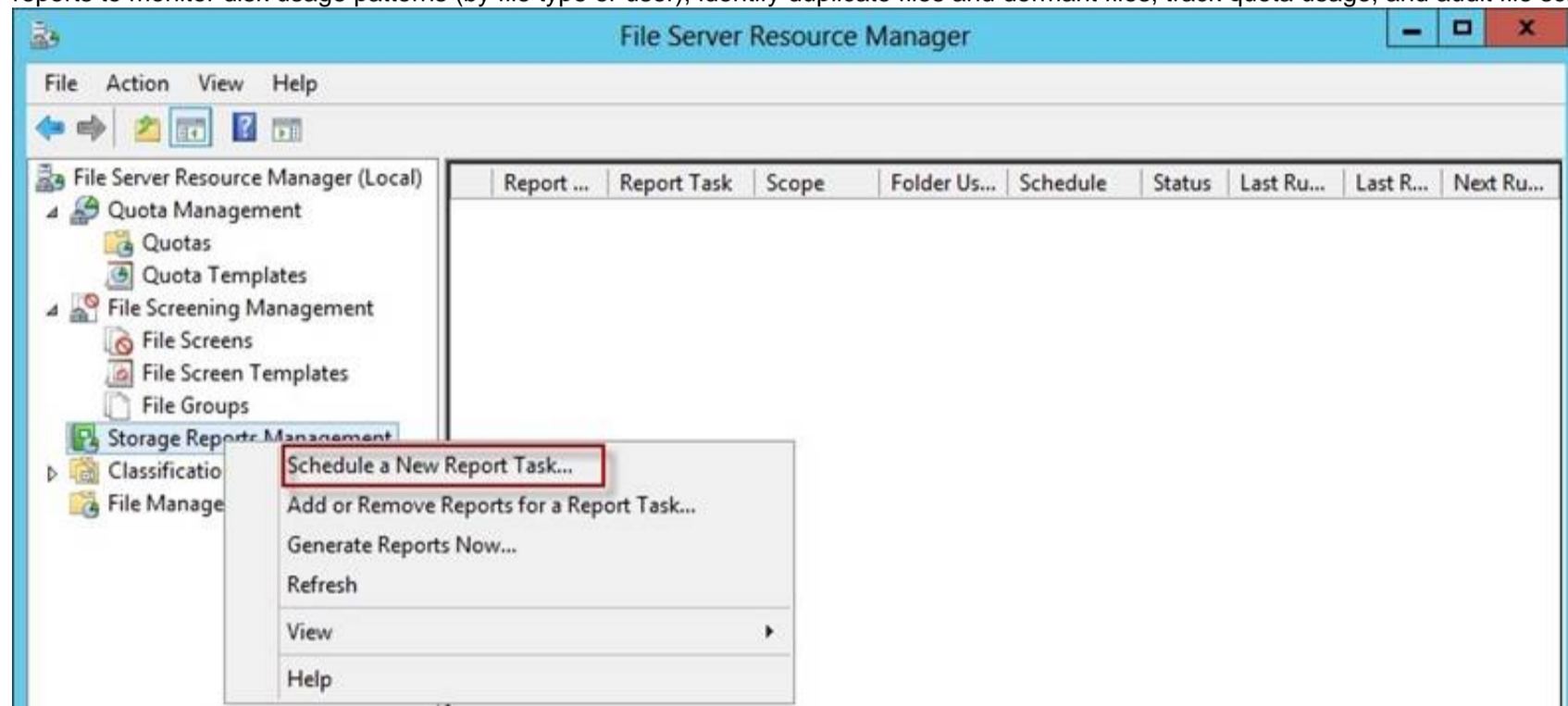
What should you configure on Server1?

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

Answer: D

Explanation:

From the Storage Reports Management node, you can generate reports that will help you understand file use on the storage server. You can use the storage reports to monitor disk usage patterns (by file type or user), identify duplicate files and dormant files, track quota usage, and audit file screening.



Before you run a File Screen Audit report, in the File Server Resource Manager Options dialog box, on the File Screen Audit tab, verify that the Record file screening activity in the auditing database check box is selected.

Reference:

<http://technet.microsoft.com/en-us/library/cc755988.aspx>

<http://technet.microsoft.com/en-us/library/cc730822.aspx>

<http://technet.microsoft.com/en-us/library/cc770594.aspx>

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

<http://technet.microsoft.com/en-us/library/cc732074.aspx>

NEW QUESTION 207

- (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 (%):
85

E-mail Message | Event Log | Command | Report

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

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

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

Subject:
[Quota Threshold]% quota threshold exceeded

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

Select variable to insert:
[Admin Email] ▼ Insert Variable
Inserts the e-mail addresses of the administrators who receive the e-mail.

Additional E-mail Headers...

OK Cancel

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

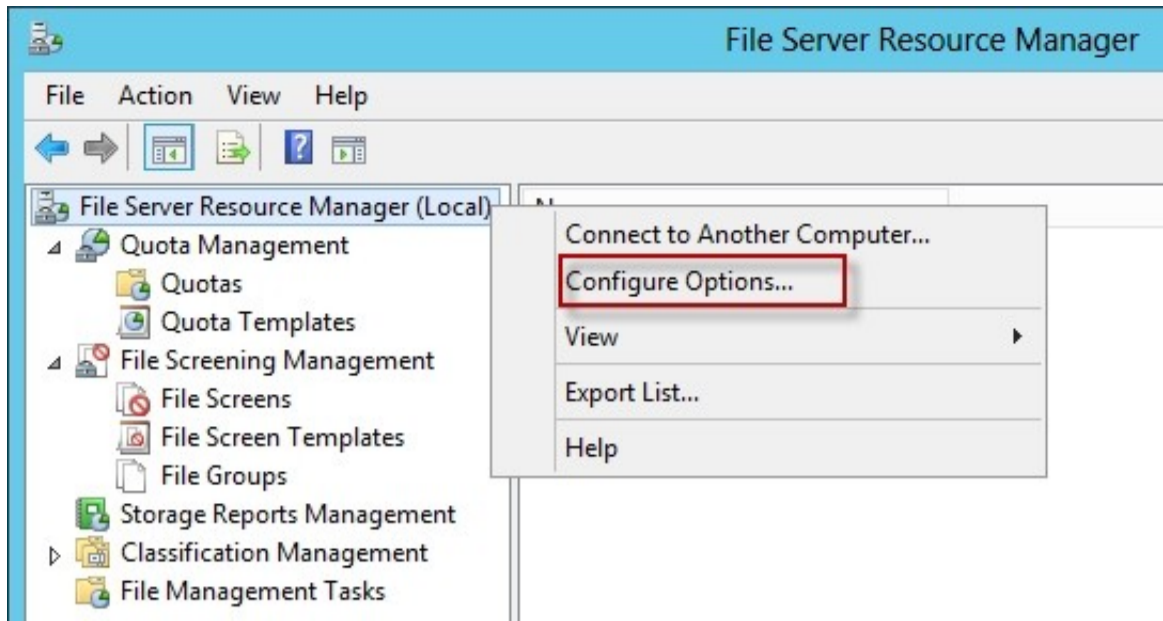
Explanation:

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.

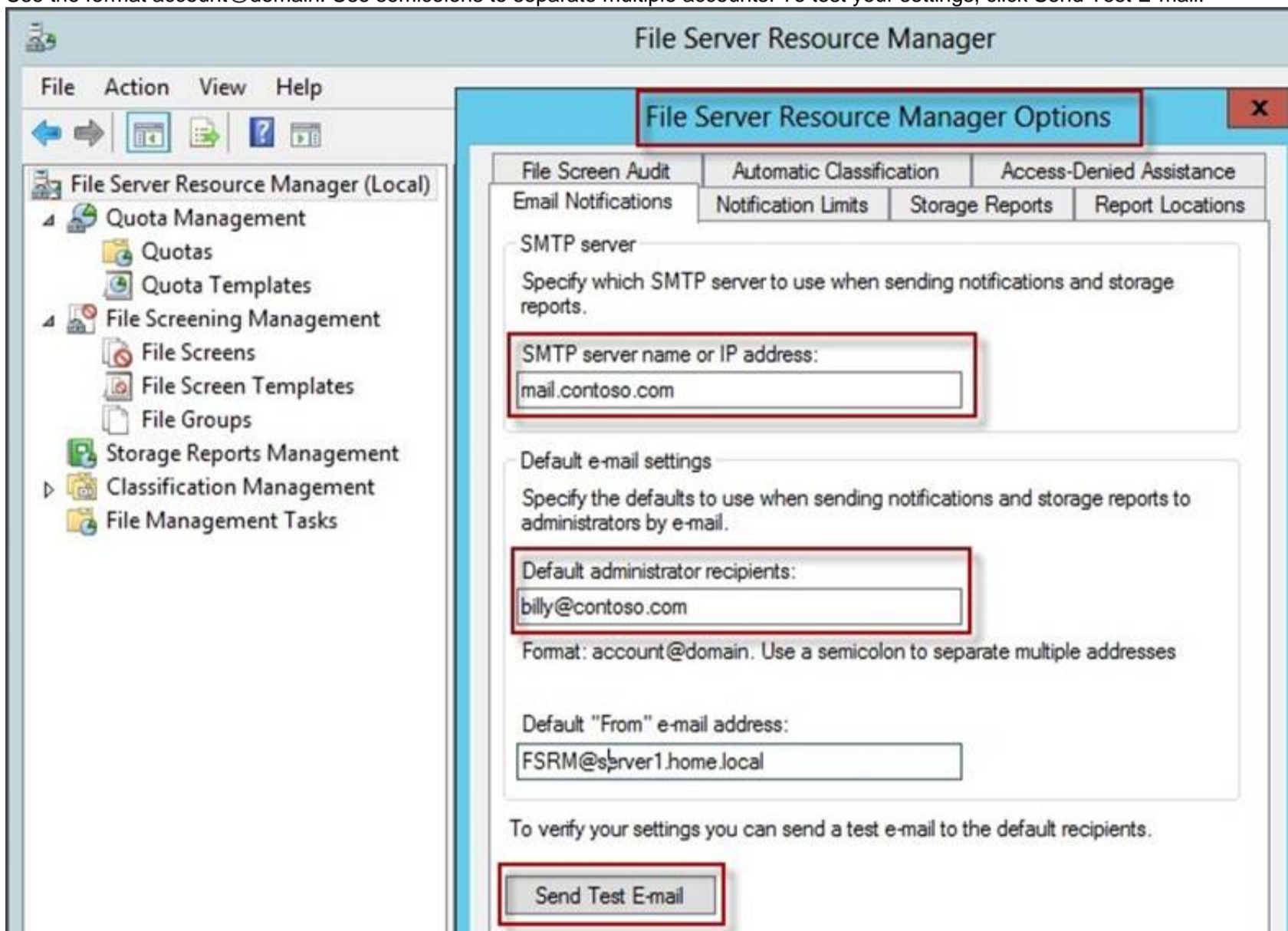
To configure e-mail options

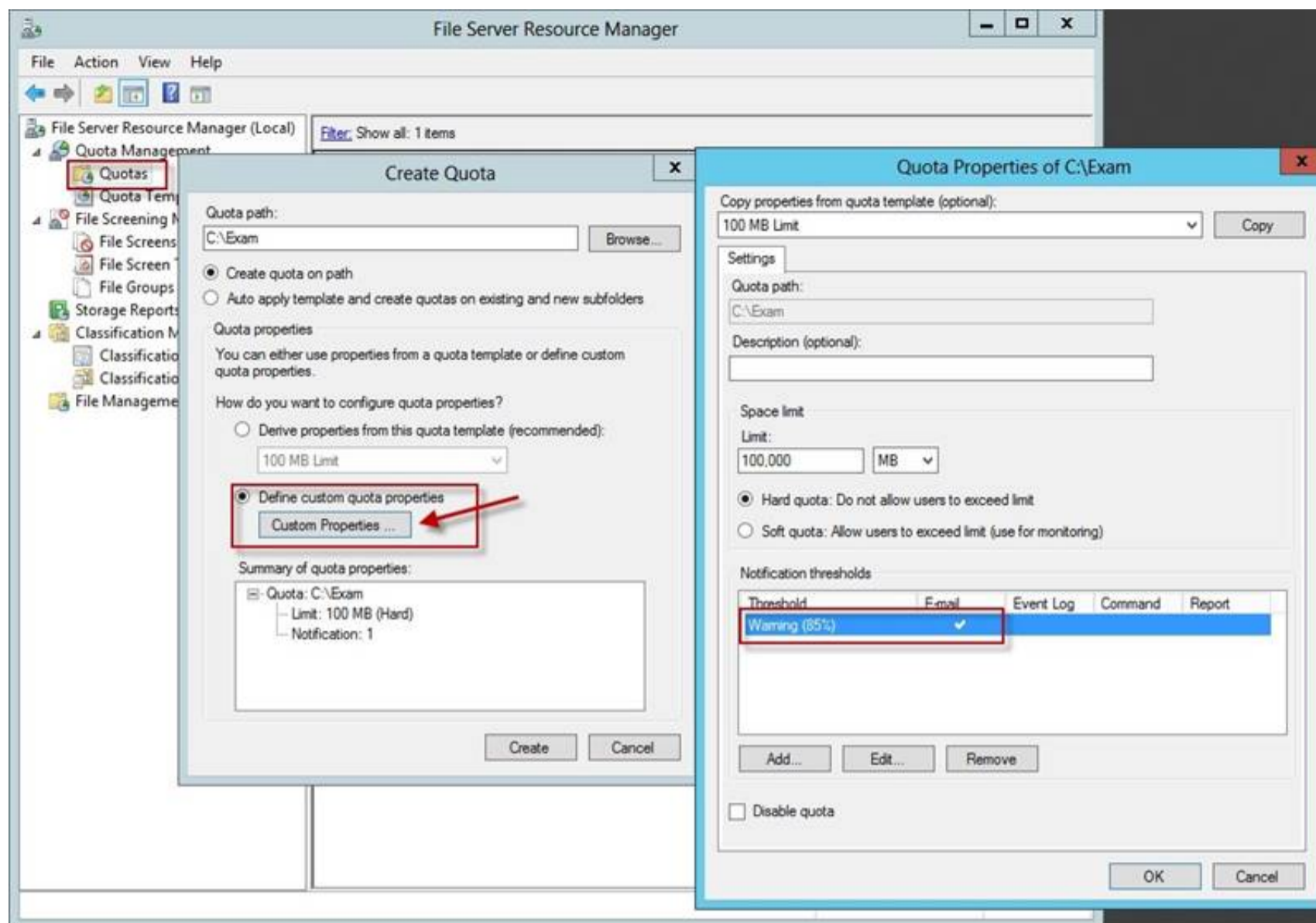
In the console tree, right-click File Server Resource Manager, and then click Configure options. The File Server Resource Manager Options dialog box opens.



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 211

- (Topic 3)

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

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

The technician needs to download updates in French and English.

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

- A. Complete the Windows Server Update Services Configuration Wizard, and then modify the update language on the server.
- B. Uninstall all instances of the Windows Internal Database.
- C. Change the update languages on the upstream server.
- D. Change the System Local of the server to French.

Answer: C

Explanation:

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

The Choose Languages page of the WSUS Configuration Wizard allows you to get updates from all languages or from a subset of languages. Selecting a subset of languages saves disk space, but it is important to choose all the languages that are needed by all the downstream servers and client computers of a WSUS server.

Downstream servers and client computers will not receive all the updates they need if you

have not selected all the necessary languages for the upstream server. Make sure you select all the languages that will be needed by all the client computers of all the downstream servers.

You should generally download updates in all languages on the root WSUS server that synchronizes to Microsoft Update. This selection guarantees that all downstream servers and client computers will receive updates in the languages that they require.

To choose update languages for a downstream server:

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

[https://technet.microsoft.com/en-us/library/hh328568\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/hh328568(v=ws.10).aspx)

NEW QUESTION 215

- (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 220

- (Topic 3)

Your network contains 25 Web servers that run Windows Server 2012 R2.

You need to configure auditing policies that meet the following requirements:

? Generate an event each time a new process is created.

? Generate an event each time a user attempts to access a file share.

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

- A. Audit access management (Not Defined)
- B. Audit directory service access (Not Defined)
- C. Audit logon events (Not Defined)
- D. Audit Object (Not Defined)
- E. Audit policy change(Not Defined)
- F. Audit privilege use (Not Defined)
- G. Audit process tracking (Not Defined)
- H. Audit system events(Not Defined)

Answer: DG

Explanation:

* Audit Object Access

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

* Audit Process Tracking

Determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

Reference: Audit object access

<https://technet.microsoft.com/en-us/library/cc976403.aspx>

Reference: Audit Process Tracking

<https://technet.microsoft.com/en-us/library/cc976411.aspx>

NEW QUESTION 225

- (Topic 3)

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

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

You need to identify which user accounts were authenticated by 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

Explanation:

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

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

NEW QUESTION 228

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 70-411 Exam with Our Prep Materials Via below:

<https://www.certleader.com/70-411-dumps.html>