

Microsoft

Exam Questions 70-411

Administering Windows Server 2012



NEW QUESTION 1

HOTSPOT - (Topic 1)

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

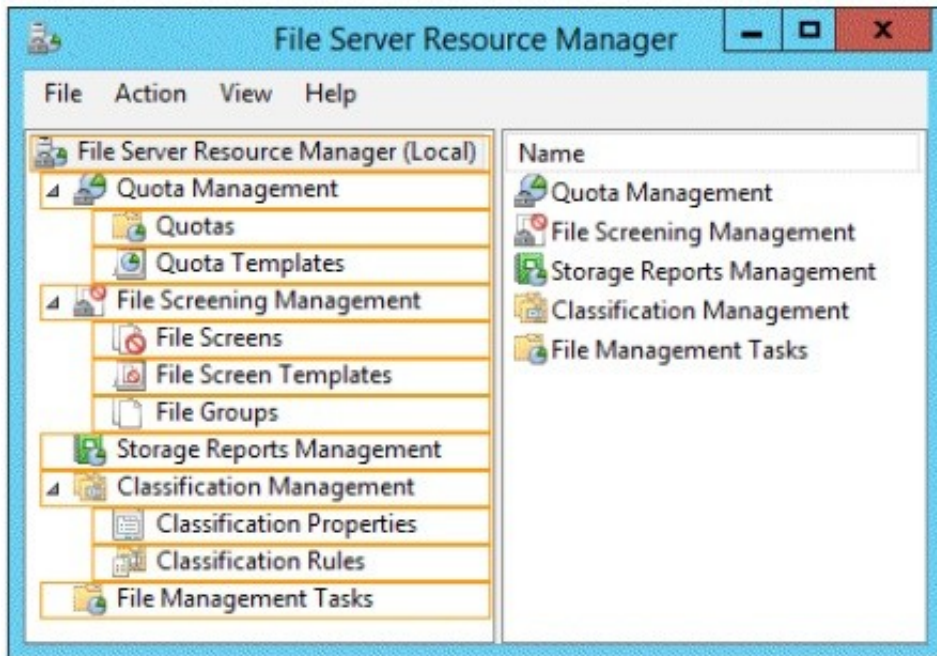
Server1 has the File Server Resource Manager role service installed.

You need to configure Server1 to meet the following requirements:

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

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

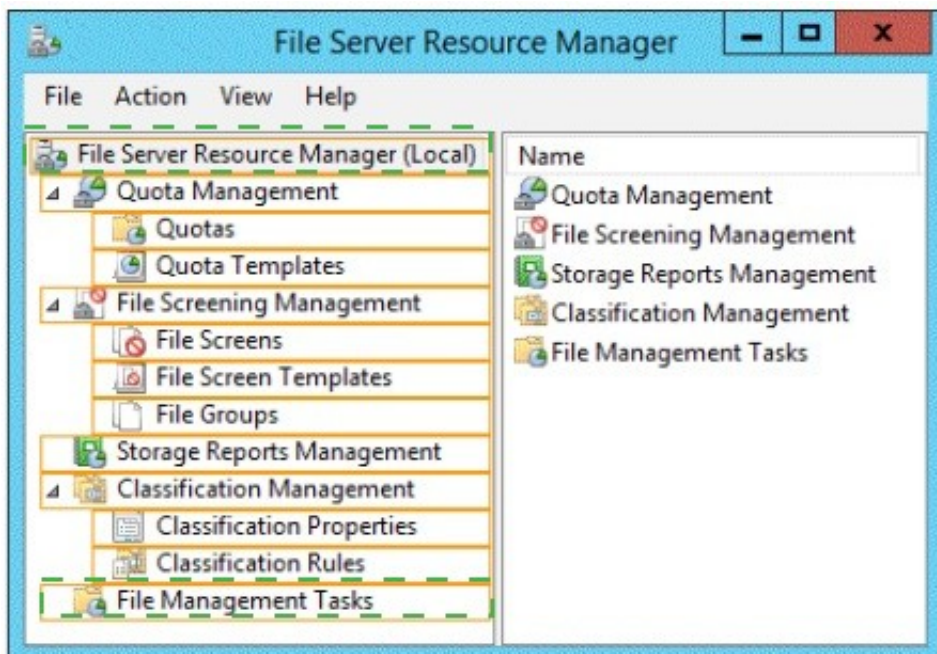
Which two nodes should you configure? To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2

- (Topic 1)

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

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

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

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

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

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (Topic 1)

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

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

You plan to unlink GPO1 from OU1.

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

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

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

Answer: AD

Explanation:

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

References:

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

NEW QUESTION 4

- (Topic 1)

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

The domain has the Active Directory Recycle Bin enabled.

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

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

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

You want to achieve this goal by using the minimum amount of administrative effort. What should you do first?

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

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.

NEW QUESTION 5

- (Topic 1)

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

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

Server1 provides VPN access to external users.

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

What should you run?

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

Answer: C

Explanation:

Add-RemoteAccessRadius

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

AccountingOnOffMsg<String>

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

? Enabled.

? Disabled. This is the default value.

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

NEW QUESTION 6

- (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>

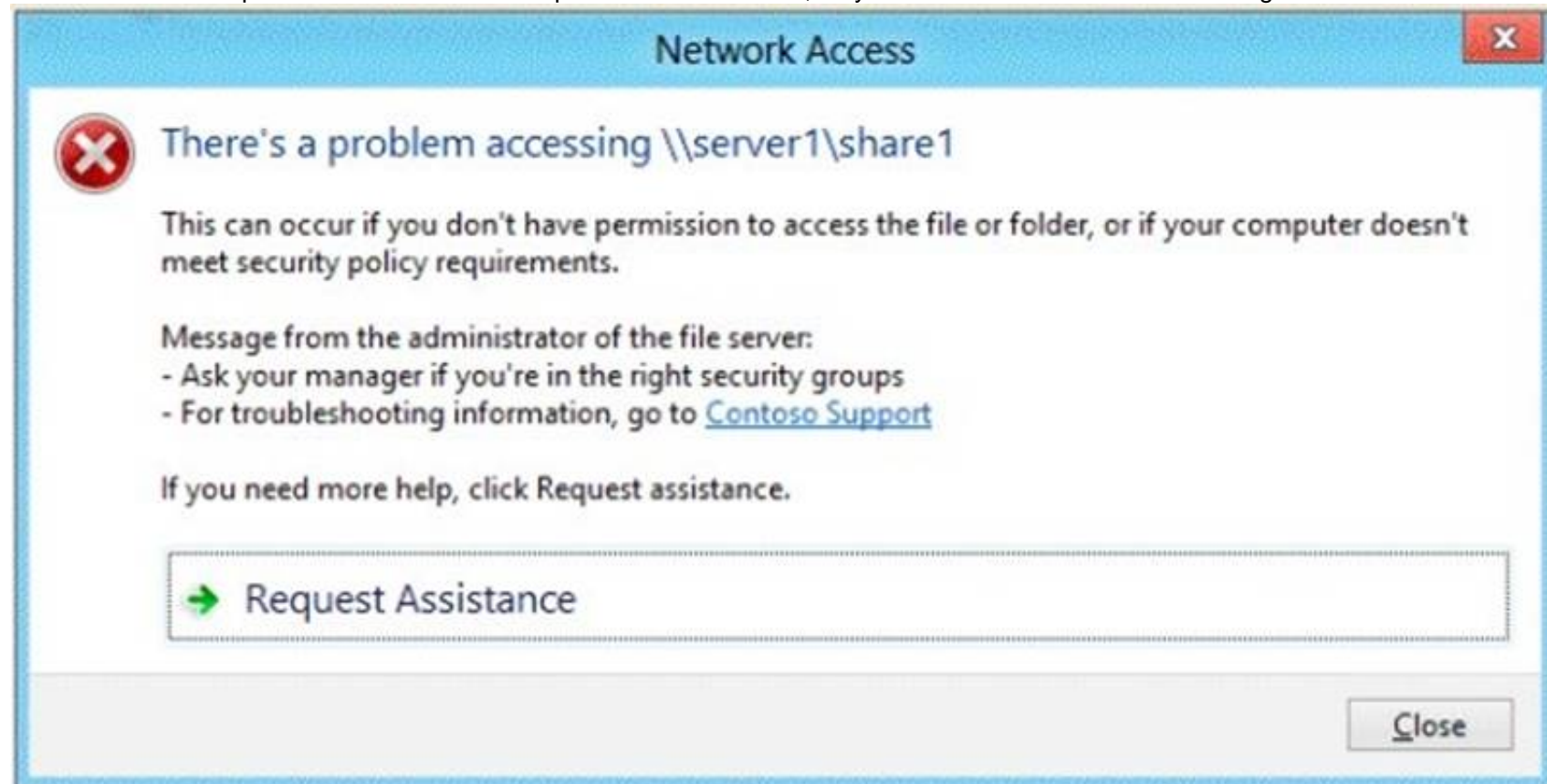
NEW QUESTION 7

- (Topic 1)

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

Server1 has a share named Share1.

When users without permission to Share1 attempt to access the share, they receive the Access Denied message as shown in the exhibit. (Click the Exhibit button.)



You deploy a new file server named Server2 that runs Windows Server 2012 R2.

You need to configure Server2 to display the same custom Access Denied message as Server1.

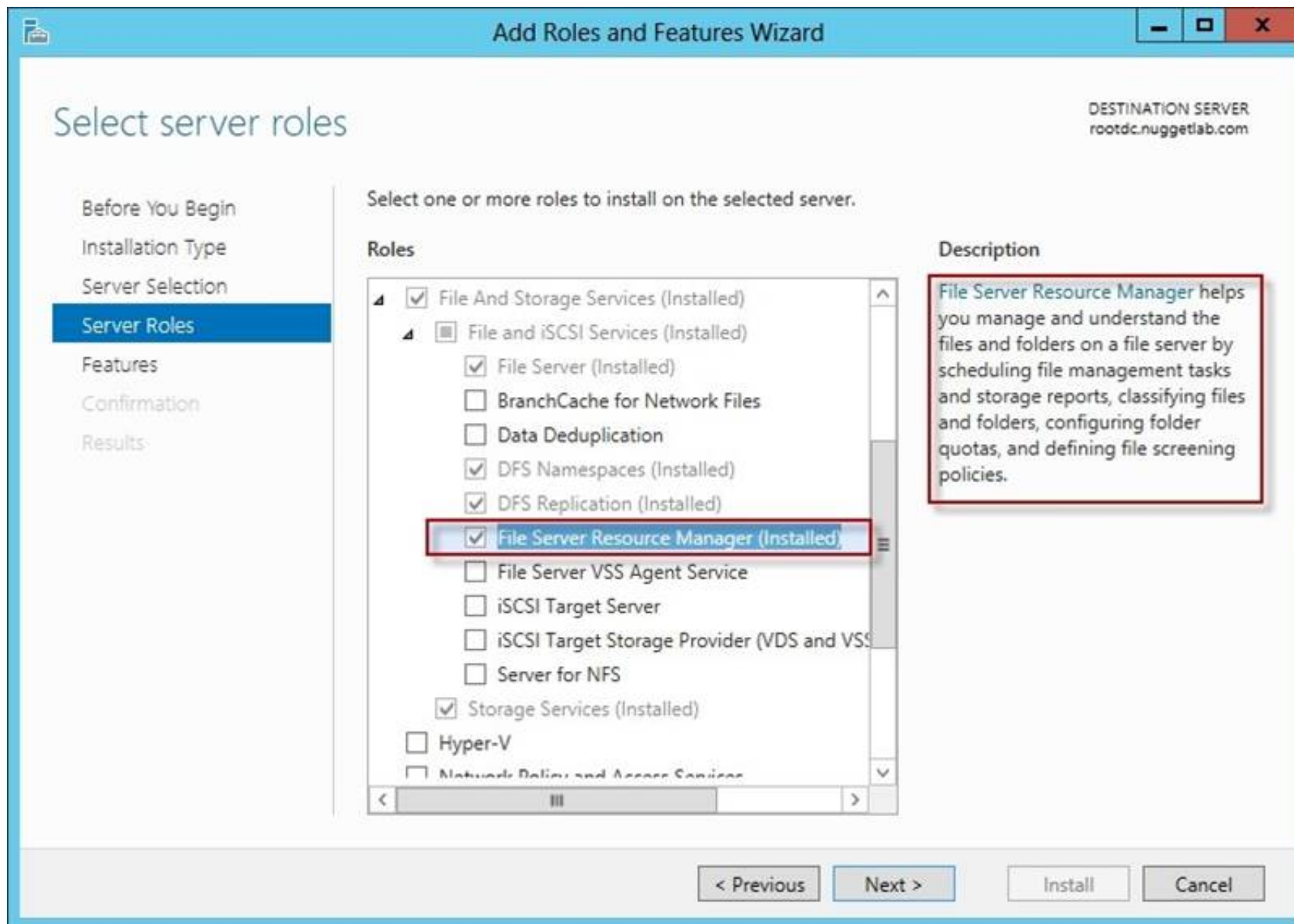
What should you install on Server2?

- A. The Remote Assistance feature
- B. The Storage Services server role
- C. The File Server Resource Manager role service
- D. The Enhanced Storage feature

Answer: C

Explanation:

Access-Denied Assistance is a new role service of the File Server role in Windows Server 2012.



We need to install the prerequisites for Access-Denied Assistance.

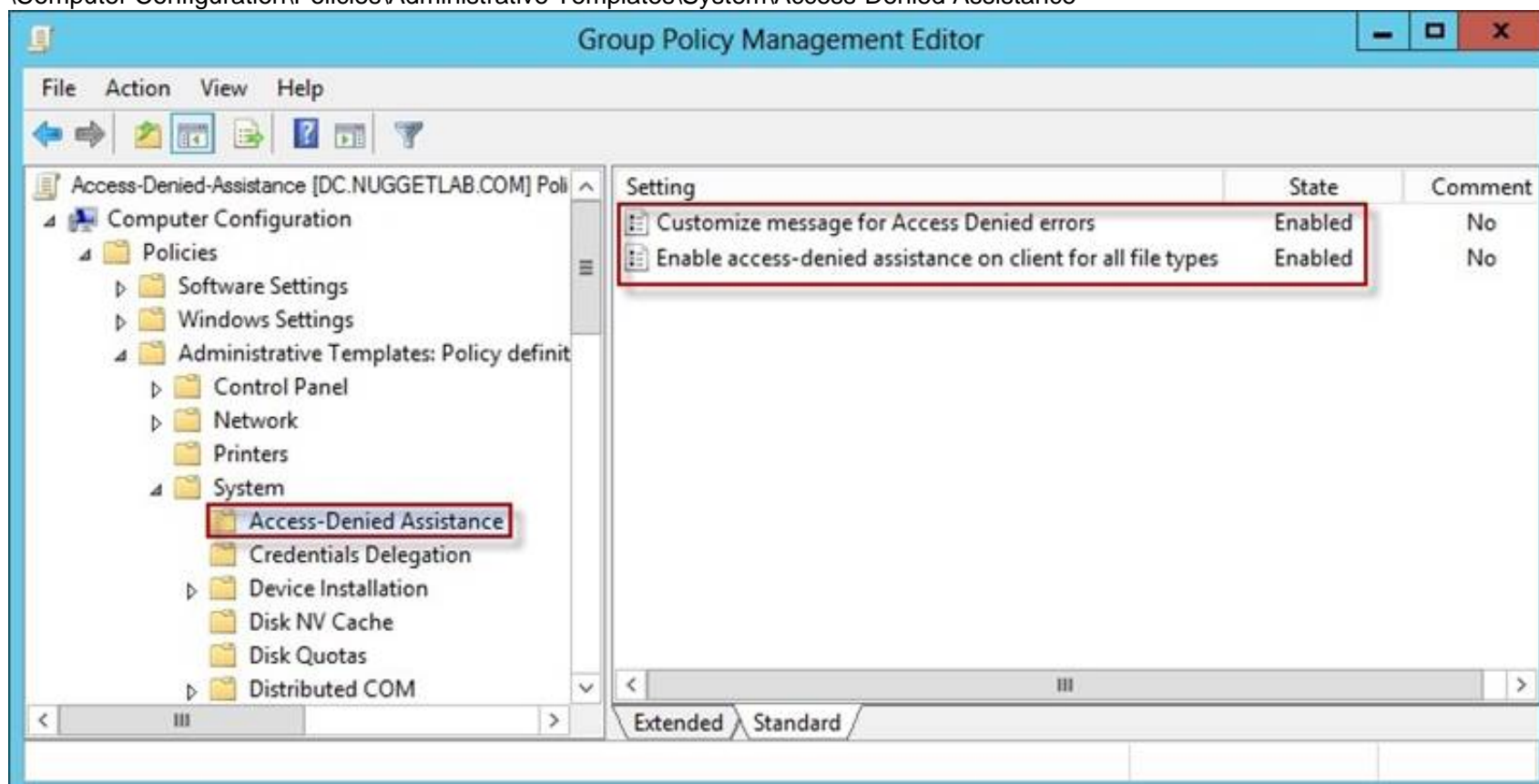
Because Access-Denied Assistance relies up on e-mail notifications, we also need to configure each relevant file server with a Simple Mail Transfer Protocol (SMTP) server address. Let's do that quickly with Windows PowerShell:

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

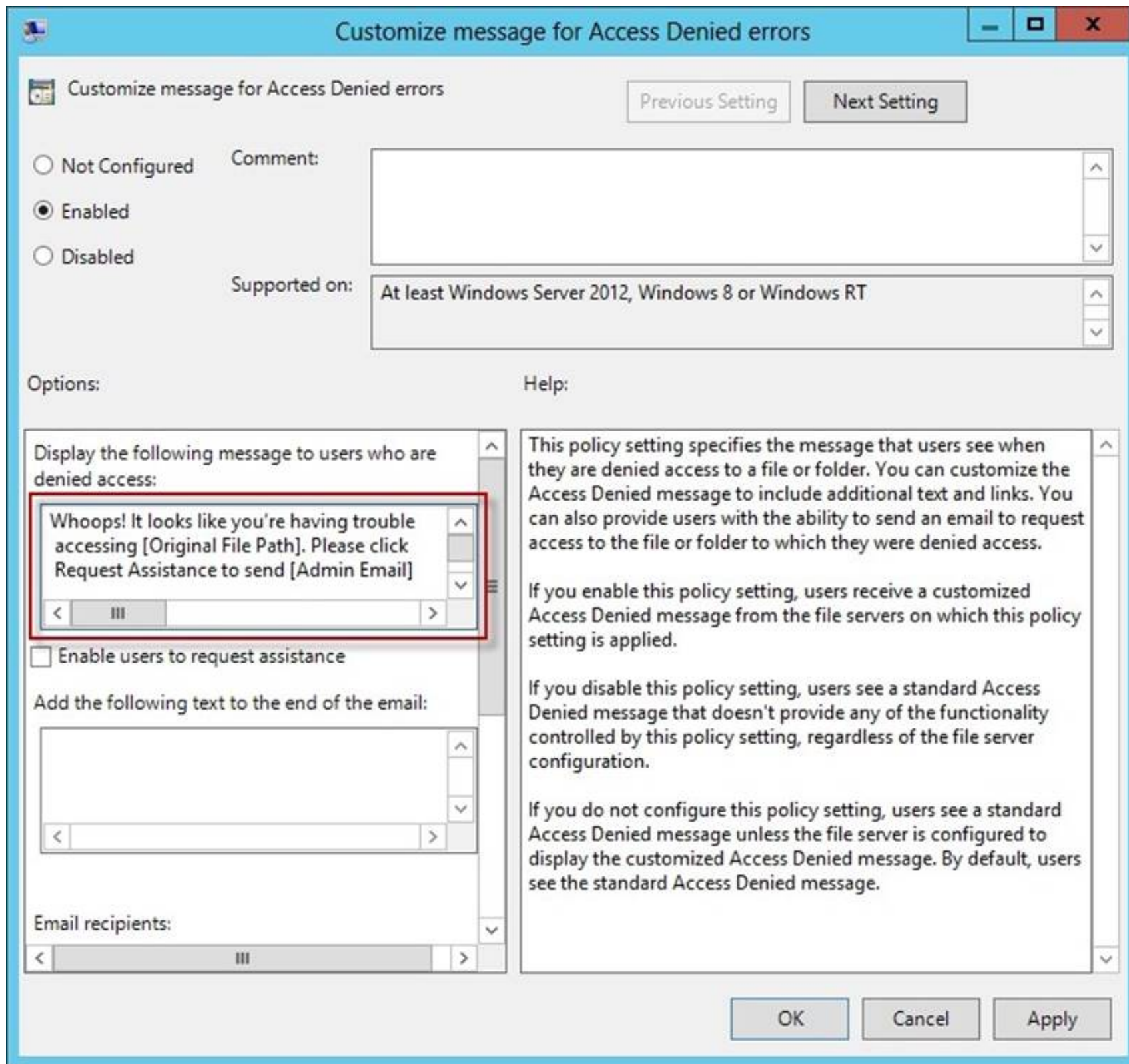
You can enable Access-Denied Assistance either on a per-server basis or centrally via Group Policy. To my mind, the latter approach is infinitely preferable from an administration standpoint.

Create a new GPO and make sure to target the GPO at your file servers' Active Directory computer accounts as well as those of your AD client computers. In the Group Policy Object Editor, we are looking for the following path to configure Access-Denied Assistance:

\Computer Configuration\Policies\Administrative Templates\System\Access-Denied Assistance



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



What's cool about this policy is that we can "personalize" the e-mail notifications to give us administrators (and, optionally, file owners) the details they need to resolve the permissions issue quickly and easily.

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

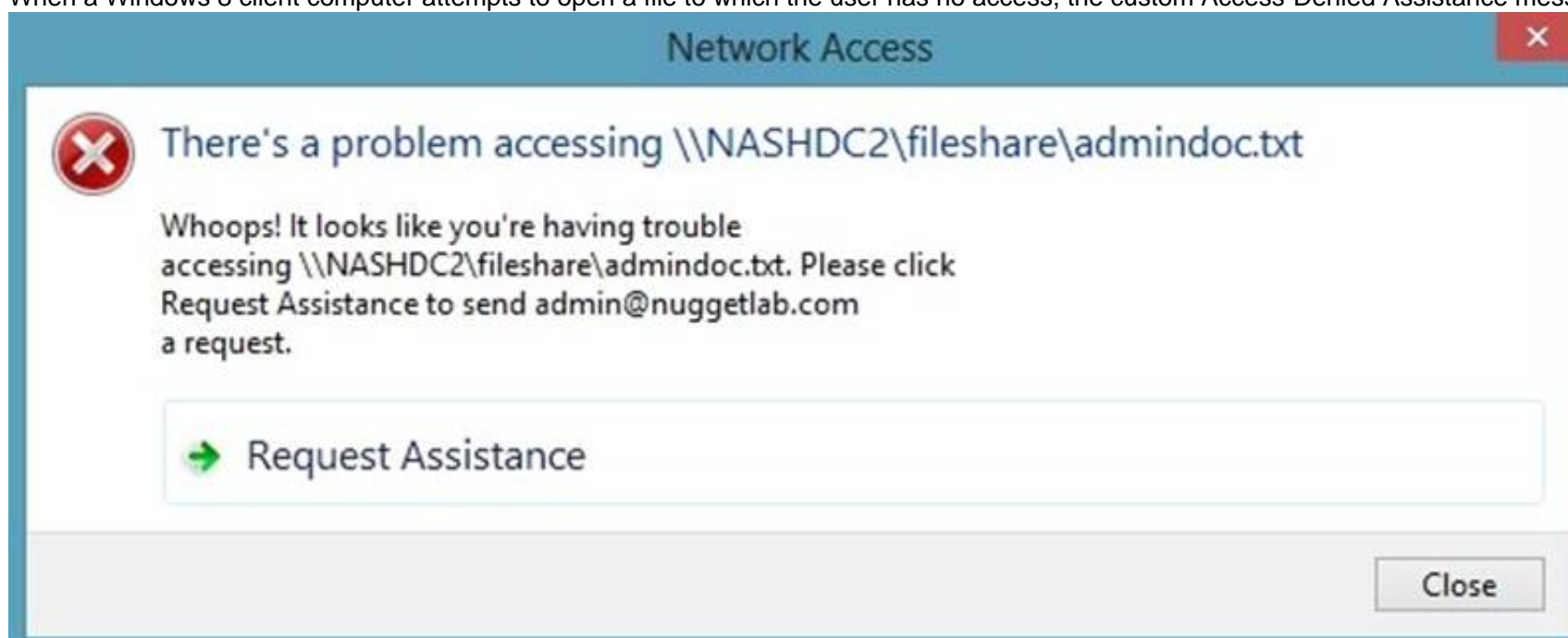
You should find that your users prefer these human-readable, informative error messages to the cryptic, non-descript error dialogs they are accustomed to dealing with.

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

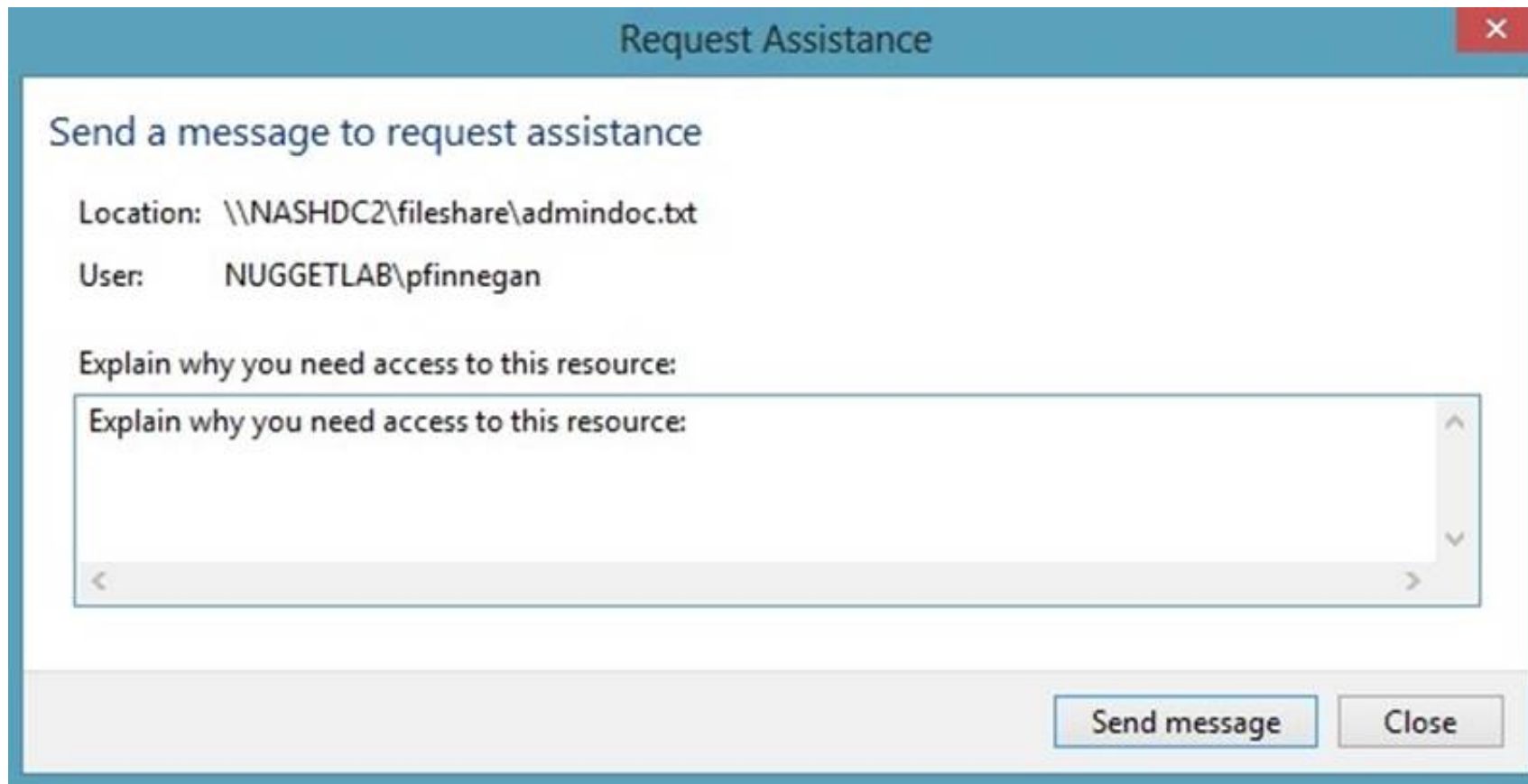
Testing the configuration

This should come as no surprise to you, but Access-Denied Assistance works only with Windows Server 2012 and Windows 8 computers. More specifically, you must enable the Desktop Experience feature on your servers to see Access-Denied Assistance messages on server computers.

When a Windows 8 client computer attempts to open a file to which the user has no access, the custom Access-Denied Assistance message should appear:



If the user clicks Request Assistance in the Network Access dialog box, they see a secondary message:



The image shows a Windows 'Request Assistance' dialog box. It has a title bar with the text 'Request Assistance' and a close button (X). The main content area is titled 'Send a message to request assistance'. It contains the following fields: 'Location: \\NASHDC2\fileshare\adminindoc.txt', 'User: NUGGETLAB\pfinnegan', and a text box labeled 'Explain why you need access to this resource:'. The text box is empty and has a scroll bar. At the bottom right, there are two buttons: 'Send message' and 'Close'.

At the end of this process, the administrator(s) will receive an e-mail message that contains the key information they need in order to resolve the access problem:
The user's Active Directory identity
The full path to the problematic file

A user-generated explanation of the problem

So that's it, friends! Access-Denied Assistance presents Windows systems administrators with an easy-to-manage method for more efficiently resolving user access problems on shared file system resources. Of course, the key caveat is that your file servers must run Windows Server 2012 and your client devices must run Windows 8, but other than that, this is a great technology that should save admins extra work and end-users extra headaches.

Reference: <http://4sysops.com/archives/access-denied-assistance-in-windows-server-2012/>

NEW QUESTION 8

- (Topic 1)

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

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

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

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

Answer: D

Explanation:

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

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

New RADIUS Client

Settings

Advanced

☒ Enable this RADIUS client

☒ Select an existing template:

Template 1

▼

Name and Address

Friendly name:

Client 1

Address (IP or DNS):

192.168.1.1

Verify...

Shared Secret

Select an existing Shared Secrets template:

None

▼

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

☒ Manual
 ☐ Generate

Shared secret:

...

Confirm shared secret:

...

OK

Cancel

NEW QUESTION 9

- (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 and has the Hyper-V server role installed.

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

Users report that App1 responds more slowly than expected.

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

Which performance object should you monitor on Server1?

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

Answer: C

Explanation:

In the simplest way of thinking the virtual processor time is cycled across the available logical processors in a round-robin type of fashion. Thus all the processing power gets used over time, and technically nothing ever sits idle.

To accurately measure the processor utilization of a guest operating system, use the "Hyper-V Hypervisor Logical Processor (Total)\% Total Run Time" performance monitor counter on the Hyper-V host operating system.

NEW QUESTION 10

- (Topic 1)

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

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

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

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

Answer: C

Explanation:

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

Reference:

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

NEW QUESTION 10

HOTSPOT - (Topic 1)

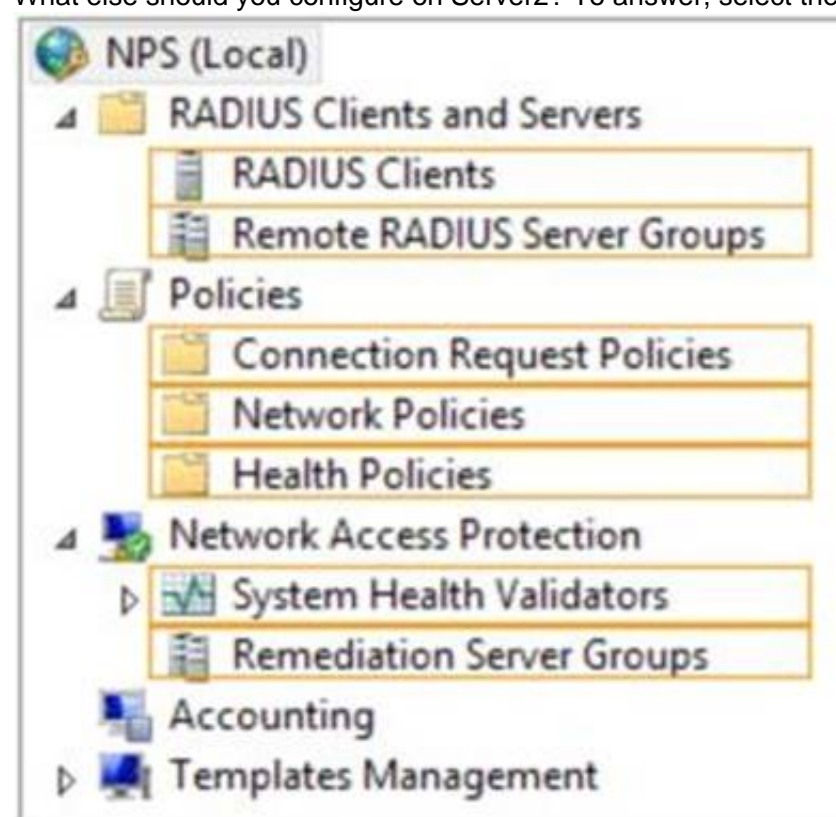
Your network contains a RADIUS server named Server1.

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.

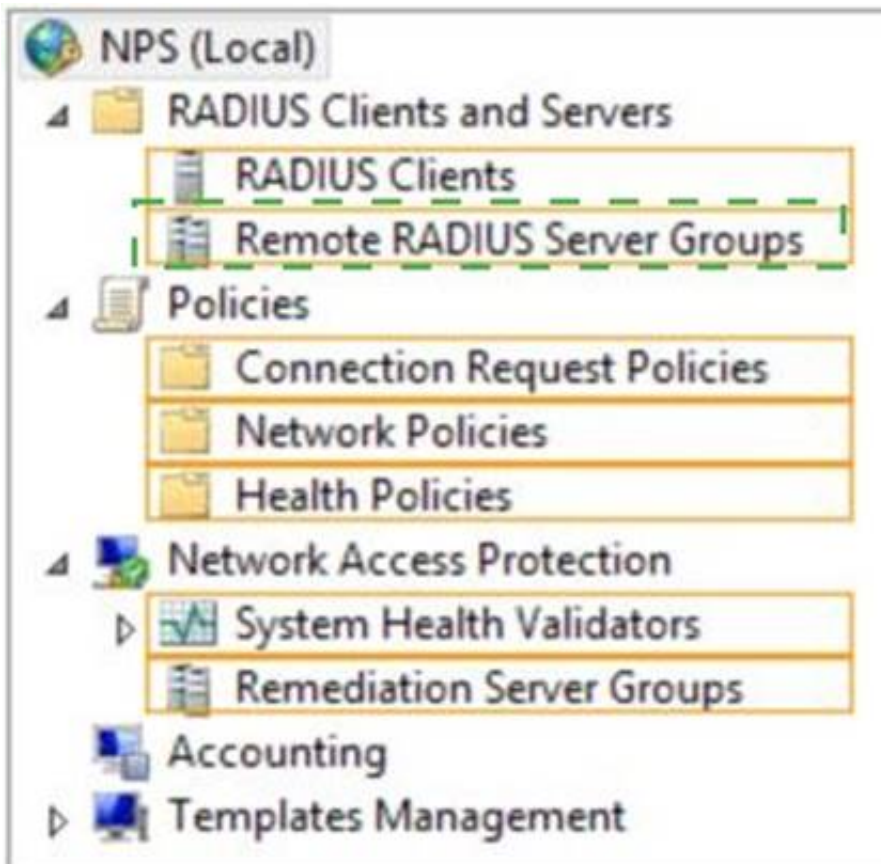
What else should you configure on Server2? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 12

- (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>

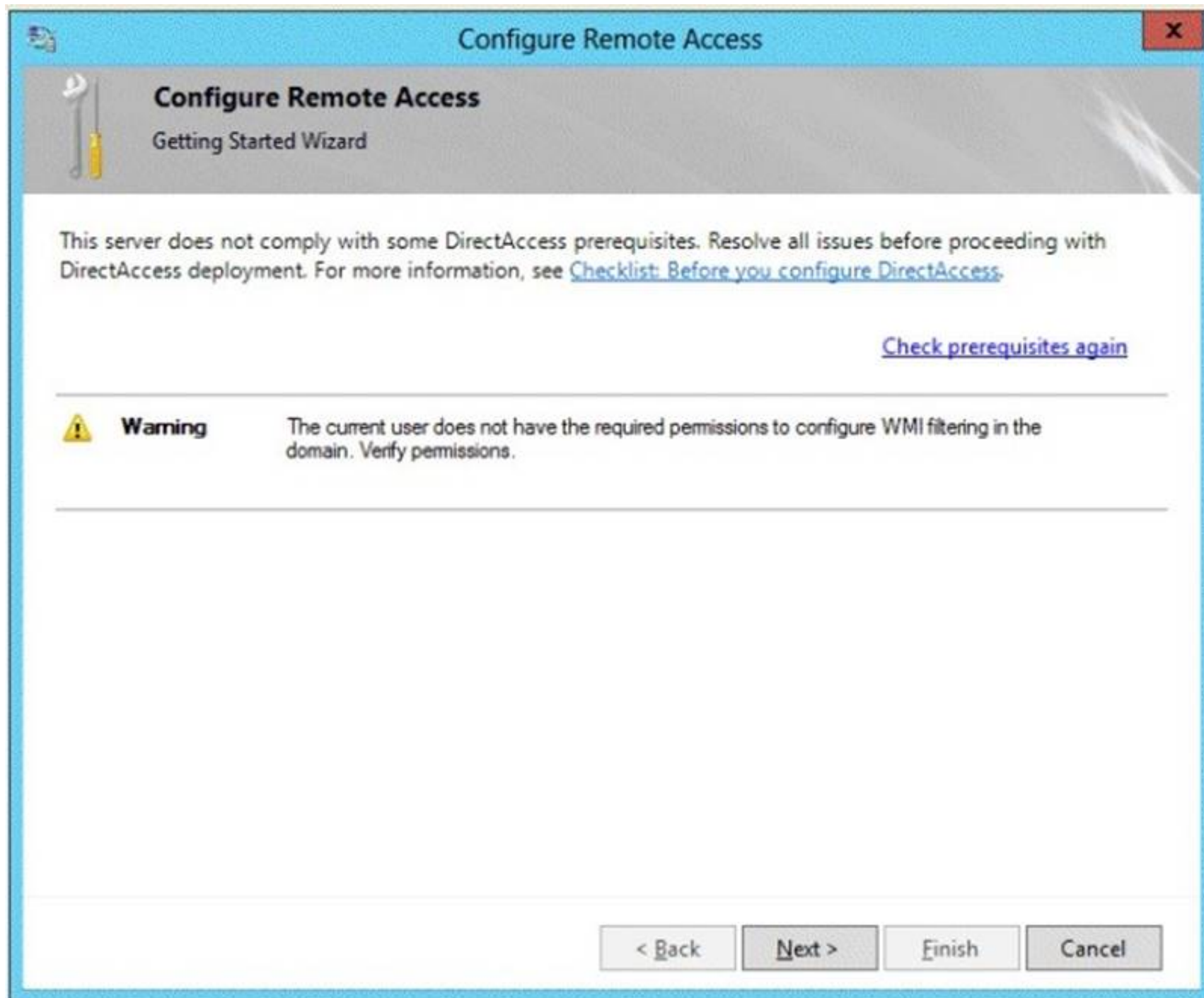
NEW QUESTION 16

- (Topic 1)

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

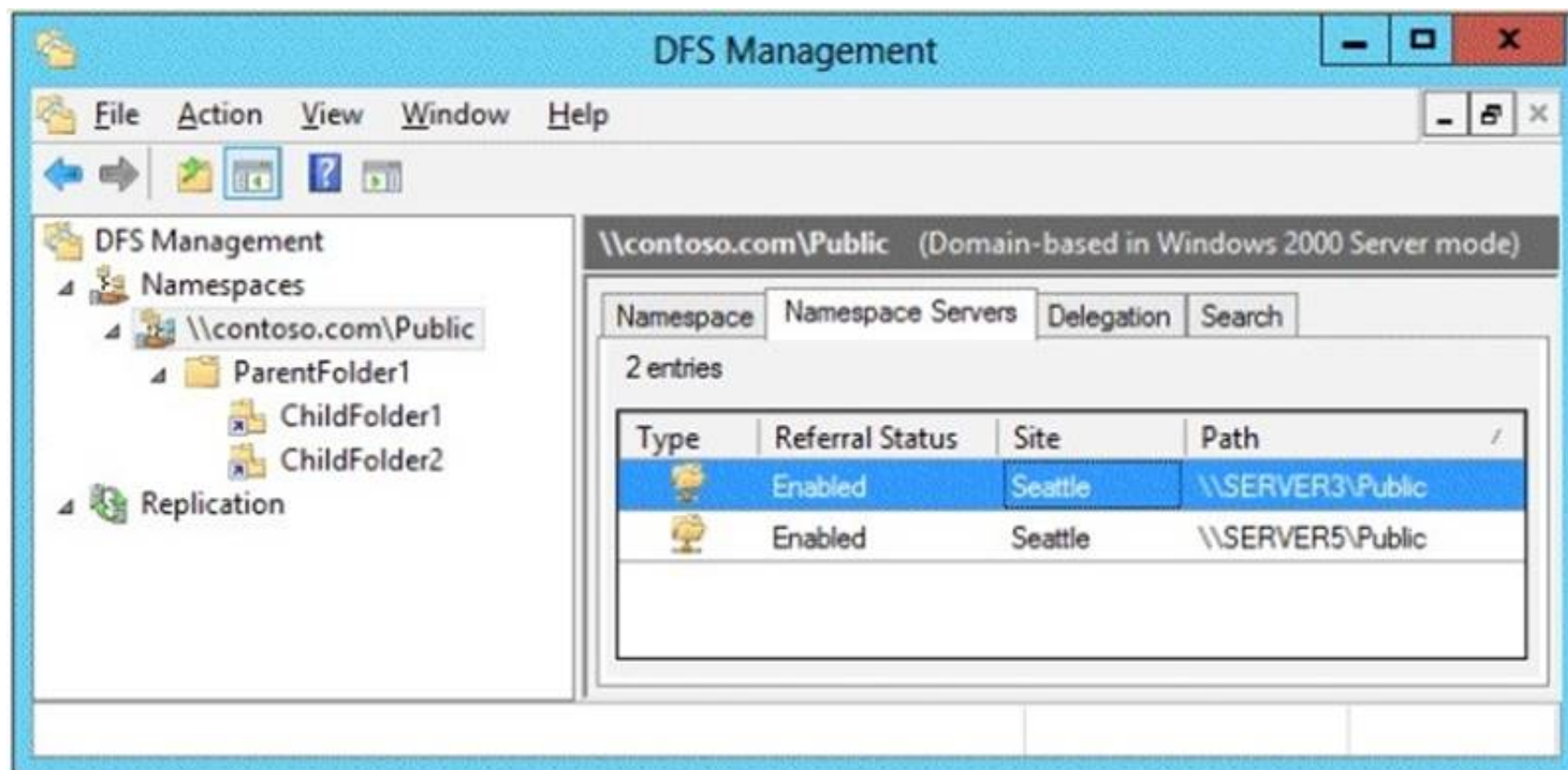
[http://technet.microsoft.com/en-us/library/cc780416\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc780416(v=ws.10).aspx) [http://technet.microsoft.com/en-us/library/cc775497\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc775497(v=ws.10).aspx)

NEW QUESTION 21

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The functional level of both the domain and the forest is Windows Server 2008 R2.

The domain contains a domain-based Distributed File System (DFS) namespace that is configured as shown in the exhibit. (Click the Exhibit button.)



You need to enable access-based enumeration on the DFS namespace. What should you do first?

- A. Raise the domain functional level.
- B. Raise the forest functional level.
- C. Install the File Server Resource Manager role service on Server3 and Server5.
- D. Delete and recreate the namespace.

Answer: D

Explanation:

Access-based enumeration is only supported on a Domain-based Namespace in Windows Server 2008 Mode. This type of Namespace requires a minimum Windows Server 2003 forest functional level and a minimum Windows Server 2008 domain functional level. The exhibit indicates that the current namespace is a Domain-based Namespace in Windows Server 2000 Mode. To migrate a domain-based namespace from Windows 2000 Server mode to Windows Server 2008 mode, you must export the namespace to a file, delete the namespace, recreate it in Windows Server 2008 mode, and then import the namespace settings.

Reference:

<http://msdn.microsoft.com/en-us/library/cc770287.aspx> <http://msdn.microsoft.com/en-us/library/cc753875.aspx>

NEW QUESTION 26

- (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 27

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.

Objects

-r

-s

AppPool1

http/contoso

https/contoso

http/secure.contoso.com

https/secure.contoso.com

Answer Area

setspn.exe

Object

Object

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 31

DRAG DROP - (Topic 1)

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

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

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

What should you create on each NPS server?

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

Objects

a connection request policy

a network policy

a RADIUS client

a remote RADIUS server group

Answer Area

NPS1:

Object

Object

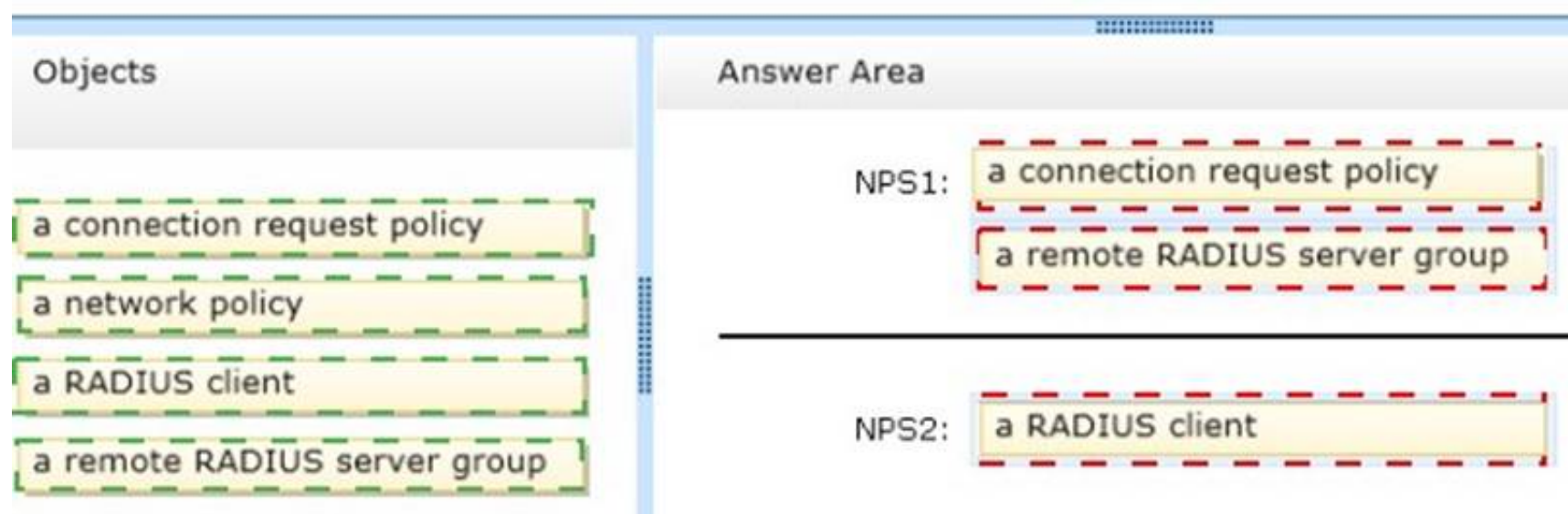
NPS2:

Object

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 33

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All user accounts reside in an organizational unit (OU) named OU1. You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preference of GPO1 to add a shortcut named Link1 to the desktop of each user. You discover that when a user deletes Link1, the shortcut is removed permanently from the desktop. You need to ensure that if a user deletes Link1, the shortcut is added to the desktop again. What should you do?

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

Answer: B

Explanation:

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

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

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

References:

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

NEW QUESTION 35

- (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 39

- (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 42

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 */Capture-Image* parameter.

Run **dism.exe** and specify the */Apply-Image* parameter.

Run **wusa.exe** and specify the */uninstall* parameter.

Run **dism.exe** and specify the */RemovePackage* parameter.

Run **dism.exe** and specify the */Cleanup-Image* 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 45

HOTSPOT - (Topic 1)

You have a server named Server4 that runs Windows Server 2012 R2. Server4 has the Windows Deployment Services server role installed. Server4 is configured as shown in the exhibit. (Click the Exhibit button.)

Windows Deployment Services

File Action View Help

Windows Deployment Services

Servers

- Server4.Contoso.com
 - Install Images
 - Boot Images
 - Pending Devices
 - Multicast Transmissions
 - Drivers
 - Active Directory Prestaged Devices

Boot Images 3 Boot Image(s)

Image Name	Architecture	Status	Expanded Size	Date	OS Version	Priority
BootImage1	x64	Online	1276 MB	8/23/...	6.3.9431	100
BootImage2	x64	Online	1276 MB	8/23/...	6.3.9431	10
BootImage3	x86	Online	1026 MB	8/23/...	6.3.9431	10

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

Answer Area

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

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

Answer Area

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

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 47

- (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

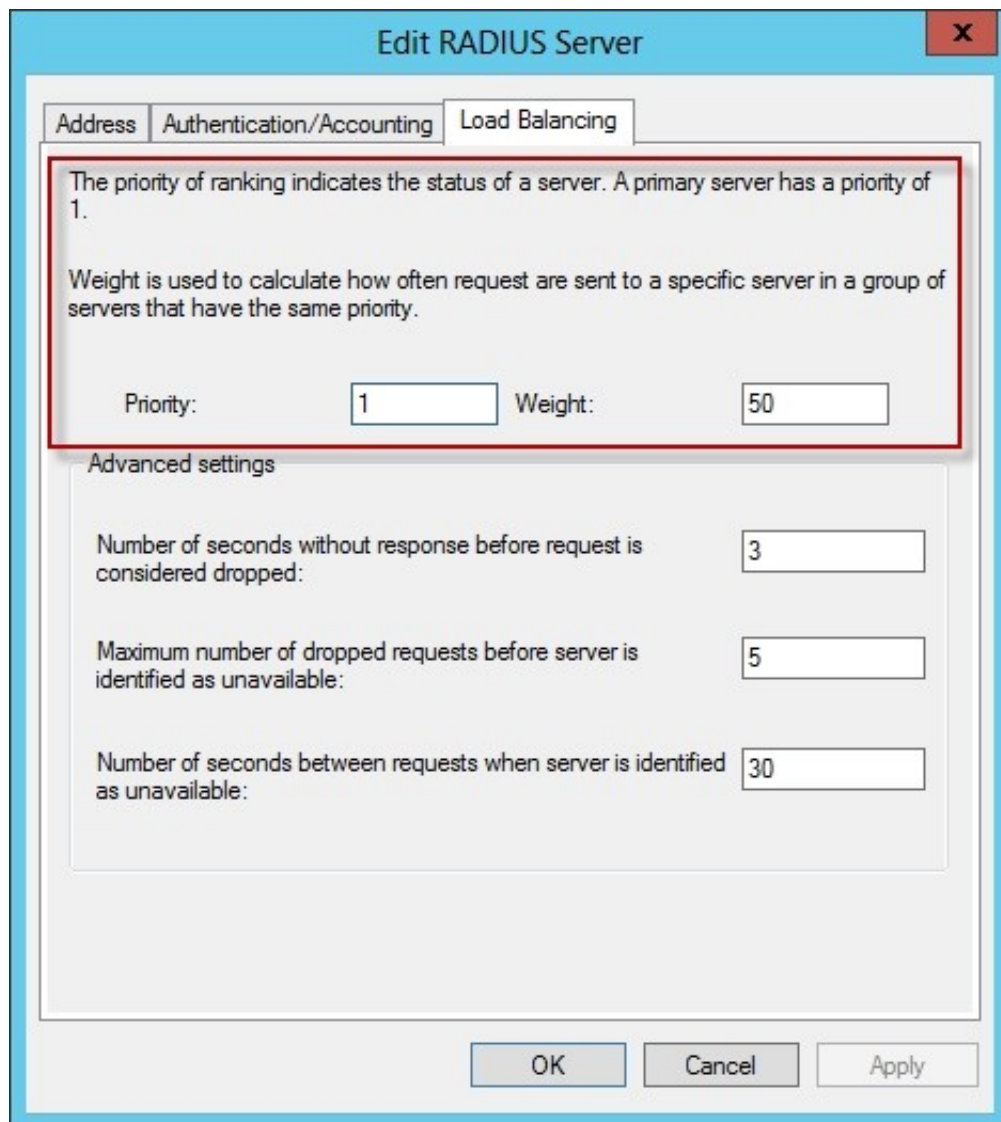
more than one RADIUS server per remote RADIUS server group. While adding group members, or after creating a RADIUS server as a group member, you can access the Add RADIUS server dialog box to configure the following items on the Load Balancing tab:

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.



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 49

- (Topic 1)

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

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 52

- (Topic 1)

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

You implement a Group Policy central store.

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

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

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

Answer: A

Explanation:

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

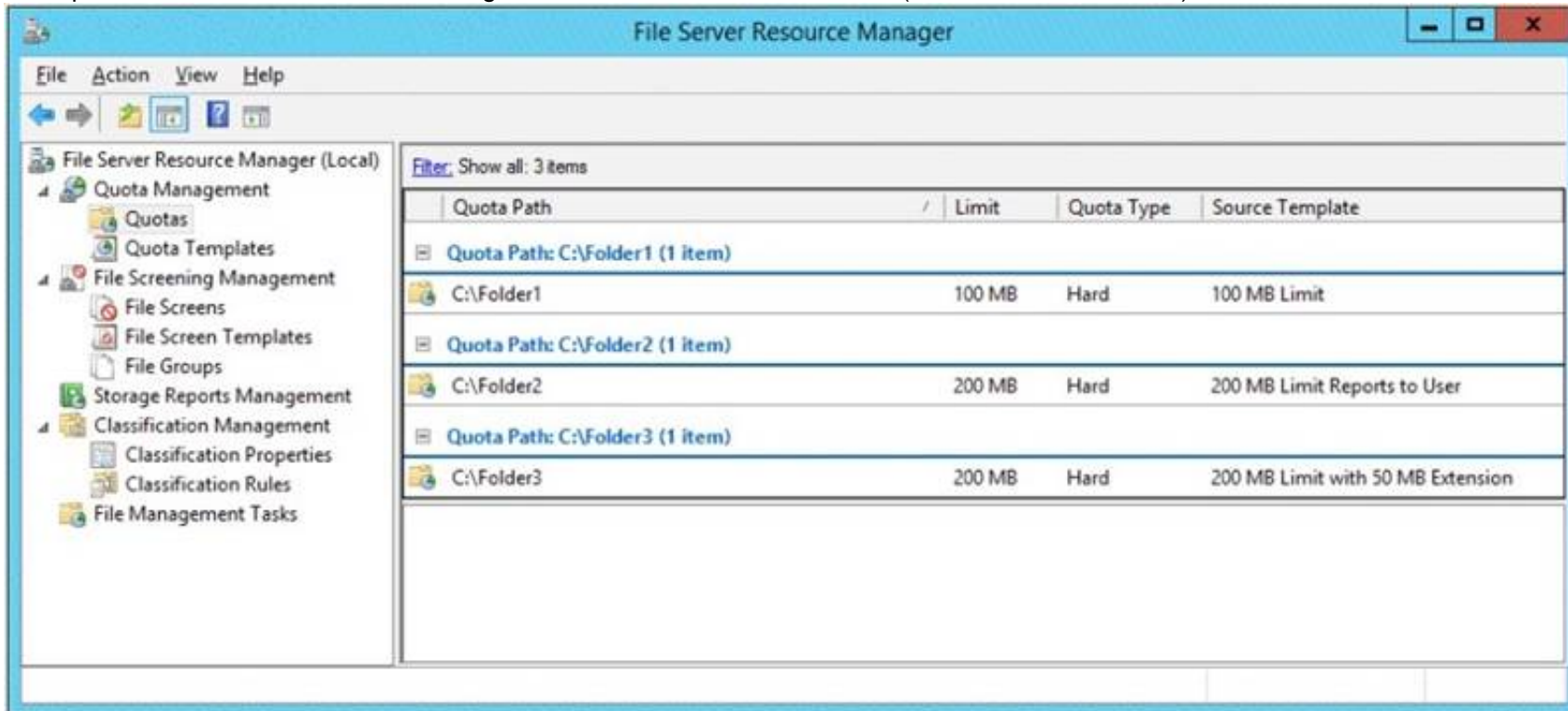
Reference: <http://technet.microsoft.com/en-us/library/dn581922.aspx>

NEW QUESTION 53

- (Topic 1)

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

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



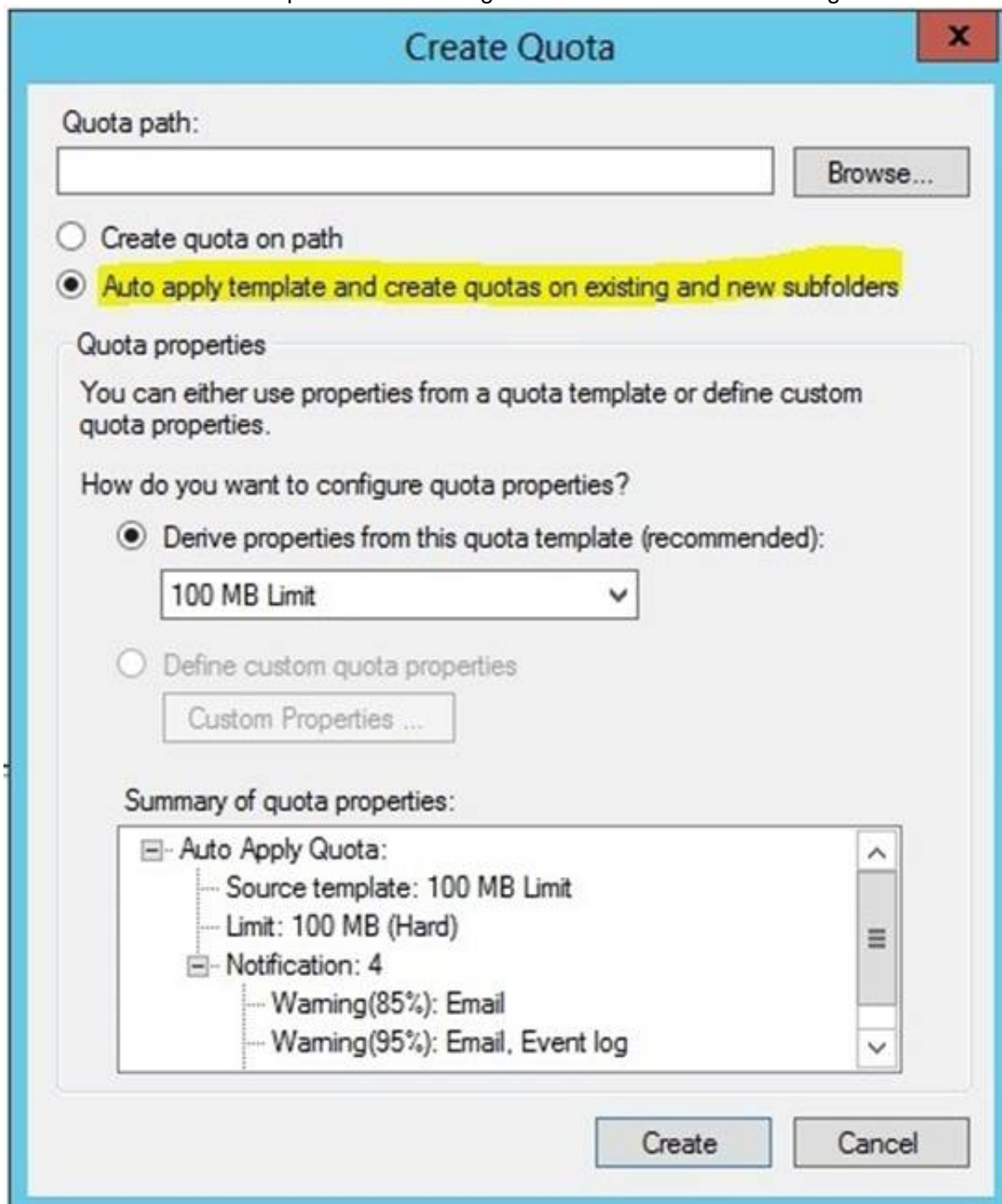
You need to ensure that all of the folders in Folder1 have a 100-MB quota limit. What should you do?

- A. Run the Update Fsrmdmcmdlet.
- B. Run the Update-FsrmdmAutoQuotacmdlet.
- C. Create a new quota for Folder1.
- D. Modify the quota properties of Folder1.

Answer: C

Explanation:

By using auto apply quotas, you can assign a quota template to a parent volume or folder. Then File Server Resource Manager automatically generates quotas that are based on that template. Quotas are generated for each of the existing subfolders and for subfolders that you create in the future.



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

NEW QUESTION 56

- (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 59

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. In a remote site, a support technician installs a server named DC10 that runs Windows Server 2012 R2. DC10 is currently a member of a workgroup. You plan to promote DC10 to a read-only domain controller (RODC). You need to ensure that a user named Contoso\User1 can promote DC10 to a RODC in the contoso.com domain. The solution must minimize the number of permissions assigned to User1. What should you do?

- A. From Active Directory Users and Computers, run the Delegation of Control Wizard on the contoso.com domain object.
- B. From Active Directory Administrative Center, pre-create an RODC computer account.
- C. From Ntdsutil, run the local roles command.
- D. Join DC10 to the domain.
- E. Run dsmod and specify the /server switch.

Answer: B

Explanation:

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

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

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

NEW QUESTION 62

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 66

DRAG DROP - (Topic 1)

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

The domain contains an organizational unit (OU) named OU1. OU1 contains an OU named OU2. OU2 contains a user named user1.

User1 is the member of a group named Group1. Group1 is in the Users container.

You create five Group Policy objects (GPO). The GPOs are configured as shown in the following table.

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

The Authenticated Users group is assigned the default permissions to all of the GPOs. There are no site-level GPOs.

You need to identify which three GPOs will be applied to User1 and in which order the GPOs will be applied to User1.

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

Actions

Answer Area

GPO5

GPO3

GPO2

GPO1

GPO4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: GPO2

Box 2: GPO4

Box 3: GPO5

Note:

* First at the domain level (GPO2), then at the highest OU level GPO4, and finally at the OU level containing user1 GPO5.

Incorrect:

* Read and Apply group policy are both needed in order for the user or computer to receive and process the policy

Not GPO1: Group1 has Deny Apply Group Policy permissions on GPO1. Not GPO3: Group1 has Deny Read permissions on GPO3.

GPO2 and GPO4 are disabled.

* When a Group Policy Object (GPO) is enforced it means the settings in the Group Policy Object on an Organization Unit (which is shown as a folder within the Active Directory Users and Computers MMC) cannot be overruled by a Group Policy Object (GPO) which is link enabled on an Organizational Unit below the Organizational Unit with the enforced Group Policy Object (GPO).

* Group Policy settings are processed in the following order: 1 Local Group Policy object

- 2 Site.
- 3 Domain
- 4 Organizational units

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

NEW QUESTION 70

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.

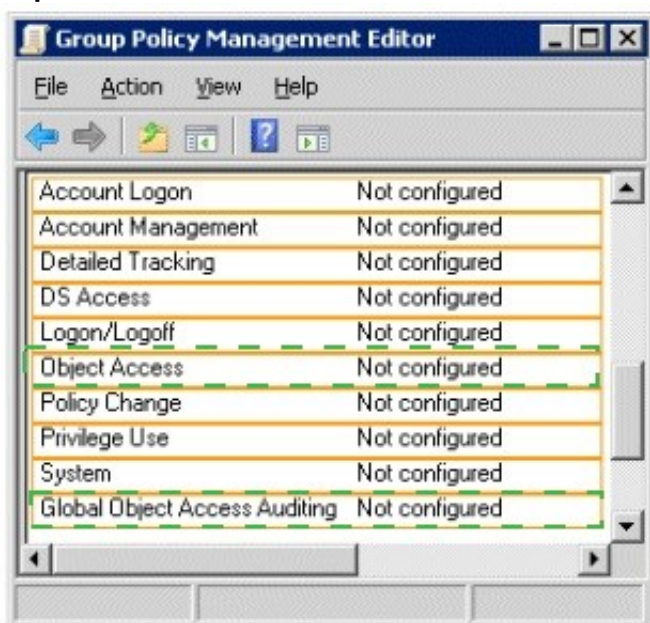
Which two audit policies should you configure in GPO1? To answer, select the appropriate two objects in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 72

- (Topic 1)

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

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

You need to ensure that Server2 can host a secondary zone for contoso.com. What should you do from Server1?

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

Answer: A

Explanation:

Typically, adding a secondary DNS server to a zone involves three steps:

1. On the primary DNS server, add the prospective secondary DNS server to the list of name servers that are authoritative for the zone.
2. On the primary DNS server, verify that the transfer settings for the zone permit the zone to be transferred to the prospective secondary DNS server.
3. On the prospective secondary DNS server, add the zone as a secondary zone.

You must add a new Name Server. To add a name server to the list of authoritative servers for the zone, you must specify both the server's IP address and its DNS name. When entering names, click Resolve to resolve the name to its IP address prior to adding it to the list.

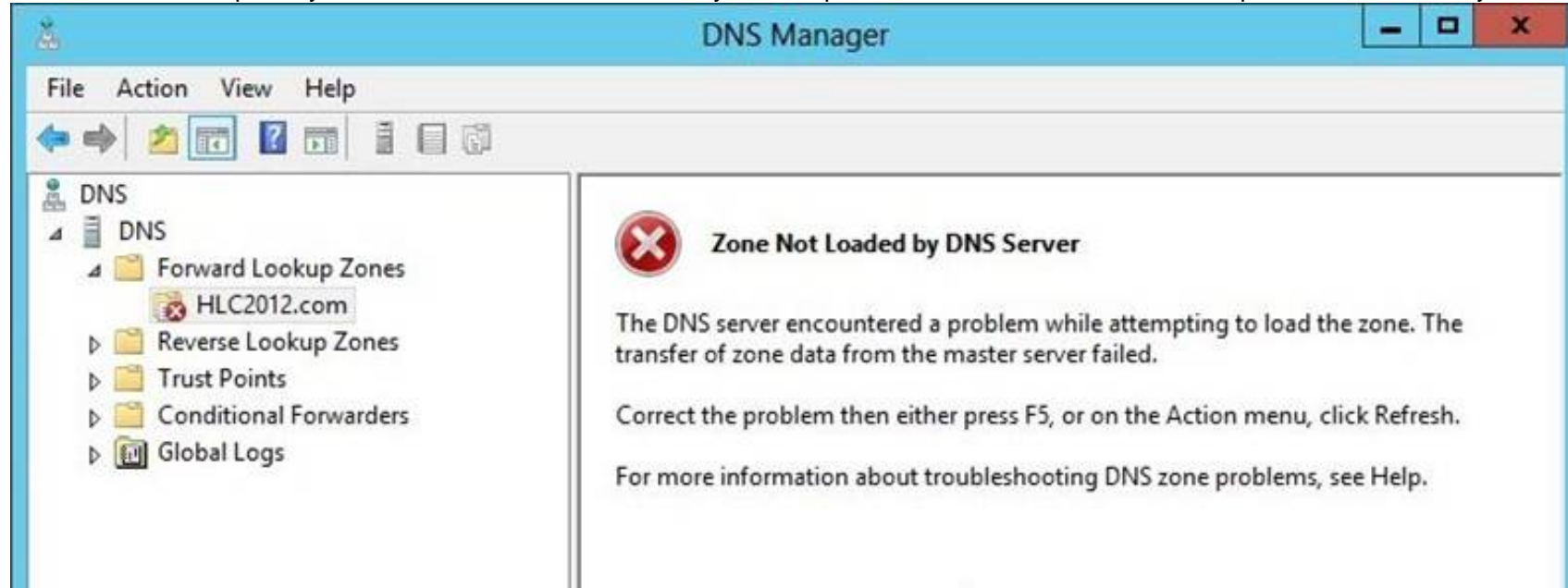
Secondary zones cannot be AD-integrated under any circumstances.

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

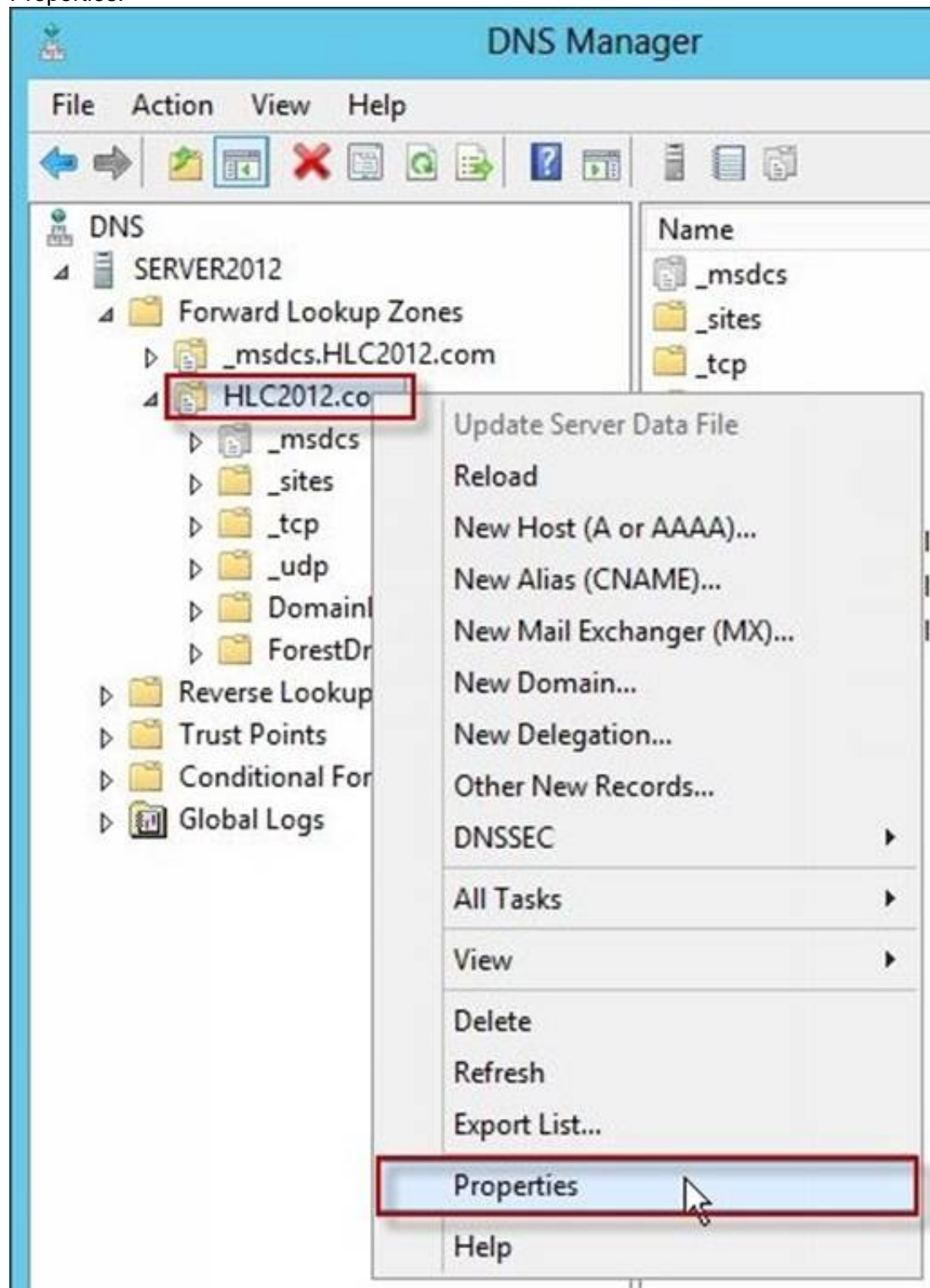
Secondary Domain Name System (DNS) servers help provide load balancing and fault tolerance. Secondary DNS servers maintain a read-only copy of zone data that is transferred periodically from the primary DNS server for the zone. You can configure DNS clients to query secondary DNS servers instead of (or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

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

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



Head over to your primary DNS server, launch DNS manager, expand Forward Lookup Zones, navigate to your primary DNS zone, right-click on it and go to Properties.



Go to "Zone Transfers" tab, by default, for security reasons, the "Allow zone transfers: " is un-checked to protect your DNS information. We need to allow zone transfers, if you value your DNS records, you do not want to select "To any server" but make sure you click on "Only to servers listed on the Name Servers tab".

HLC2012.com Properties

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

A zone transfer sends a copy of the zone to the servers that request a copy.

☒ Allow zone transfers:

☐ To any server

☒ Only to servers listed on the Name Servers tab

☐ Only to the following servers

IP Address	Server FQDN
------------	-------------

Edit

To specify secondary servers to be notified of zone updates, click Notify.

Notify...

OK Cancel Apply Help

Head over to the "Name Servers" tab, click Add.

HLC2012.com Properties

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

To add name servers to the list, click Add.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
server2012.hlc2012.com.	[10.10.10.105]

Add... Edit... Remove

* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.

OK Cancel Apply Help

You will get "New Name Server Record" window, type in the name of your secondary DNS server. it is always better to validate by name not IP address to avoid future problems in case your IP addresses change. Once done, click OK.

New Name Server Record

Enter a server name and one or more IP addresses. Both are required to identify the name server.

Server fully qualified domain name (FQDN):

IP Addresses of this NS record:

IP Address	Validated
<Click here to add an IP Address>	
✓ 10.10.10.106	OK

Buttons: Resolve, Delete, Up, Down, OK, Cancel

You will see your secondary DNS server is now added to your name servers selection, click OK.

HLC2012.com Properties

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

To add name servers to the list, click Add.

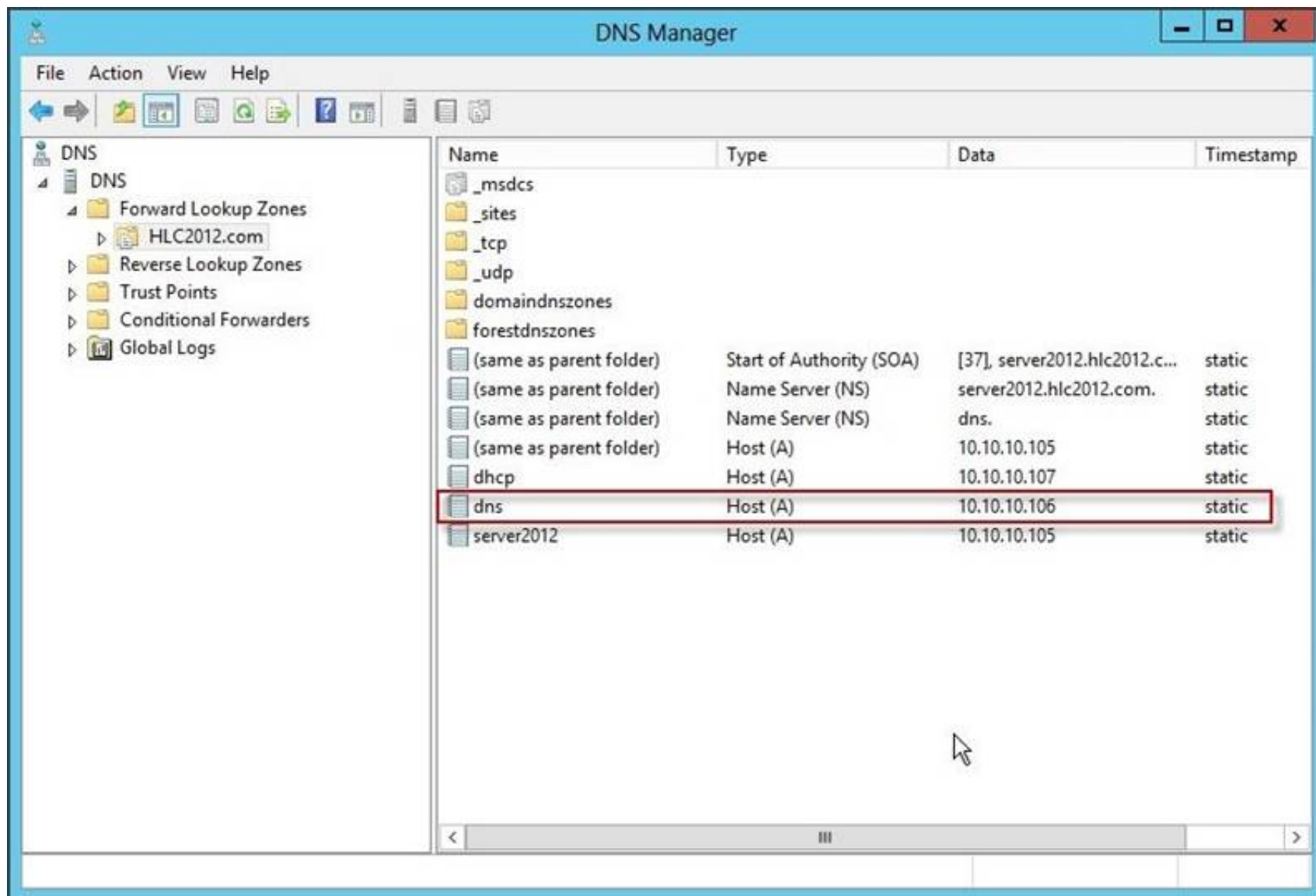
Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
dns.	[10.10.10.106]
server2012.hlc2012.com.	[10.10.10.105]

Buttons: Add..., Edit..., Remove, OK, Cancel, Apply, Help

* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.

Now if you head back to your secondary DNS server and refresh, the big red X will go away and your primary zone data will populate.



Your secondary DNS is fully setup now. You cannot make any DNS changes from your secondary DNS. Secondary DNS is a read-only DNS, Any DNS changes have to be done from the primary DNS.

References:

- <http://technet.microsoft.com/en-us/library/cc816885%28v=ws.10%29.aspx>
- <http://technet.microsoft.com/en-us/library/cc816814%28v=ws.10%29.aspx>
- <http://blog.hyperexpert.com/how-to-configure-a-secondary-dns-server-in-windows-server-2012/>
- <http://technet.microsoft.com/en-us/library/cc770984.aspx>
- <http://support.microsoft.com/kb/816101>
- <http://technet.microsoft.com/en-us/library/cc753500.aspx>
- [http://technet.microsoft.com/en-us/library/cc771640\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc771640(v=ws.10).aspx)
- [http://technet.microsoft.com/en-us/library/ee649280\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee649280(v=ws.10).aspx)

NEW QUESTION 77

- (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 is configured as a VPN server. You need to configure Server1 to perform network address translation (NAT). What should you do?

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

Answer: D

Explanation:

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

1. Open Server Manager.
2. Expand Roles, and then expand Network Policy and Access Services.
3. Right-click Routing and Remote Access, and then click Properties.
4. Select IPv4 Remote access Server or IPv6 Remote access server, or both.

NEW QUESTION 78

- (Topic 1)

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

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

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

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

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

Answer: DE

Explanation:

Folder preference items allow you to create, update, replace, and delete folders and their contents. (To configure individual files rather than folders, see Files

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

NEW QUESTION 83

- (Topic 1)

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

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

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

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

What should you do on Server1?

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

Answer: C

Explanation:

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

When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone.

With secondary, you have ability to resolve records from the other domain even if its DNS servers are temporarily unavailable.

While secondary zones contain copies of all the resource records in the corresponding zone on the master name server, stub zones contain only three kinds of resource records: A copy of the SOA record for the zone.

Copies of NS records for all name servers authoritative for the zone. Copies of A records for all name servers authoritative for the zone.

References:

http://www.windowsnetworking.com/articles-tutorials/windows-2003/DNS_Stub_Zones.html

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

<http://redmondmag.com/Articles/2004/01/01/The-Long-and-Short-of-Stub-Zones.aspx?Page=2>

NEW QUESTION 84

- (Topic 2)

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

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

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

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

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

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

Answer: C

Explanation:

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

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

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

? Force Active Directory replication throughout the domain.

? Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:

DFSRDIAG POLLAD

? You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated.

? On the same DN from Step 1, set: msDFSR-Enabled=TRUE

? Force Active Directory replication throughout the domain.

? Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:

DFSRDIAG POLLAD

? You will see Event ID 4614 and 4604 in the DFSR event log indicating SYSVOL has been initialized. That domain controller has now done a "D2" of SYSVOL.

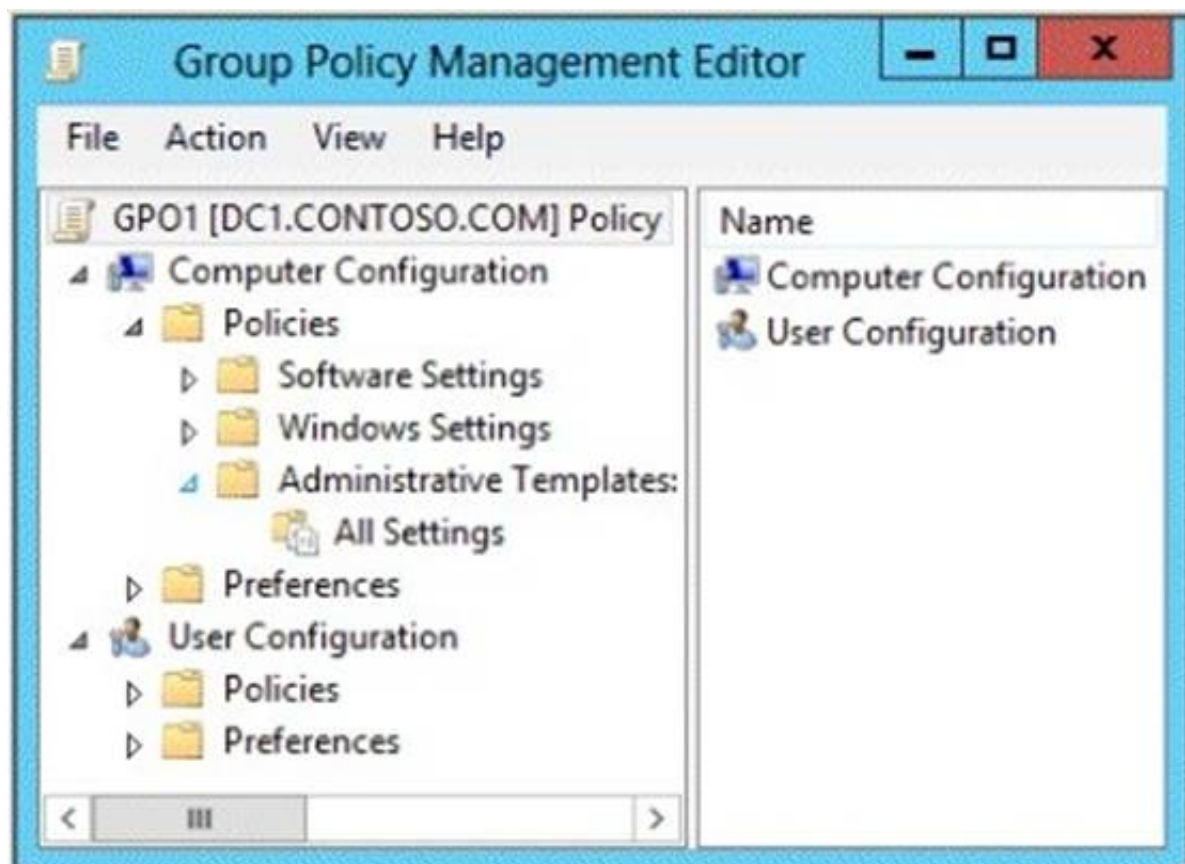
Note: Active Directory Service Interfaces Editor (ADSI Edit) is a Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory. ADSI Edit (adsiedit. msc) provides a view of every object and attribute in an Active Directory forest. You can use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

NEW QUESTION 86

- (Topic 2)

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

A user named User1 creates a central store and opens the Group Policy Management Editor as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that the default Administrative Templates appear in GPO1. What should you do?

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

Answer: B

Explanation:

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

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

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

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

\\FQDN\SYSVOL\FQDN\policies

Reference:

<http://support.microsoft.com/kb/929841>

NEW QUESTION 88

- (Topic 2)

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

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

A server named Server1 is a DNS server that runs a UNIX-based operating system. You plan to use Server1 as a secondary DNS server for the contoso.com zone.

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

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

Answer: C

Explanation:

There are two ways that a secondary DNS server can be added. In both scenarios you will need to add the new server to the Forwarders list of the primary Domain Controller.

1. The Set-DnsServerForwarder cmdlet changes forwarder settings on a Domain Name System (DNS) server.

2. From the primary server, open DNS Manager, right click on the server name and select Properties. Click on the Forwarders tab and click the Edit button in the middle of the dialogue box.

NEW QUESTION 91

HOTSPOT - (Topic 2)

Your network contains a RADIUS server named Admin1.

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

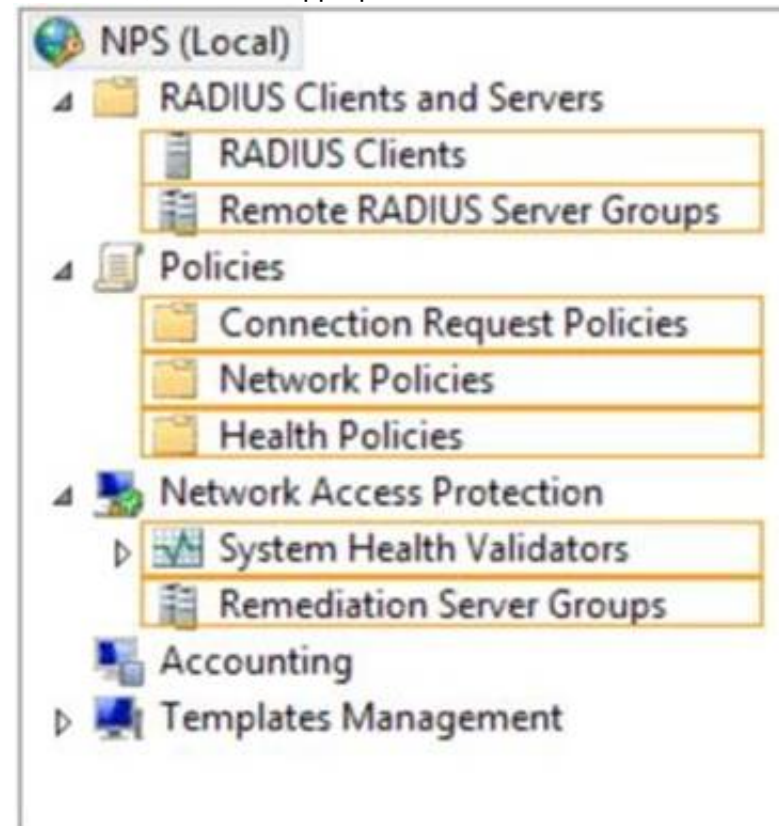
You need to ensure that all accounting requests for Server2 are forwarded to Admin1. On Server2, you create a new remote RADIUS server group named Group1

that contains

Admin1.

What should you configure next on Server2?

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 94

- (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 99

- (Topic 2)

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

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

Internal DNS name: server1.contoso.com

External DNS name: da1.contoso.com

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

External IPv4 address: 65.55.37.62

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

Remote Access Setup

Infrastructure Server Setup
 Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server
 DNS
 DNS Suffix Search List
 Management

Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.

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

Select a local name resolution option:

☐ Use local name resolution if the name does not exist in DNS (most restrictive)
☒ Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended)
☐ Use local name resolution for any kind of DNS resolution error (least restrictive)

< Back Next > Finish Cancel

You need to ensure that client computers on the Internet can establish DirectAccess connections to Server1. Which additional name suffix entry should you add from the Remote Access Setup wizard?

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

Answer: A

Explanation:

Split-brain DNS is the use of the same DNS domain for both Internet and intranet resources. For example, the Contoso Corporation is using split brain DNS; contoso.com is the domain name for intranet resources and Internet resources. Internet users use http: //www.contoso.com to access Contoso's public Web site and Contoso employees on the Contoso intranet use http: //www.contoso.com to access Contoso's intranet Web site. A Contoso employee with their laptop that is not a DirectAccess client on the intranet that accesses http: //www.contoso.com sees the intranet Contoso Web site. When they take their laptop to the local coffee shop and access that same URL, they will see the public Contoso Web site. When a DirectAccess client is on the Internet, the Name Resolution Policy Table (NRPT) sends DNS name queries for intranet resources to intranet DNS servers. A typical NRPT for DirectAccess will have a rule for the namespace of the organization, such as contoso.com for the Contoso Corporation, with the Internet Protocol version 6 (IPv6) addresses of intranet DNS servers. With just this rule in the NRPT, when a user on a DirectAccess client on the Internet attempts to access the uniform resource locator (URL) for their Web site (such as http: //www.contoso.com), they will see the intranet version. Because of this rule, they will never see the public version of this URL when they are on the Internet. For split-brain DNS deployments, you must list the FQDNs that are duplicated on the Internet and intranet and decide which resources the DirectAccess client should reach, the intranet version or the public (Internet) version. For each name that corresponds to a resource for which you want DirectAccess clients to reach the public version, you must add the corresponding FQDN as an exemption rule to the NRPT for your DirectAccess clients. Name suffixes that do not have corresponding DNS servers are treated as exemptions.

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

NEW QUESTION 104

- (Topic 2)

Your network contains a Network Policy Server (NPS) server named Server1. The network contains a server named SQL1 that has Microsoft SQL Server 2008 R2 installed. All servers run Windows Server 2012 R2.

You configure NPS on Server1 to log accounting data to a database on SQL1.

You need to ensure that the accounting data is captured if SQL1 fails. The solution must minimize cost.

What should you do?

- A. Implement Failover Clustering.
- B. Implement database mirroring.
- C. Run the Accounting Configuration Wizard.
- D. Modify the SQL Server Logging properties.

Answer: C

Explanation:

In Windows Server 2008 R2, an accounting configuration wizard is added to the Accounting node in the NPS console. By using the Accounting Configuration wizard, you

can configure the following four accounting settings:

? SQL logging only. By using this setting, you can configure a data link to a SQL Server that allows NPS to connect to and send accounting data to the SQL server. In addition, the wizard can configure the database on the SQL Server to ensure that the database is compatible with NPS SQL server logging.

? Text logging only. By using this setting, you can configure NPS to log accounting data to a text file.

? Parallel logging. By using this setting, you can configure the SQL Server data link and database. You can also configure text file logging so that NPS logs

simultaneously to the text file and the SQL Server database.

? SQL logging with backup. By using this setting, you can configure the SQL Server data link and database. In addition, you can configure text file logging that NPS uses if SQL Server logging fails.

NEW QUESTION 108

- (Topic 2)

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

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

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

Which action should you run first?

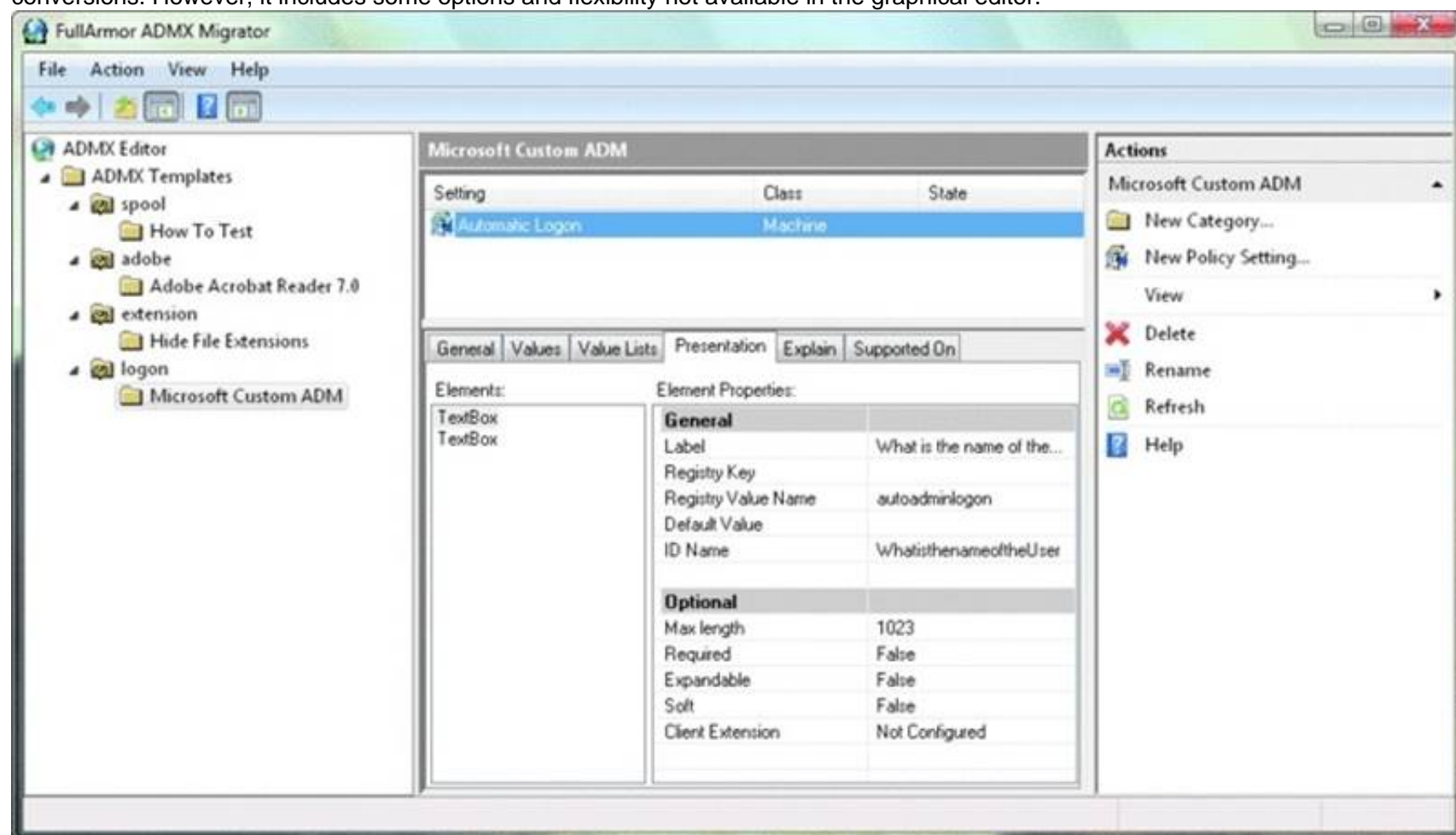
- A. Load Template
- B. New Policy Setting
- C. Generate ADMX from ADM
- D. New Category

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 112

- (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.

Update Files

Update Languages



You can specify where to store update files. Storing files locally requires sufficient disk space.

☒ Store update files locally on this server

☒ Download update files to this server only when updates are approved

☒ Download express installation files
 Express installation files provide faster download and installation on computers, but are larger and will increase download times for your server.

☐ Download files from Microsoft Update; do not download from upstream server

☐ Do not store update files locally; computers install from Microsoft Update

Note: Saving file and language settings may take several minutes. During this time, computers cannot receive updates and other settings cannot be saved.

OK

Cancel

Apply

Reference:

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

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

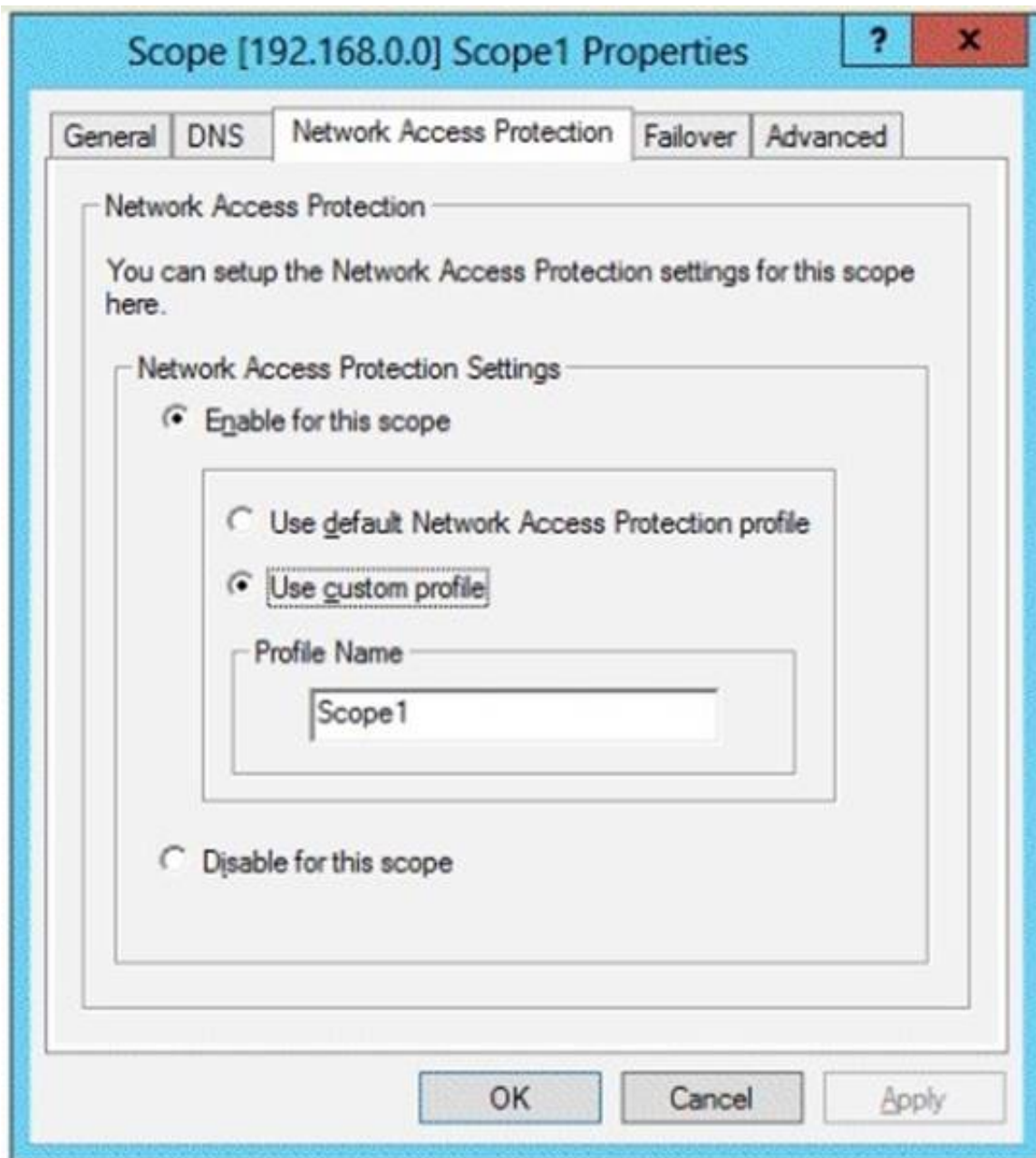
NEW QUESTION 116

- (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.

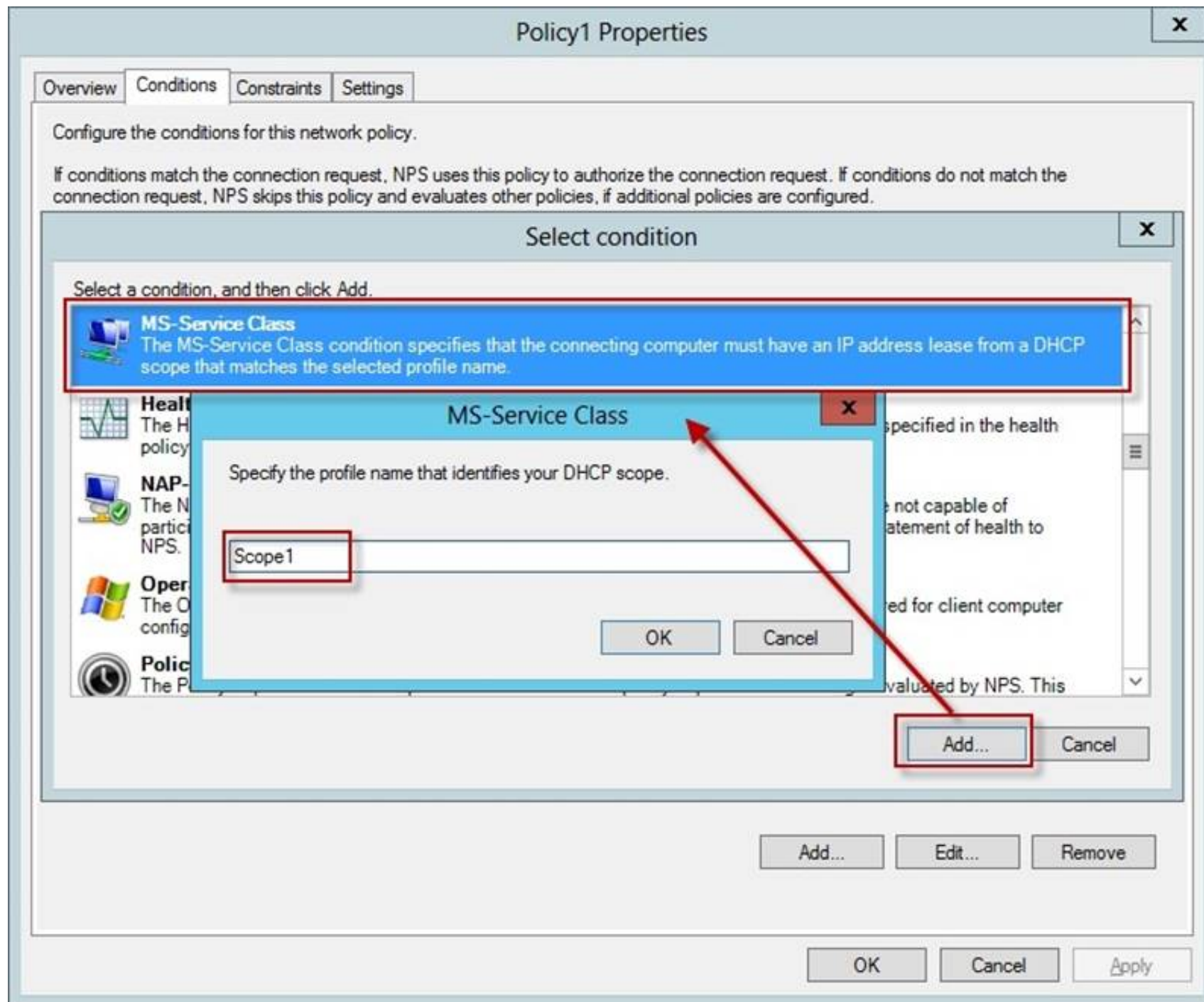
Open the NPS console, double-click Policies, click Network Policies, and then double-click the policy you want to configure.

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 121

- (Topic 2)

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

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

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

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

Answer: B

Explanation:

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

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

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

NEW QUESTION 125

HOTSPOT - (Topic 2)

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

You need to create a certificate template for the BitLocker Drive Encryption (BitLocker) Network Unlock feature.

Which Cryptography setting of the certificate template should you modify? To answer, select the appropriate setting in the answer area.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 130

- (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."

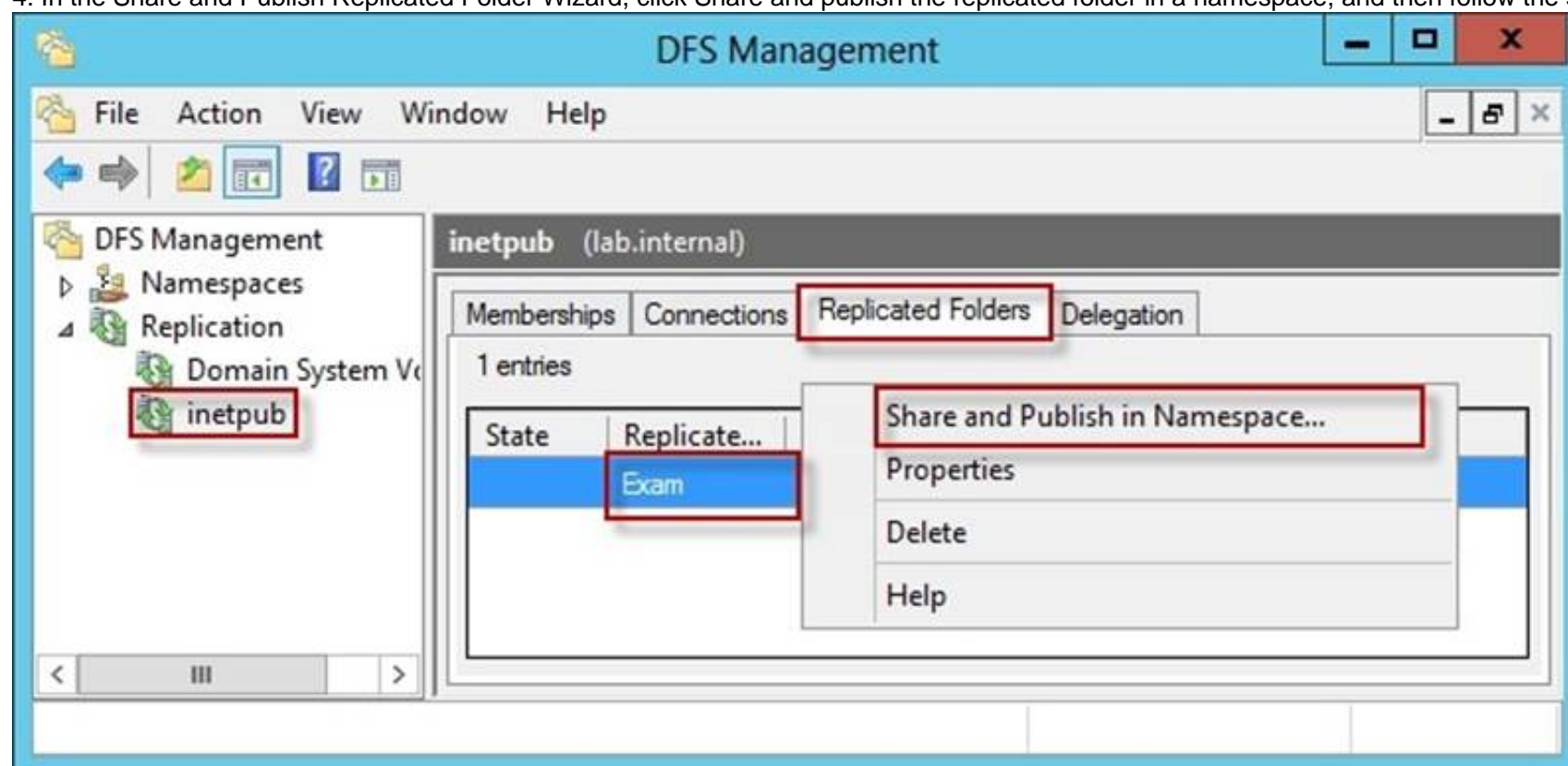
To share a replicated folder and publish it to a DFS namespace

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

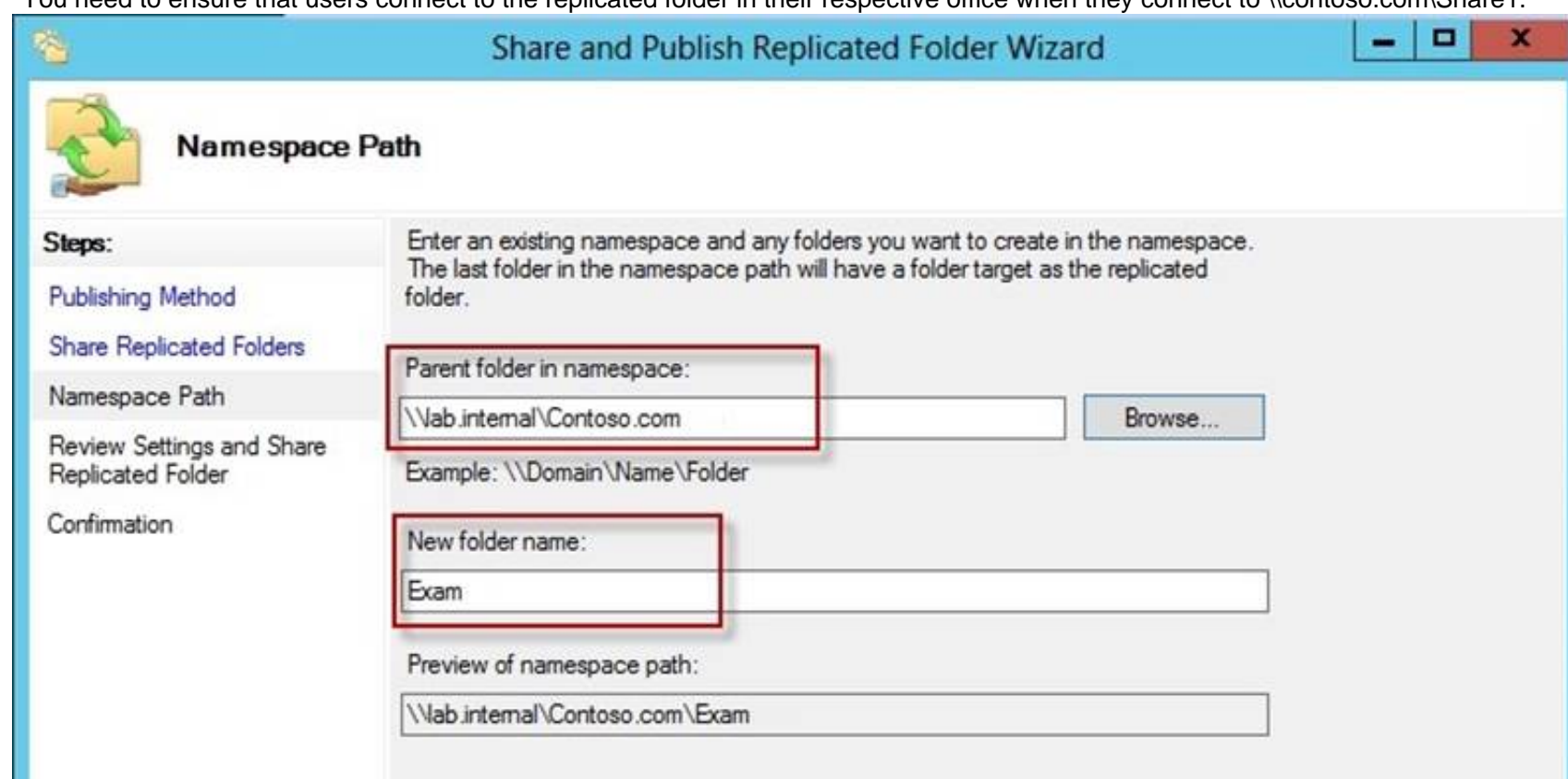
2. In the console tree, under the Replication node, click the replication group that contains the replicated folder you want to share.

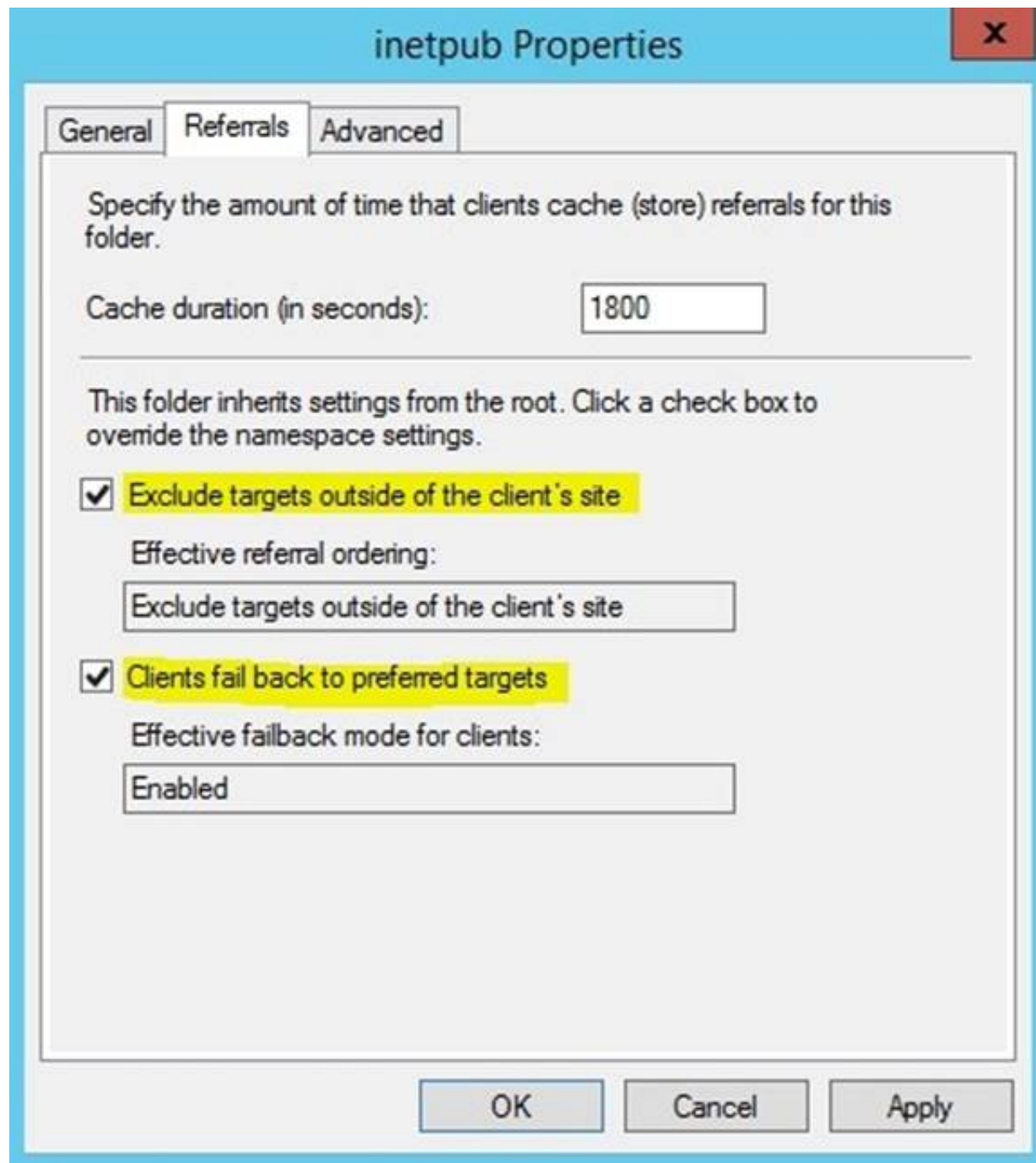
3. In the details pane, on the Replicated Folders tab, right-click the replicated folder that you want to share, and then click Share and Publish in Namespace.

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 133

- (Topic 2)

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

Files created by users in the human resources department are assigned the Department classification property automatically.

You are configuring a file management task named Task1 to remove user files that have not been accessed for 60 days or more.

You need to ensure that Task1 only removes files that have a Department classification property of human resources. The solution must minimize administrative effort.

What should you configure on Task1?

- A. Configure a file screen
- B. Create a condition
- C. Create a classification rule
- D. Create a custom action

Answer: B

Explanation:

Create a File Expiration Task

The following procedure guides you through the process of creating a file management task for expiring files. File expiration tasks are used to automatically move all files that match certain criteria to a specified expiration directory, where an administrator can then back those files up and delete them. Property conditions. Click Add to create a new condition based on the file's classification. This will open the Property Condition dialog box, which allows you to select a property, an operator to perform on the property, and the value to compare the property against. After clicking OK, you can then create additional conditions, or edit or remove an existing condition.

NEW QUESTION 137

- (Topic 2)

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

You plan to create a new Active Directory-integrated zone named contoso.com. You need to ensure that the new zone will be replicated to only four of the domain controllers.

What should you do first?

- A. Create an application directory partition.

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

Answer: A

Explanation:

Application directory partitions

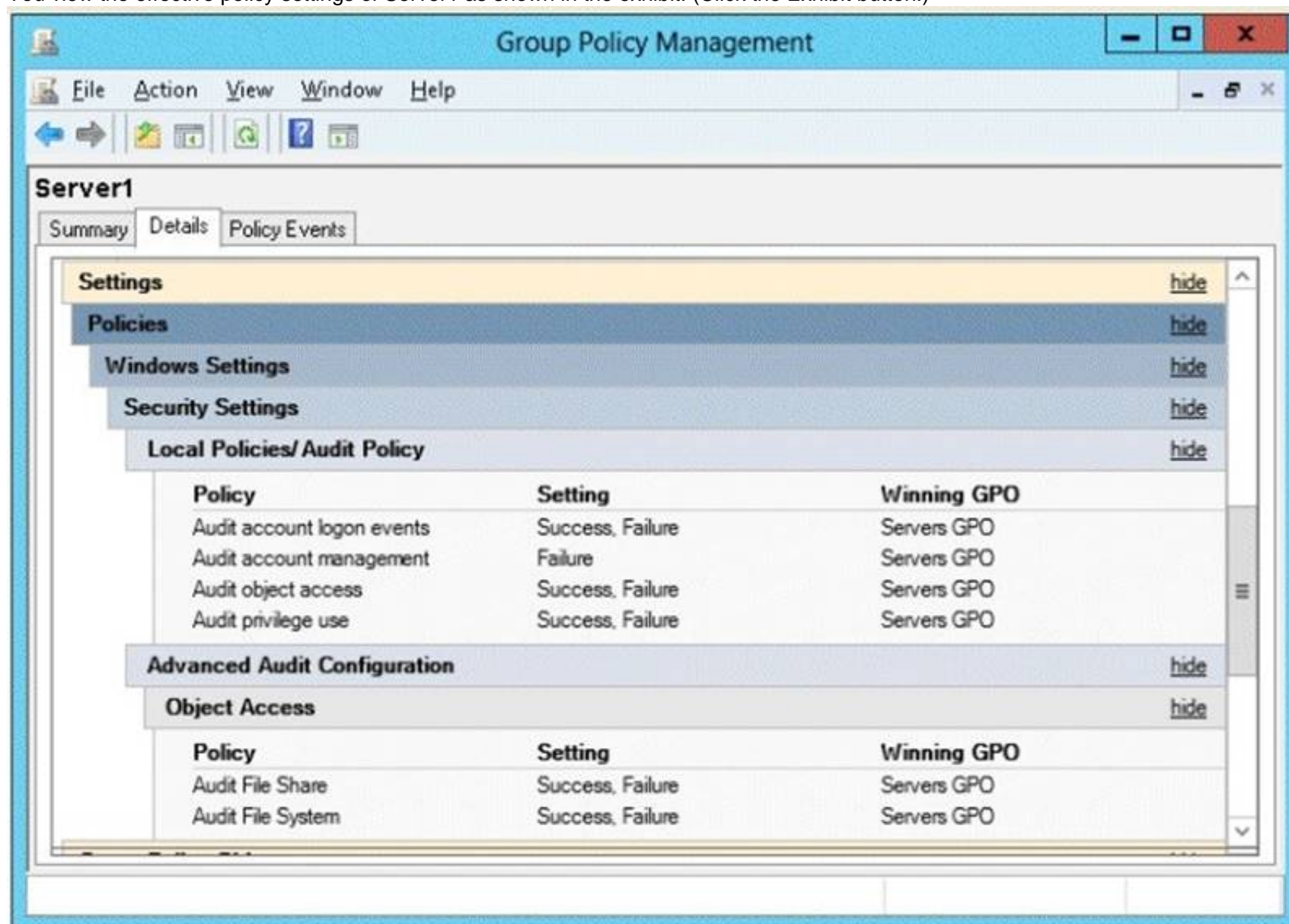
An application directory partition is a directory partition that is replicated only to specific domain controllers. A domain controller that participates in the replication of a particular application directory partition hosts a replica of that partition. Only domain controllers running Windows Server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

NEW QUESTION 138

- (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.

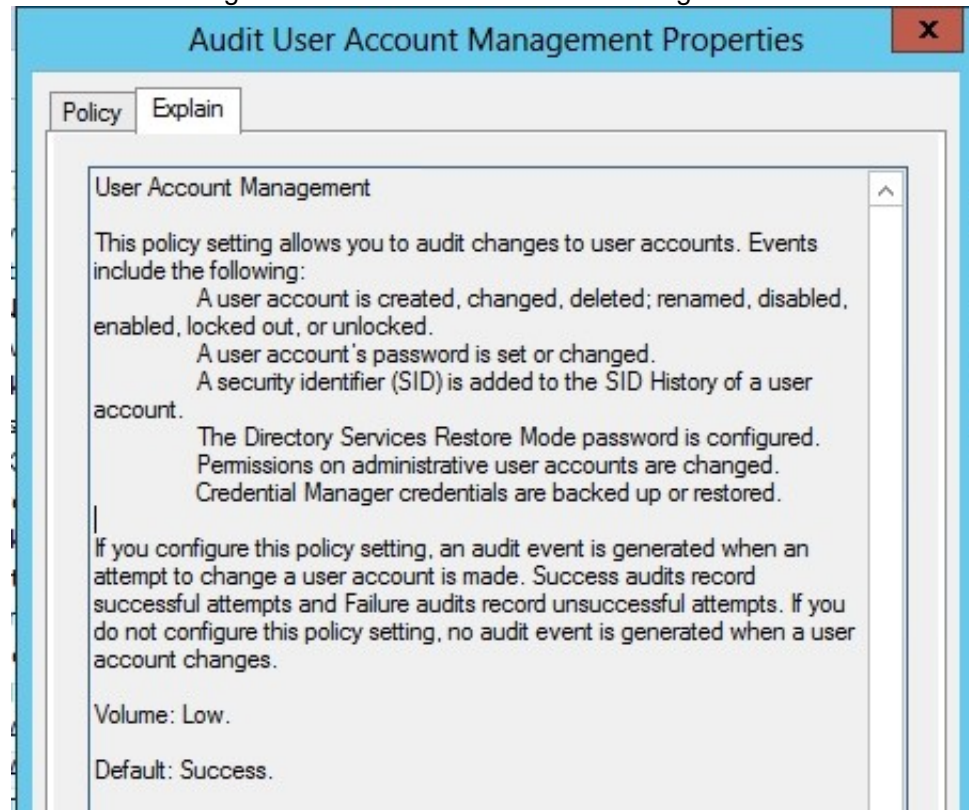
? The correct system access control list (SACL) is applied to every file and folder or registry key on a computer or file share as a verifiable safeguard against undetected access.

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

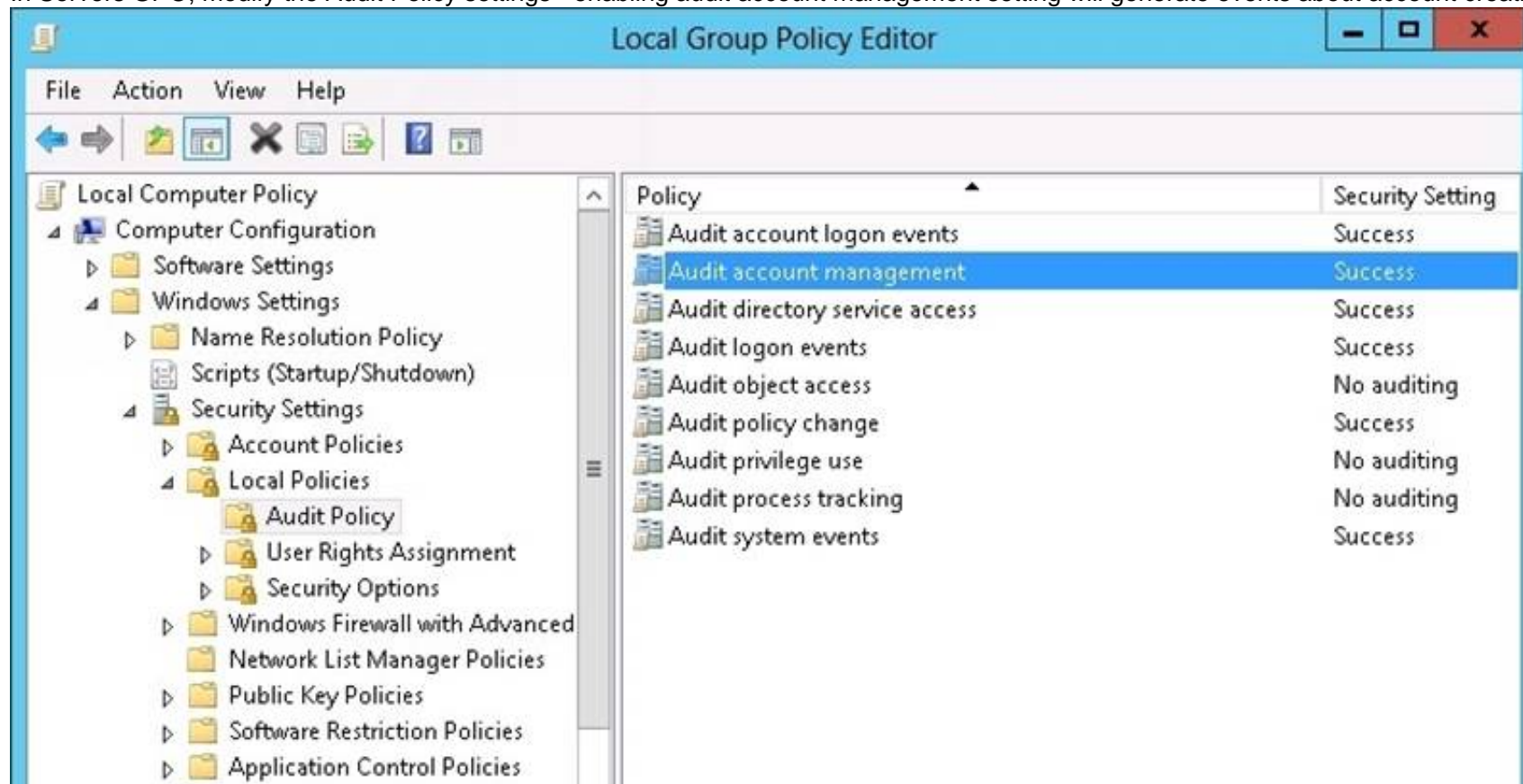
Advanced Audit Configuration Settings

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 142

- (Topic 2)

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

An organizational unit (OU) named OU1 contains 200 client computers that run Windows 8 Enterprise. A Group Policy object (GPO) named GPO1 is linked to OU1.

You make a change to GPO1.

You need to force all of the computers in OU1 to refresh their Group Policy settings

immediately. The solution must minimize administrative effort. Which tool should you use?

- A. The Secedit command
- B. The Invoke-GpUpdate cmdlet
- C. Group Policy Object Editor
- D. Server Manager

Answer: B

Explanation:

Invoke-GPUdate

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

The Invoke-GPUdate cmdlet refreshes Group Policy settings, including security settings that are set on remote computers by scheduling the running of the Gpupdate command on a remote computer. You can combine this cmdlet in a scripted fashion to schedule the Gpupdate command on a group of computers. The refresh can be scheduled to immediately start a refresh of policy settings or wait for a specified period of time, up to a maximum of 31 days. To avoid putting a load on the network, the refresh times will be offset by a random delay.

Note:

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

The remote Group Policy refresh updates all Group Policy settings, including security settings that are set on a group of remote computers, by using the functionality that is added to the context menu for an OU in the Group Policy Management Console (GPMC). When you select an OU to remotely refresh the Group Policy settings on all the computers in that OU, the following operations happen:

? An Active Directory query returns a list of all computers that belong to that OU.

? For each computer that belongs to the selected OU, a WMI call retrieves the list of signed in users.

? A remote scheduled task is created to run GPUdate.exe /force for each signed in

user and once for the computer Group Policy refresh. The task is scheduled to run with a random delay of up to 10 minutes to decrease the load on the network traffic. This random delay cannot be configured when you use the GPMC, but you can configure the random delay for the scheduled task or set the scheduled task to run immediately when you use the Invoke-GPUdate cmdlet.

Reference: Force a Remote Group Policy Refresh (GPUdate)

NEW QUESTION 144

- (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?

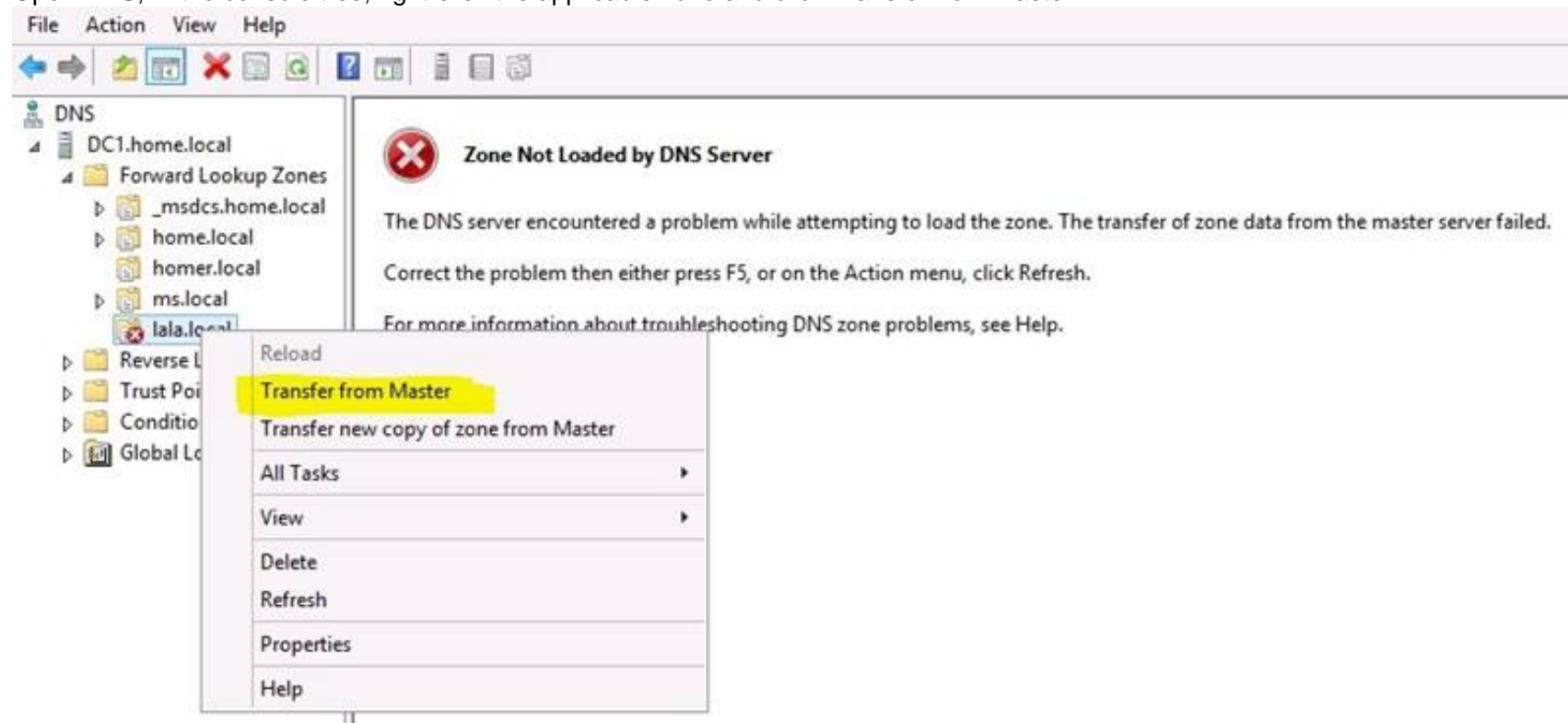
- A. Right-click the contoso.com zone and click Reload.
- B. Right-click the contoso.com zone and click Transfer from Master.
- C. Right-click Server2 and click Update Server Data Files.
- D. Right-click Server2 and click Refresh.

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 149

- (Topic 2)

Your network contains two Active Directory forests named contoso.com and adatum.com. The contoso.com forest contains a server named Server1.contoso.com. The adatum.com forest contains a server named server2. adatum.com. Both servers have the Network Policy Server role service installed.

The network contains a server named Server3. Server3 is located in the perimeter network and has the Network Policy Server role service installed.

You plan to configure Server3 as an authentication provider for several VPN servers. You need to ensure that RADIUS requests received by Server3 for a specific VPN server

are always forwarded to Server1.contoso.com.

Which two should you configure on Server3? (Each correct answer presents part of the solution. Choose two.)

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

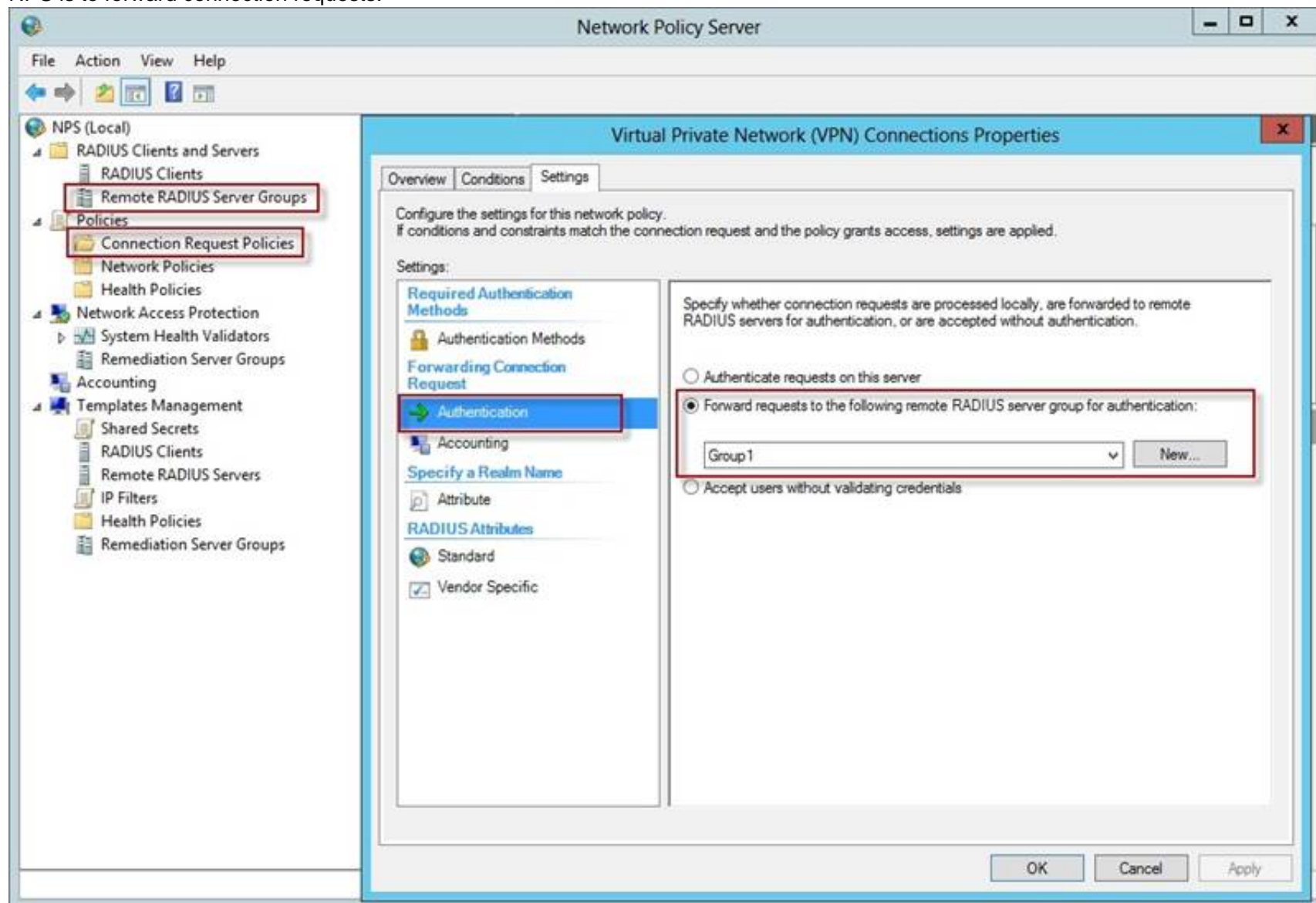
Answer: BC

Explanation:

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

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

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



References:

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

NEW QUESTION 150

- (Topic 2)

You have a server that runs Windows Server 2012 R2.

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

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 154

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The network contains several group Managed Service Accounts that are used by four member servers. You need to ensure that if a group Managed Service Account resets a password of a domain user account, an audit entry is created. You create a Group Policy object (GPO) named GPO1. What should you do next?

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

Answer: A

Explanation:

Audit User Account Management

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

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

? A user account password is set or changed.

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

? The Directory Services Restore Mode password is set.

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

? Credential Manager credentials are backed up or restored.

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

NEW QUESTION 158

- (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 server role installed.

You need to allow connections that use 802.1x. What should you create?

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

Answer: C

Explanation:

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

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

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

? EAP-MS-CHAP v2 (EAP-Microsoft Challenge Handshake Authentication Protocol version 2) is a mutual authentication method that supports password-based user or computer authentication.

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

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

With connection request policies, you can use NPS as a RADIUS server or as a RADIUS proxy, based on factors such as the following:

? The time of day and day of the week

? The realm name in the connection request

? The type of connection being requested

? The IP address of the RADIUS client

NEW QUESTION 162

- (Topic 2)

Your company has a main office and a branch office.

The main office contains a server that hosts a Distributed File System (DFS) replicated folder.

You plan to implement a new DFS server in the branch office.

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

You recommend using the Export-DfsrClone and Import-DfsrClonecmdlets. Which additional command or cmdlet should you include in the recommendation?

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

Answer: A

Explanation:

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

NEW QUESTION 166

- (Topic 2)

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

Windows Server 2012 R2.

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

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

Answer: C

Explanation:

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

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

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

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

References:

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

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

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

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

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

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

NEW QUESTION 169

- (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

- (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed. Each time a user receives an access-denied message after attempting to access a folder on Server1, an email notification is sent to a distribution list named DL1. You create a folder named Folder1 on Server1, and then you configure custom NTFS permissions for Folder 1. You need to ensure that when a user receives an access-denied message while attempting to access Folder1, an email notification is sent to a distribution list named DL2. The solution must not prevent DL1 from receiving notifications about other access-denied messages. What should you do?

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

Answer: C

Explanation:

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

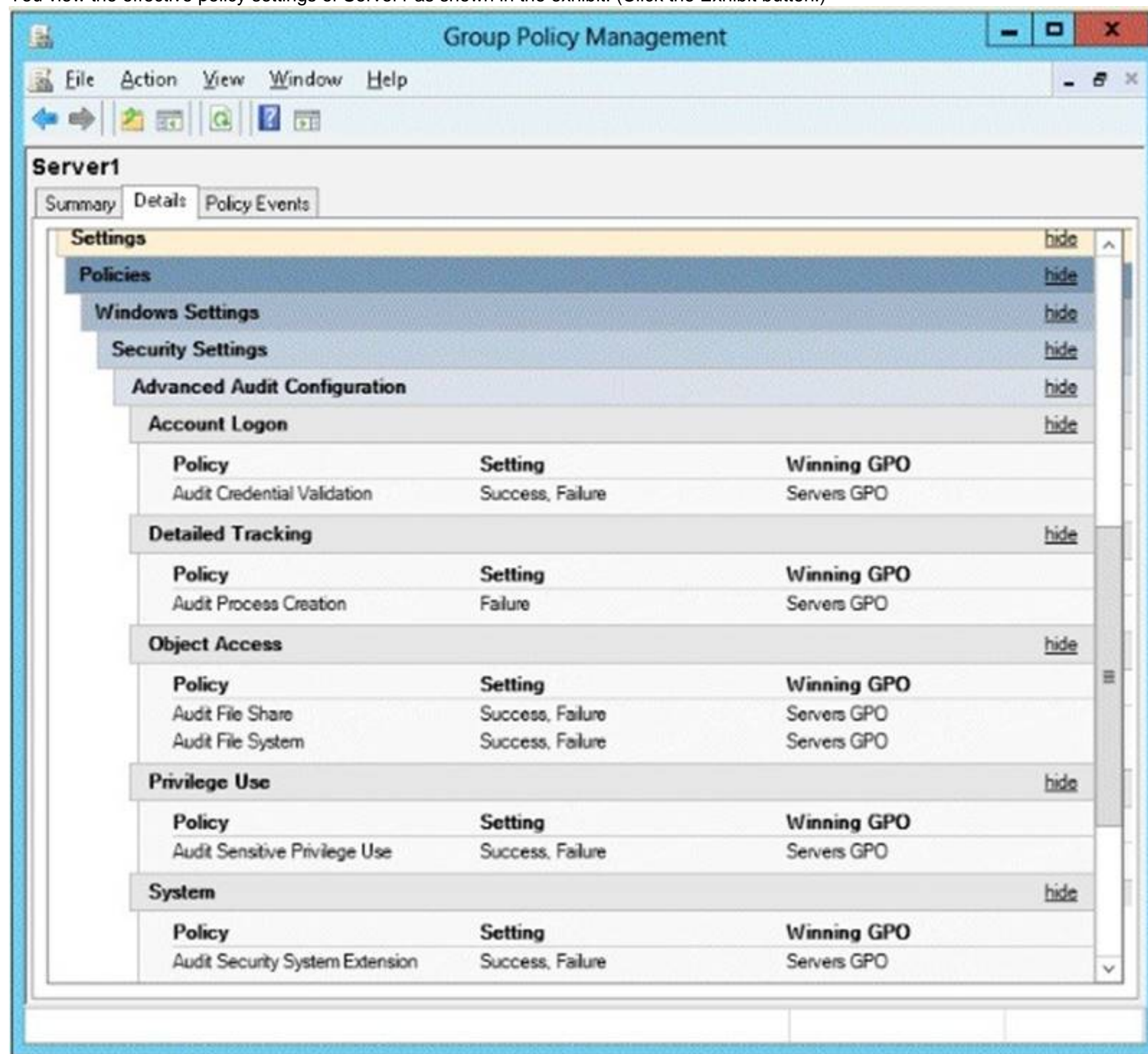
You can use the File Server Resource Manager console to configure the owner distribution list by editing the management properties of the classification properties.

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

NEW QUESTION 172

- (Topic 2)

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



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

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

What should you configure?

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

Answer: D

Explanation:

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

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

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

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

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

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

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

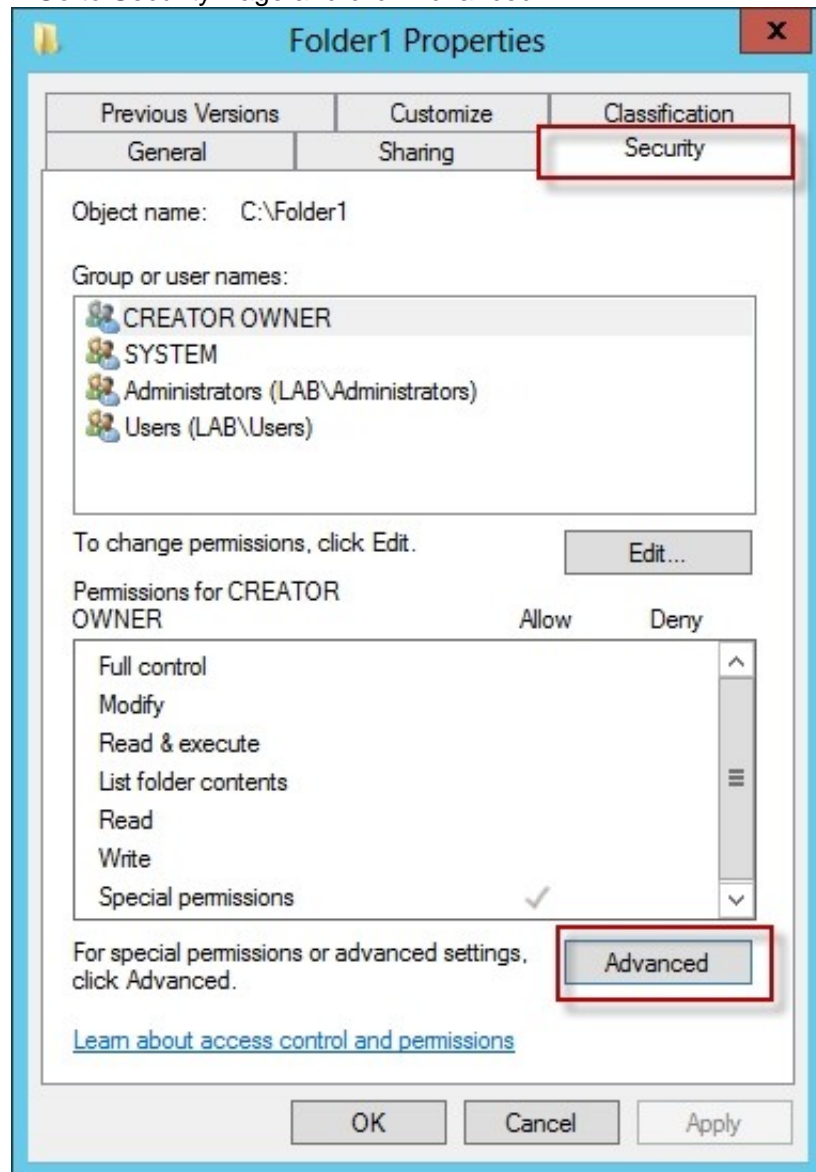
? Click start and run "secpol. msc" without quotes.

? Open the Local Policies\Audit Policy

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

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

? Go to Security Page and click Advanced.



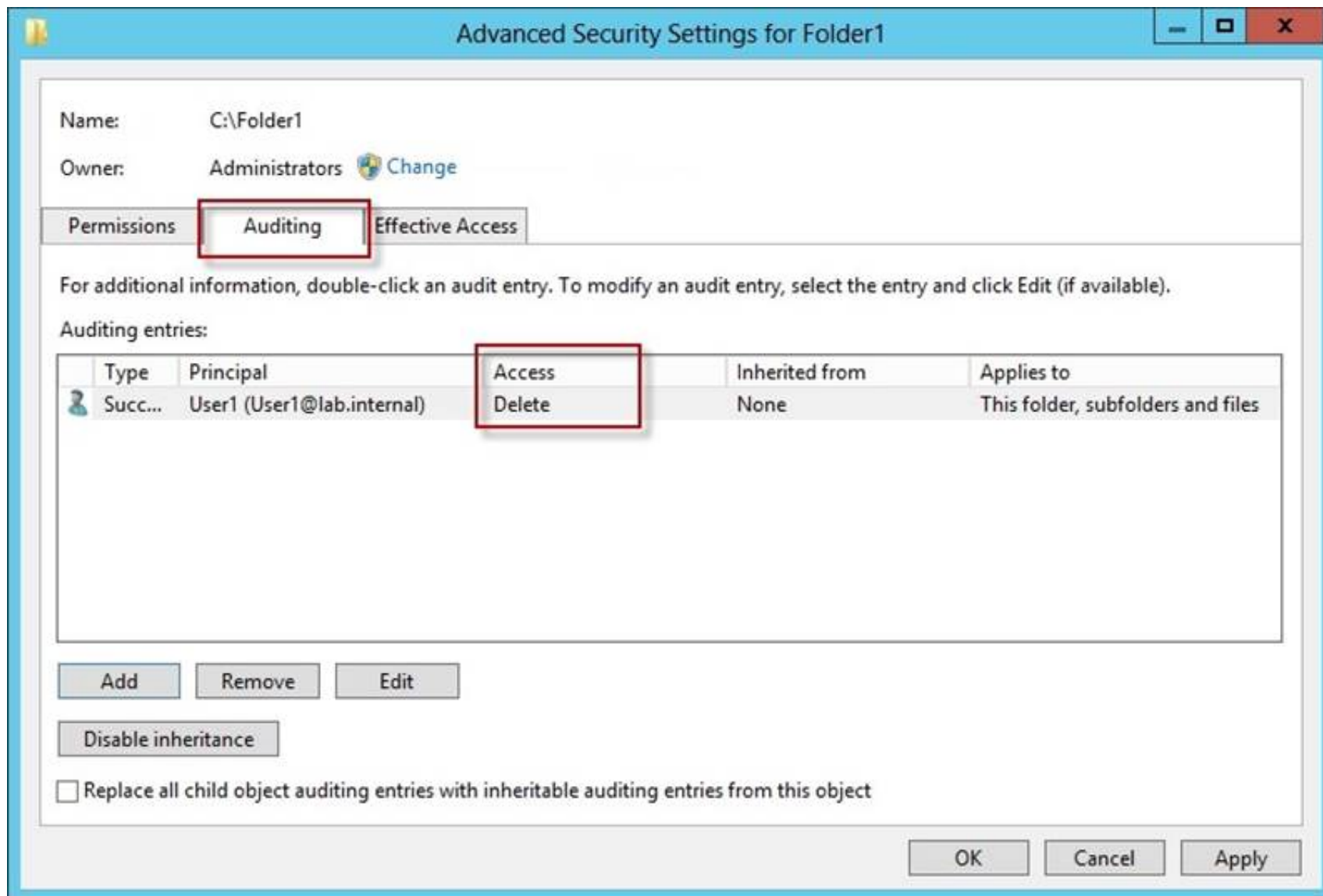
? Click Auditing and Edit.

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

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

? Tick on the box "Change permissions"

? Click OK.



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

References:

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

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

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

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

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

NEW QUESTION 177

HOTSPOT - (Topic 2)

You have a server named Server1 that runs Windows Server 2012 R2. You configure Network Access Protection (NAP) on Server1.

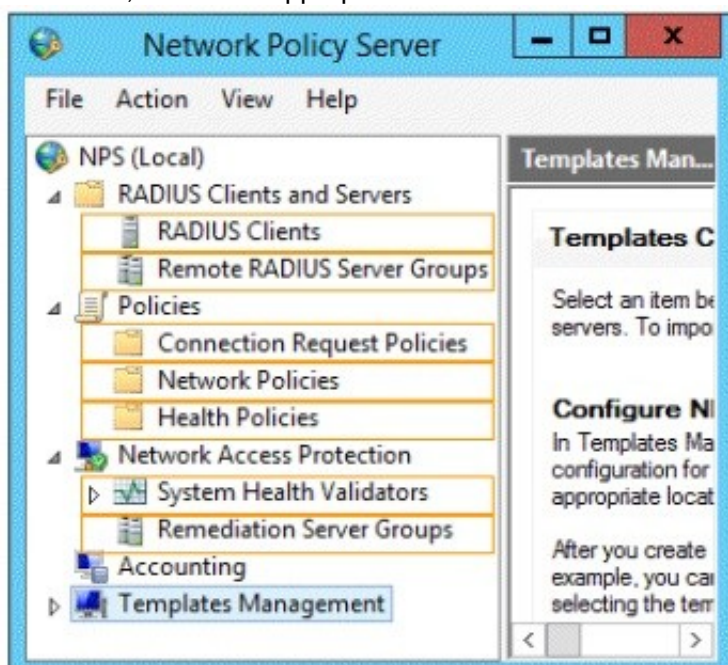
Your company implements a new security policy stating that all client computers must have the latest updates installed. The company informs all employees that they have two weeks

to update their computer accordingly.

You need to ensure that if the client computers have automatic updating disabled, they are provided with full access to the network until a specific date and time.

Which two nodes should you configure?

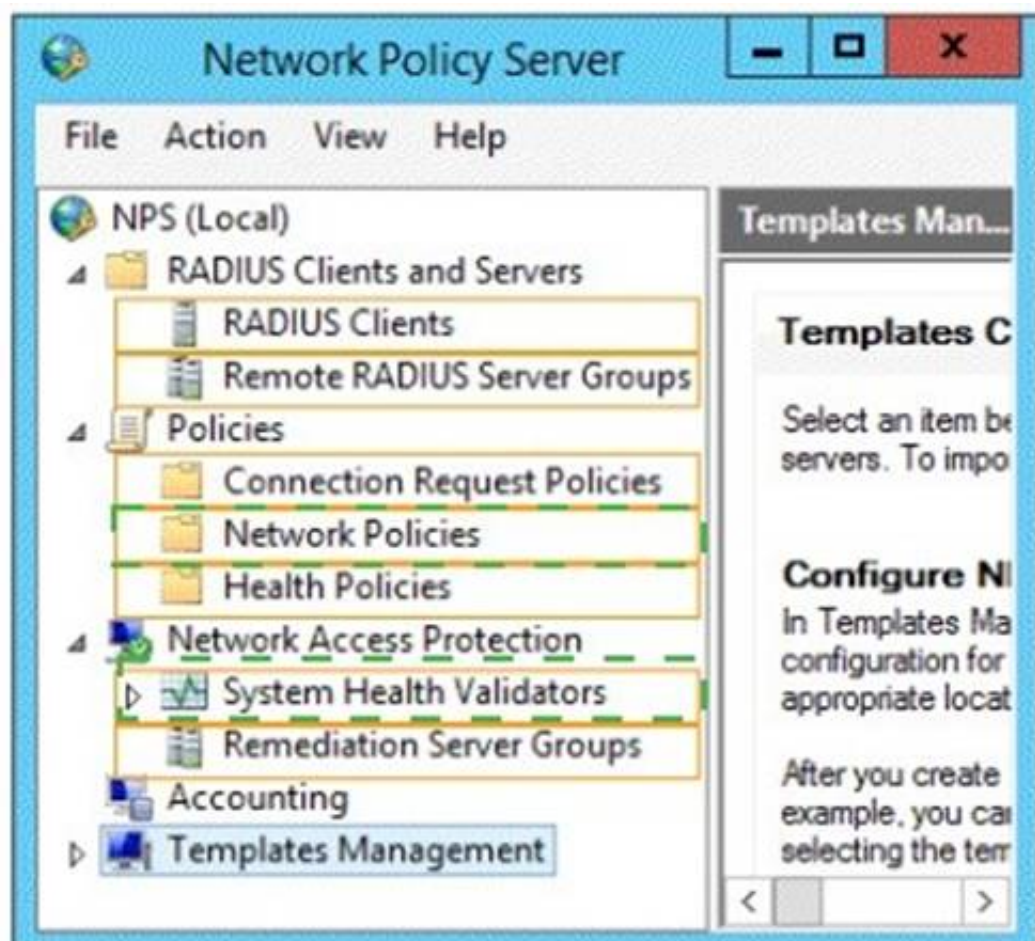
To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



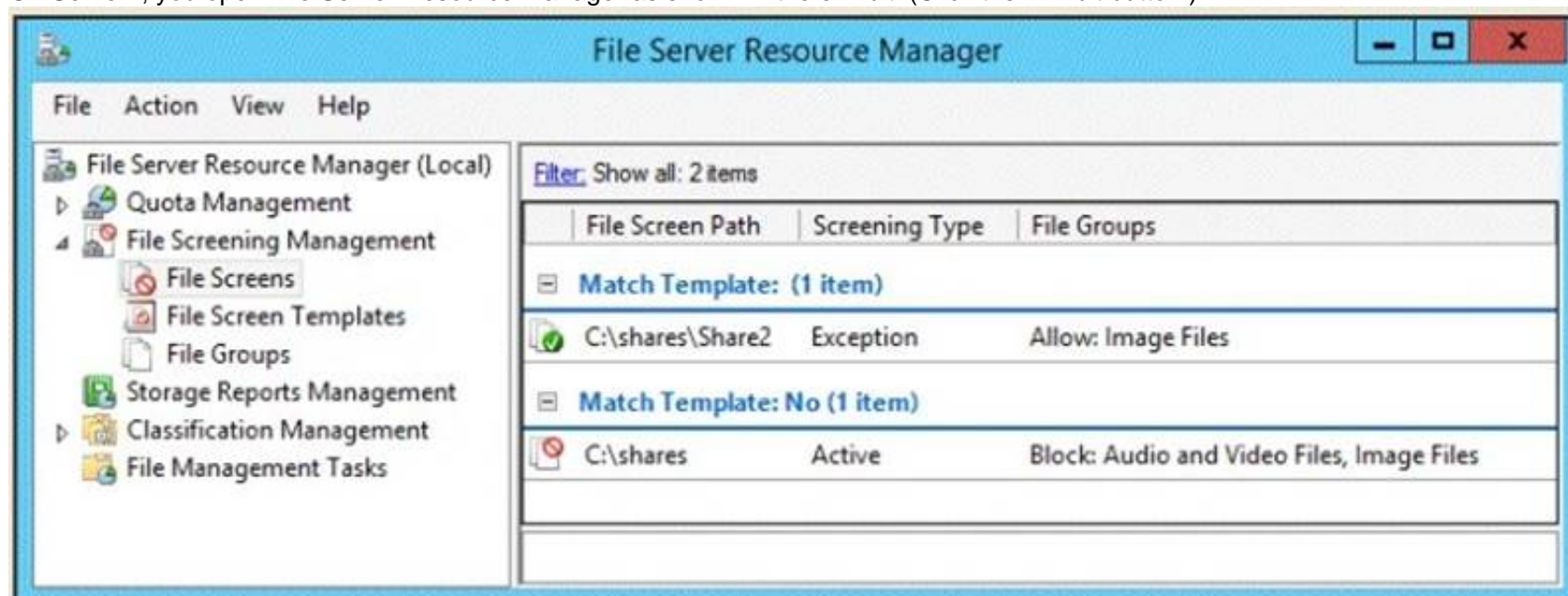
NEW QUESTION 180

HOTSPOT - (Topic 2)

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

A user named User1 is assigned the modify NTFS permission to a folder named C:\shares and all of the subfolders of C:\shares.

On Server1, you open File Server Resource Manager as shown in the exhibit. (Click the Exhibit button.)



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

Answer Area

User1 can copy a file named ... to C:\shares.

User1 cannot copy a file named ... to a folder named C:\shares\share2.

Answer Area

User1 can copy a file named ... to C:\shares.

File1.gif
 File2.bmp
 File3.jpg.zip
 File4.mp3

User1 cannot copy a file named ... to a folder named C:\shares\share2.

File1.gif
 File2.bmp
 File3.jpg.zip
 File4.mp3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1 can copy a file named ... to C:\shares.

User1 cannot copy a file named ... to a folder named C:\shares\share2.



NEW QUESTION 183

- (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\ntp. 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\ntp\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 184

- (Topic 2)

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

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

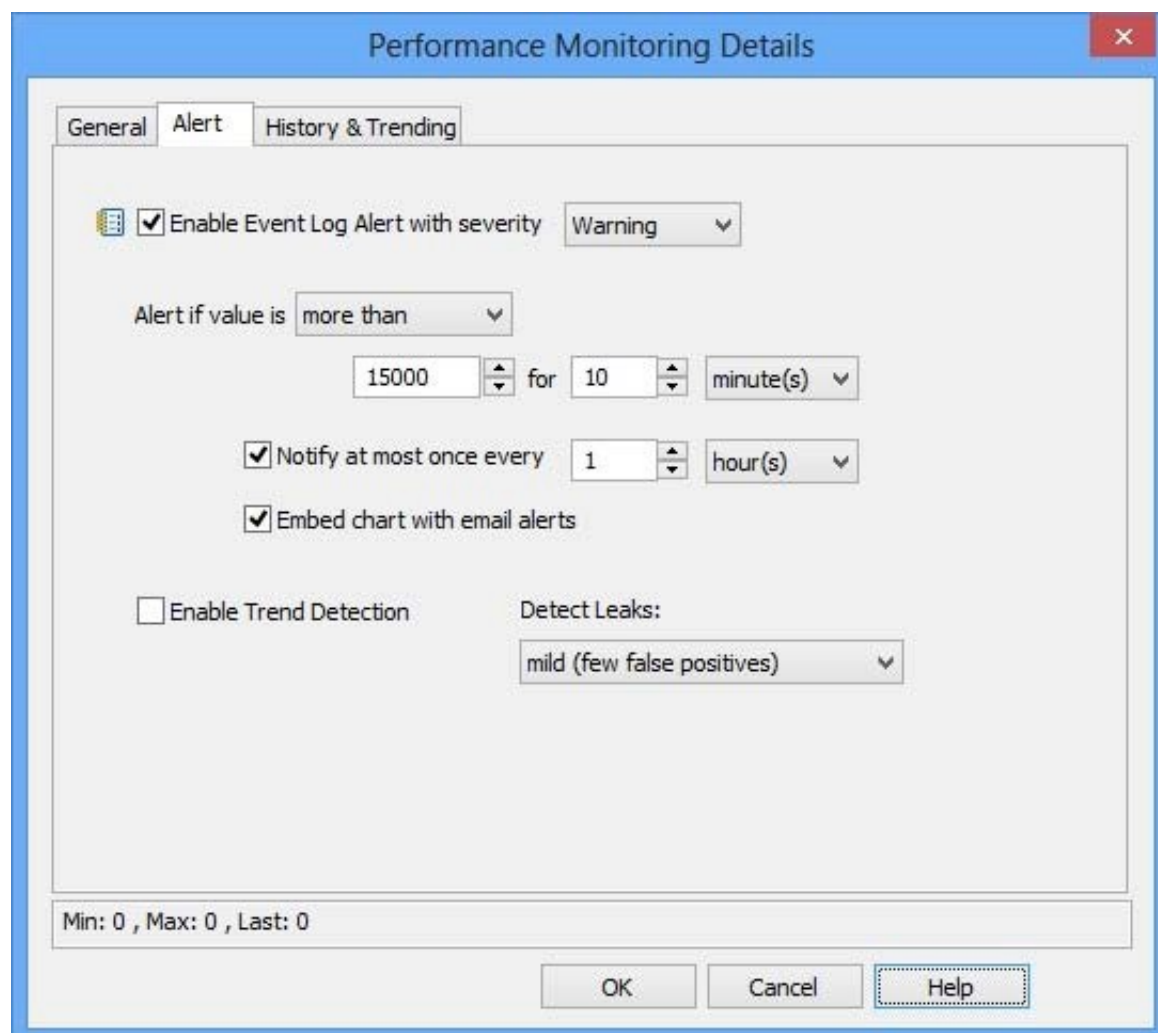
Which type of data collector should you create?

- A. A performance counter alert
- B. A configuration data collector
- C. A performance counter data collector
- D. An event trace data collector

Answer: A

Explanation:

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



The image shows a Windows-style dialog box titled "Performance Monitoring Details". It has three tabs: "General", "Alert", and "History & Trending". The "Alert" tab is selected. Inside the dialog, there are several settings:

- ☒ Enable Event Log Alert with severity: Warning (dropdown)
- Alert if value is: more than (dropdown)
- 15000 (spin box) for 10 (spin box) minute(s) (dropdown)
- ☒ Notify at most once every: 1 (spin box) hour(s) (dropdown)
- ☒ Embed chart with email alerts
- ☐ Enable Trend Detection
- Detect Leaks: mild (few false positives) (dropdown)

At the bottom, there is a status bar showing "Min: 0 , Max: 0 , Last: 0". Below the dialog box are three buttons: "OK", "Cancel", and "Help".

NEW QUESTION 187

HOTSPOT - (Topic 2)

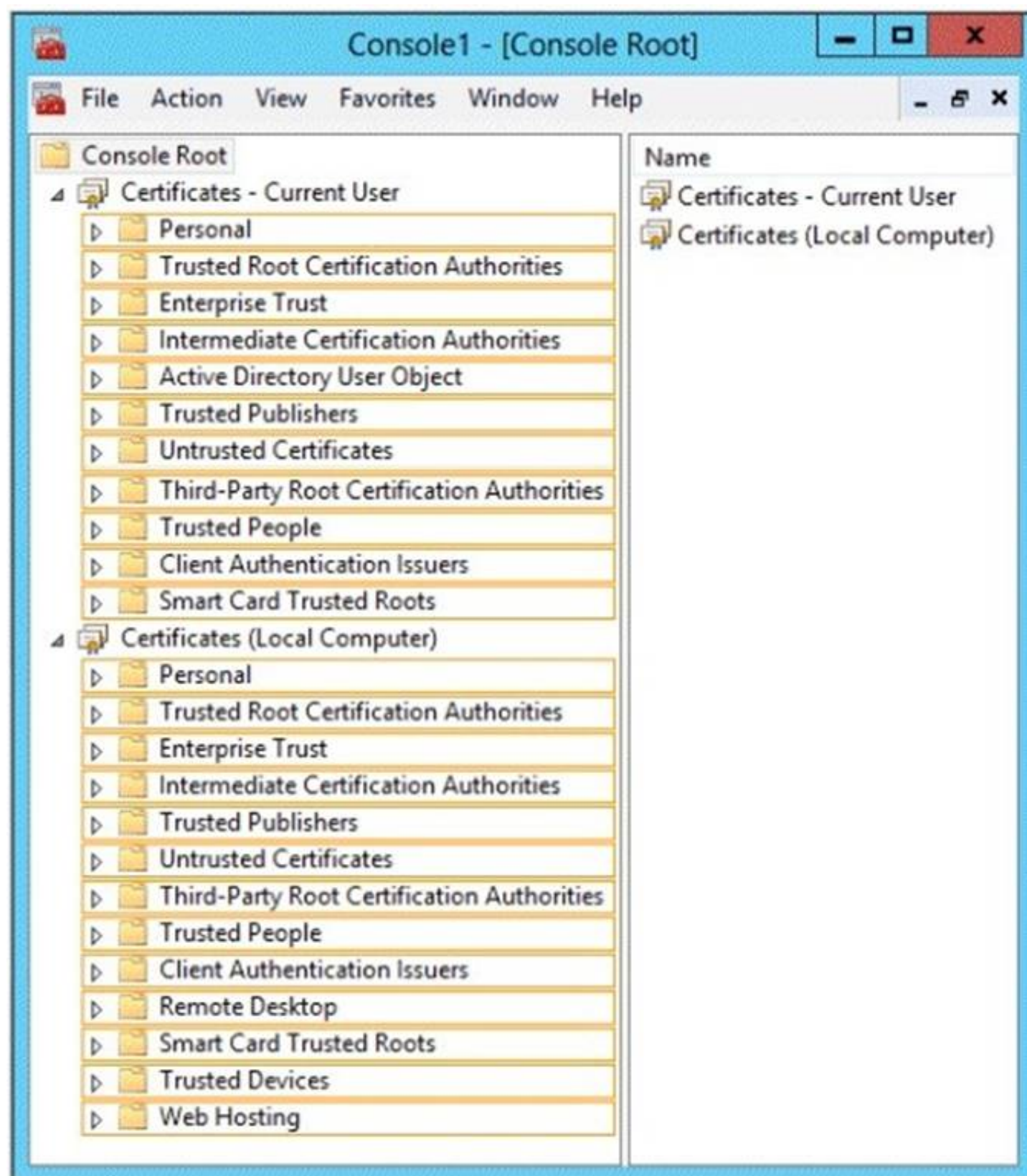
You have a server named Server1 that has the Network Policy and Access Services server role installed.

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

You obtain a certificate for NPS.

You need to ensure that NPS can perform certificate-based authentication. To which store should you import the certificate?

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

When organizations deploy their own public key infrastructure (PKI) and install a private trusted root CA, their CA automatically sends its certificate to all domain member computers in the organization. The domain member client and server computers store the CA certificate in the Trusted Root Certification Authorities certificate store. After this occurs, the domain member computers trust certificates that are issued by the organization trusted root CA.

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

On computers that are running the Windows operating system, certificates that are installed on the computer are kept in a storage area called the certificate store. The certificate store is accessible using the Certificates Microsoft Management Console (MMC) snap-in.

This store contains multiple folders, where certificates of different types are stored. For example, the certificate store contains a Trusted Root Certification Authorities folder where the certificates from all trusted root CAs are kept.

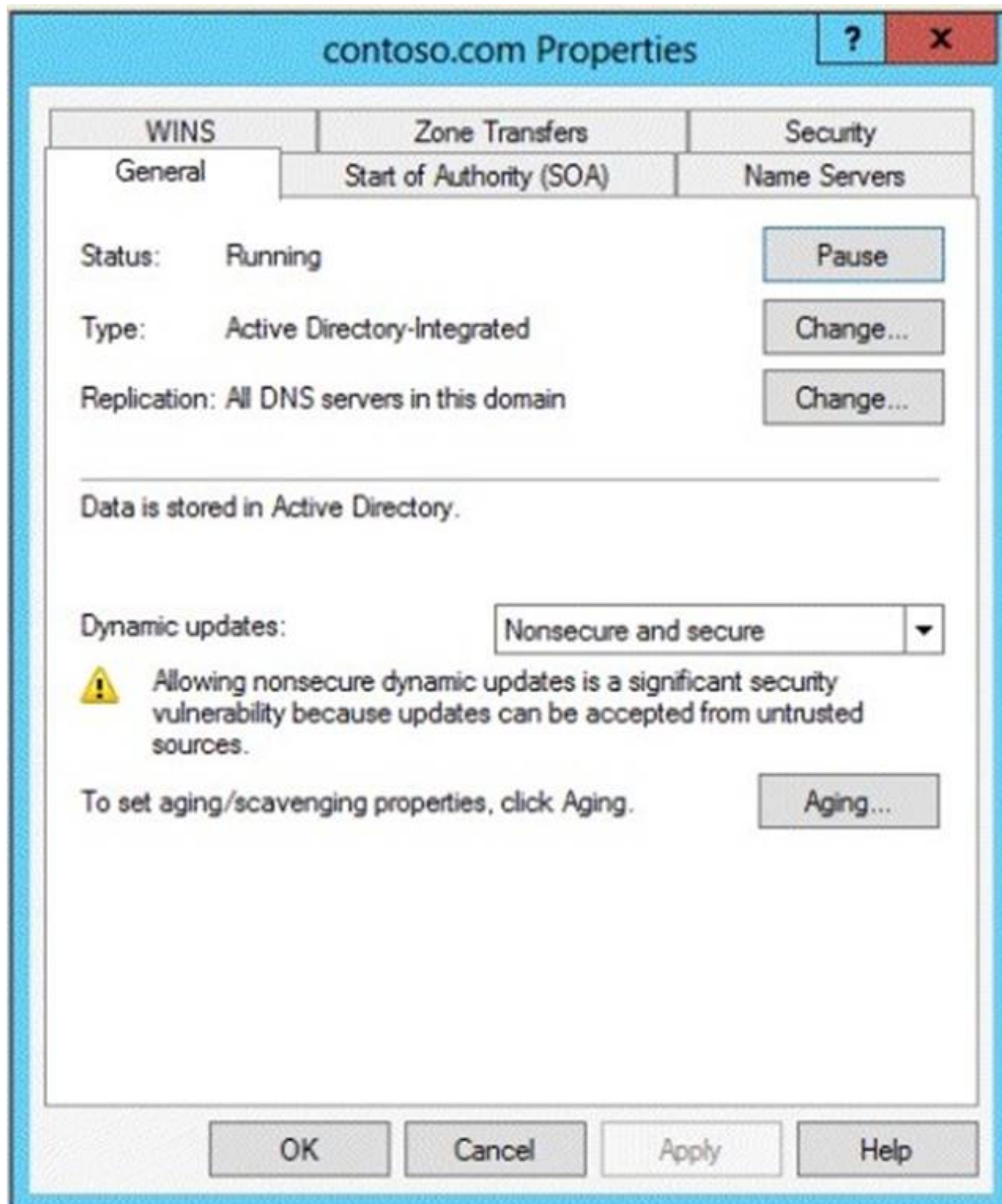
When your organization deploys a PKI and installs a private trusted root CA using AD CS, the CA automatically sends its certificate to all domain member computers in the organization. The domain member client and server computers store the CA certificate in the Trusted Root Certification Authorities folder in the Current User and the Local Computer certificate stores. After this occurs, the domain member computers trust certificates that are issued by the trusted root CA. Similarly, when you autoenroll computer certificates to domain member client computers, the certificate is kept in the Personal certificate store for the Local Computer. When you autoenroll certificates to users, the user certificate is kept in the Personal certificate store for the Current User.

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

NEW QUESTION 191

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1. DC1 is a DNS server for contoso.com. The properties of the contoso.com zone are configured as shown in the exhibit. (Click the Exhibit button.)



The domain contains a server named Server1 that is part of a workgroup named Workgroup. Server1 is configured to use DC1 as a DNS server. You need to ensure that Server1 dynamically registers a host (A) record in the contoso.com zone. What should you configure?

- A. The workgroup name of Server1
- B. The Security settings of the contoso.com zone
- C. The Dynamic updates setting of the contoso.com zone
- D. The primary DNS suffix of Server1

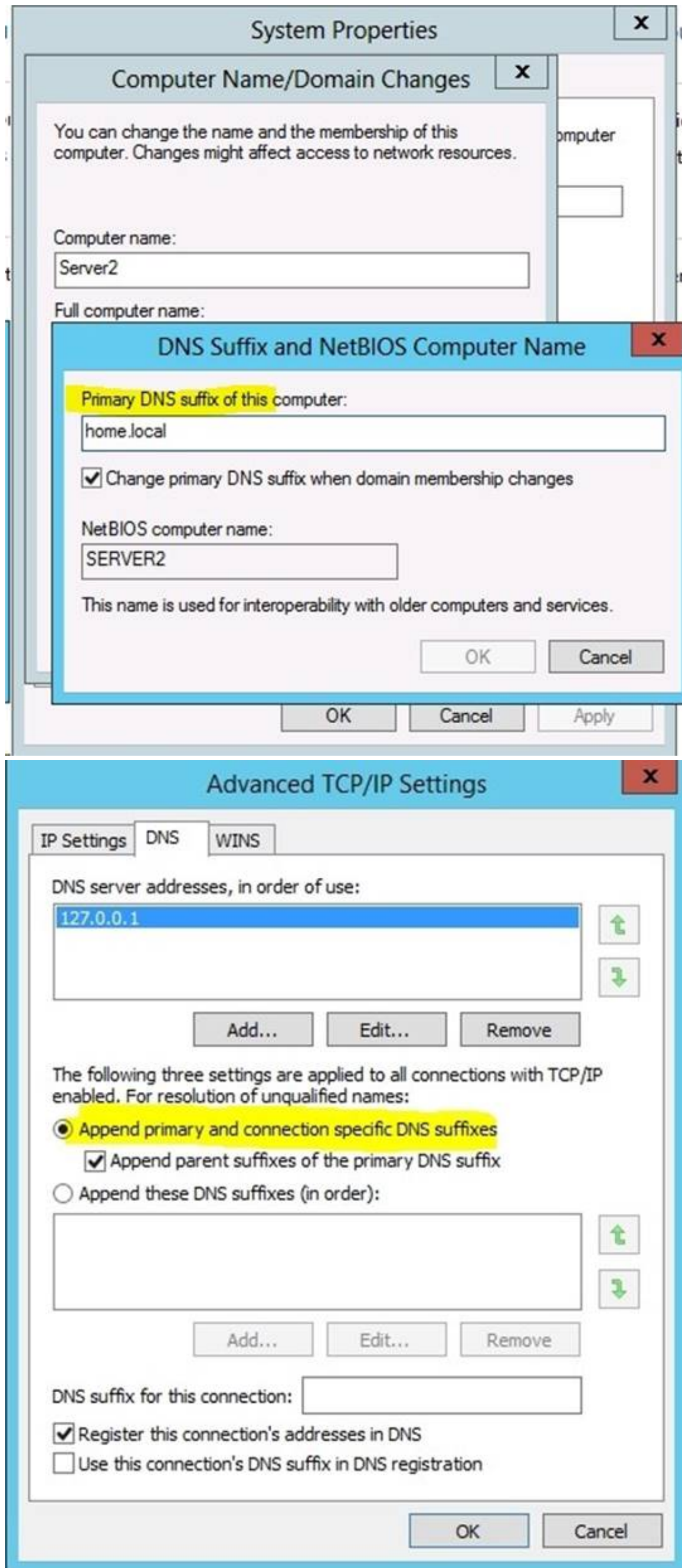
Answer: D

Explanation:

When any computer or a standalone server is added to a domain as a member, the network identifies that computer with its Fully Qualified Domain Name or FQDN. A Fully Qualified Domain Name consist of a hostname and the DNS suffix separated by a "." called period. An example for this can be server01.msftdomain.com where "server01" is the hostname of the computer and "msftdomain.com" is the DNS suffix which follows the hostname. A complete FQDN of a client computer or a member server uniquely identifies that computer in the entire domain.

Primary DNS suffix must manually be added in Windows 8 computer to change its hostname to Fully Qualified Domain Name so that it becomes eligible to send queries and receive responses from the DNS server. Following are the steps which can be implemented to add primary DNS suffix to a Windows 8 computer hostname:

- ? Log on to Windows 8 computer with administrator account.
- ? From the options available on the screen click Control Panel.
- ? On the opened window click More Settings from the left pane.
- ? On the next window click System and Security category and on the appeared window click System.
- ? On View basic information about your computer window click Change settings under Computer name, domain, and workgroup settings section.
- ? On System Properties box make sure that Computer Name tab is selected and click Change button.
- ? On Computer Name/Domain Changes box click More button.
- ? On DNS Suffix and NetBIOS Computer Name box type in the DNS domain name as the DNS suffix to the Windows 8 computer under Primary DNS suffix of this computer field.
- ? Click Ok button on all the boxes and restart the computer to allow changes to take effect.



For years, Windows DNS has supported dynamic updates, whereas a DNS client host registers and dynamically updates the resource records with a DNS server. If a host's IP address changes, the resource record (particularly the A record) for the host is automatically updated, while the host utilizes the DHCP server to dynamically update its Pointer (PTR) resource record. Therefore, when a user or service needs to contact a client PC, it can look up the IP address of the host. With larger organizations, this becomes an essential feature, especially for clients that frequently move or change locations and use DHCP to automatically obtain an IP address. For dynamic DNS updates to succeed, the zone must be configured to accept dynamic updates:



New Zone Wizard

Dynamic Update
 You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- ☒ **Allow only secure dynamic updates (recommended for Active Directory)**
 This option is available only for Active Directory-integrated zones.
- ☐ Allow both nonsecure and secure dynamic updates
 Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☐ Do not allow dynamic updates
 Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

References:

<http://technet.microsoft.com/en-us/library/cc778792%28v=ws.10%29.aspx>
<http://technet.microsoft.com/en-us/library/cc778792%28v=ws.10%29.aspx>
<http://www.advicehow.com/adding-primary-dns-suffix-in-microsoft-windows-8/>
<http://technet.microsoft.com/en-us/library/cc959611.aspx>

NEW QUESTION 196

- (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 198

- (Topic 2)

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

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

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

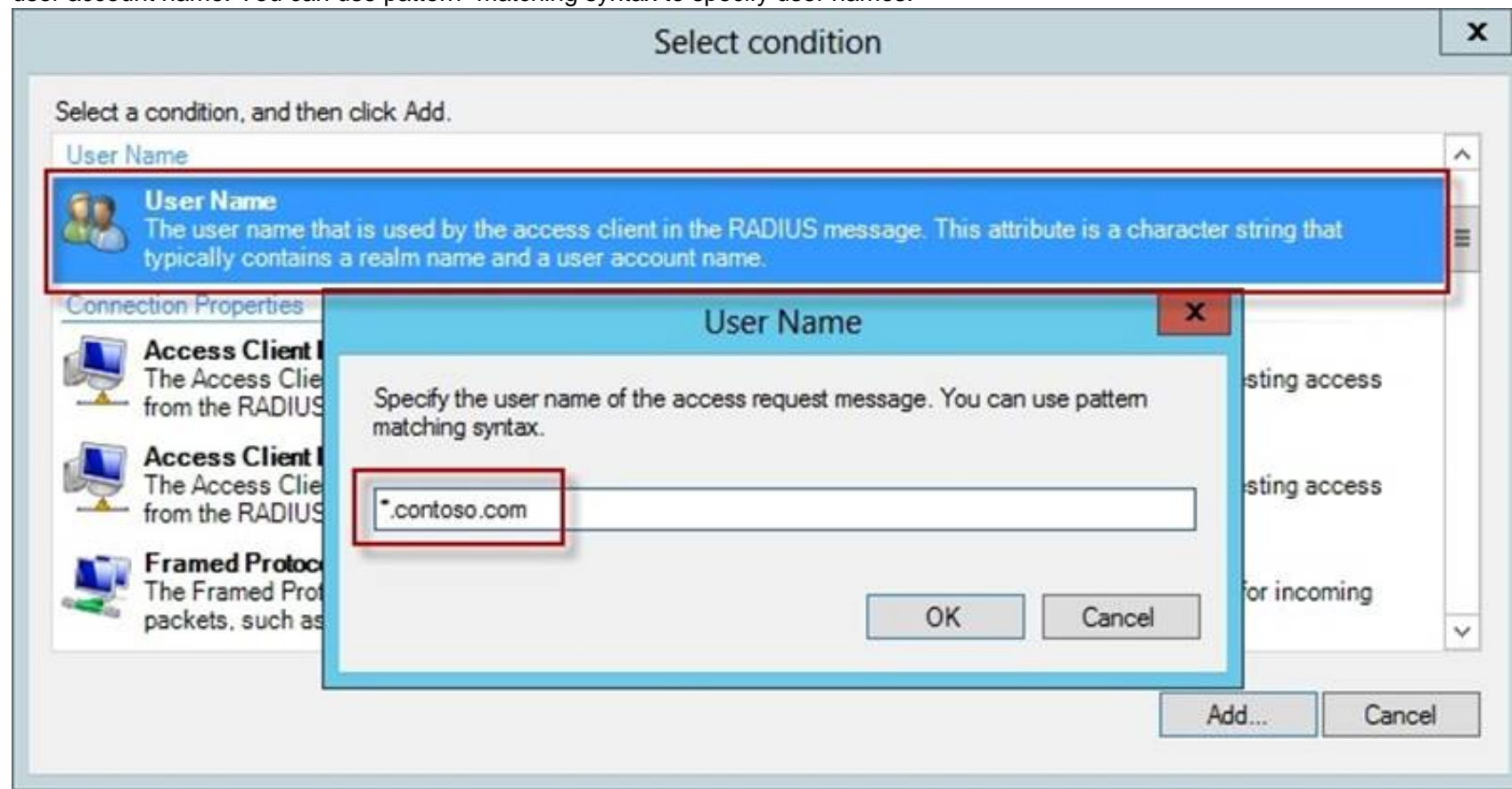
Which two should you configure in the connection request policies on Server1? (Each correct answer presents part of the solution. Choose two.)

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

Answer: AE

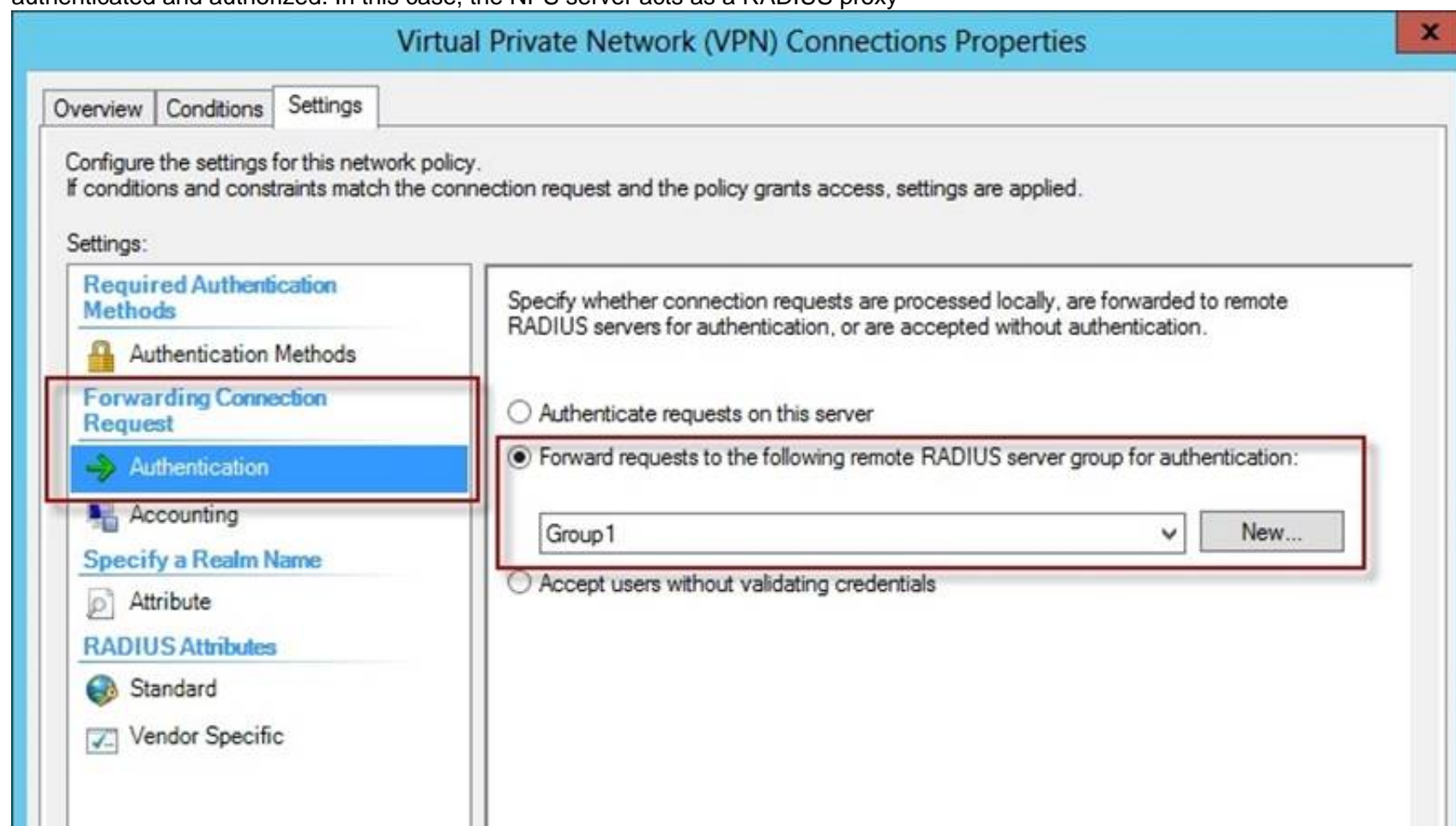
Explanation:

The User Name attribute group contains the User Name attribute. By using this attribute, you can designate the user name, or a portion of the user name, that must match the user name supplied by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name. You can use pattern- matching syntax to specify user names.



By using this setting, you can override the authentication settings that are configured in all network policies and you can designate the authentication methods and types that are required to connect to your network.

Forward requests to the following remote RADIUS server group . By using this setting, NPS forwards connection requests to the remote RADIUS server group that you specify. If the NPS server receives a valid Access-Accept message that corresponds to the Access- Request message, the connection attempt is considered authenticated and authorized. In this case, the NPS server acts as a RADIUS proxy



Connection request policies are sets of conditions and profile settings that give network administrators flexibility in configuring how incoming authentication and accounting request messages are handled by the IAS server. With connection request policies, you can create a series of policies so that some RADIUS request messages sent from RADIUS clients are processed locally (IAS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (IAS is being used as a RADIUS proxy). This capability allows IAS to be deployed in many new RADIUS scenarios.

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

References:

<http://technet.microsoft.com/en-us/library/cc757328.aspx>

<http://technet.microsoft.com/en-us/library/cc753603.aspx>

NEW QUESTION 201

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

70-411 Practice Exam Features:

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

100% Actual & Verified — Instant Download, Please Click
[Order The 70-411 Practice Test Here](#)