

70-411 Dumps

Administering Windows Server 2012

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



NEW QUESTION 1

- (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 2

- (Topic 1)

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

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

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

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

Answer: C

Explanation:

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

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

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

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

auditpol /resourceSACL

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

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

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

References:

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

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

NEW QUESTION 3

- (Topic 1)

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

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

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

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

You implement a Distributed File System (DFS) replication group named Rep1Group. Rep1Group is used to replicate a folder on each file server. Rep1Group uses a hub and

spoke topology. NYC-SVR1 is configured as the hub server. You need to ensure that replication can occur if NYC-SVR1 fails.

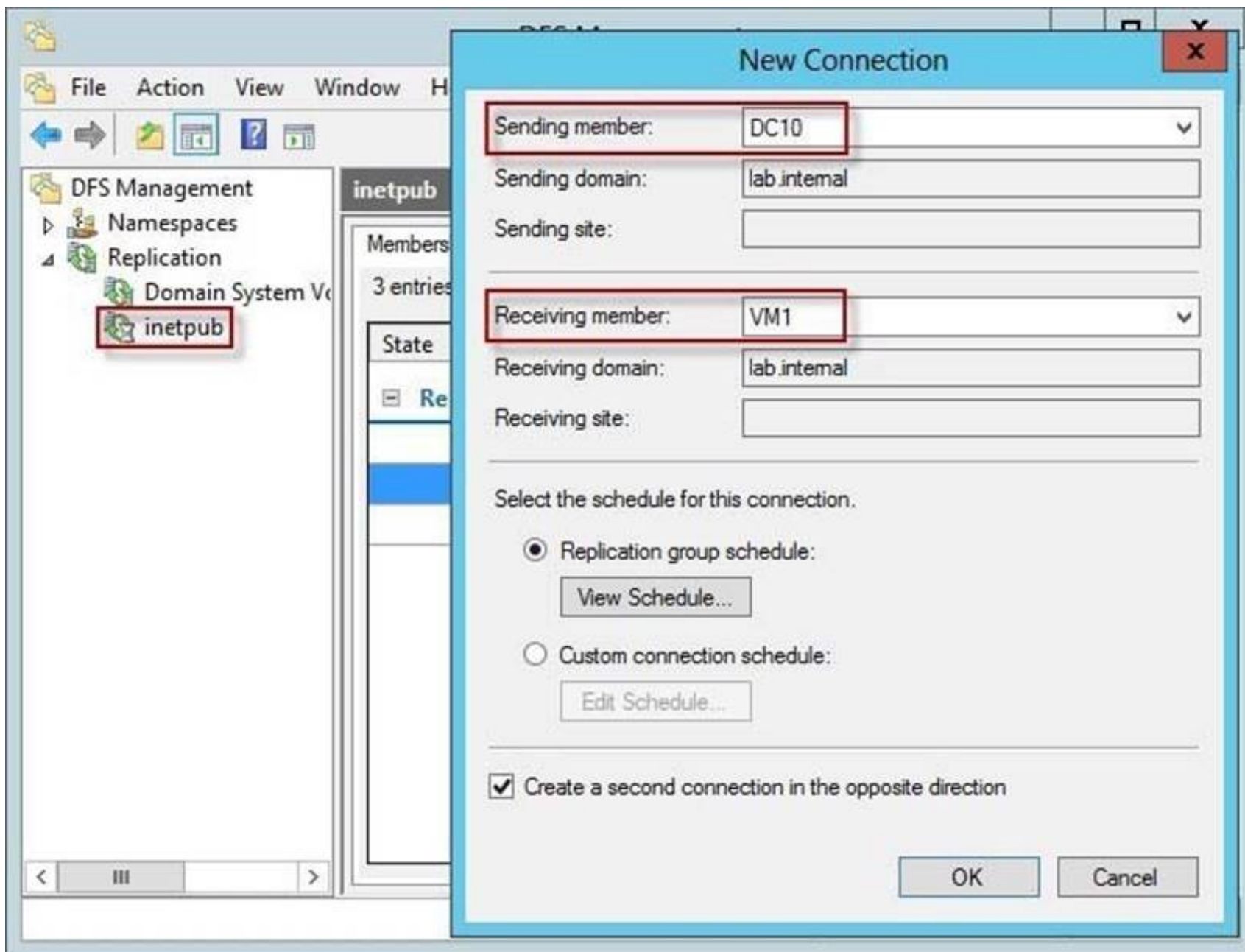
What should you do?

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

Answer: D

Explanation:

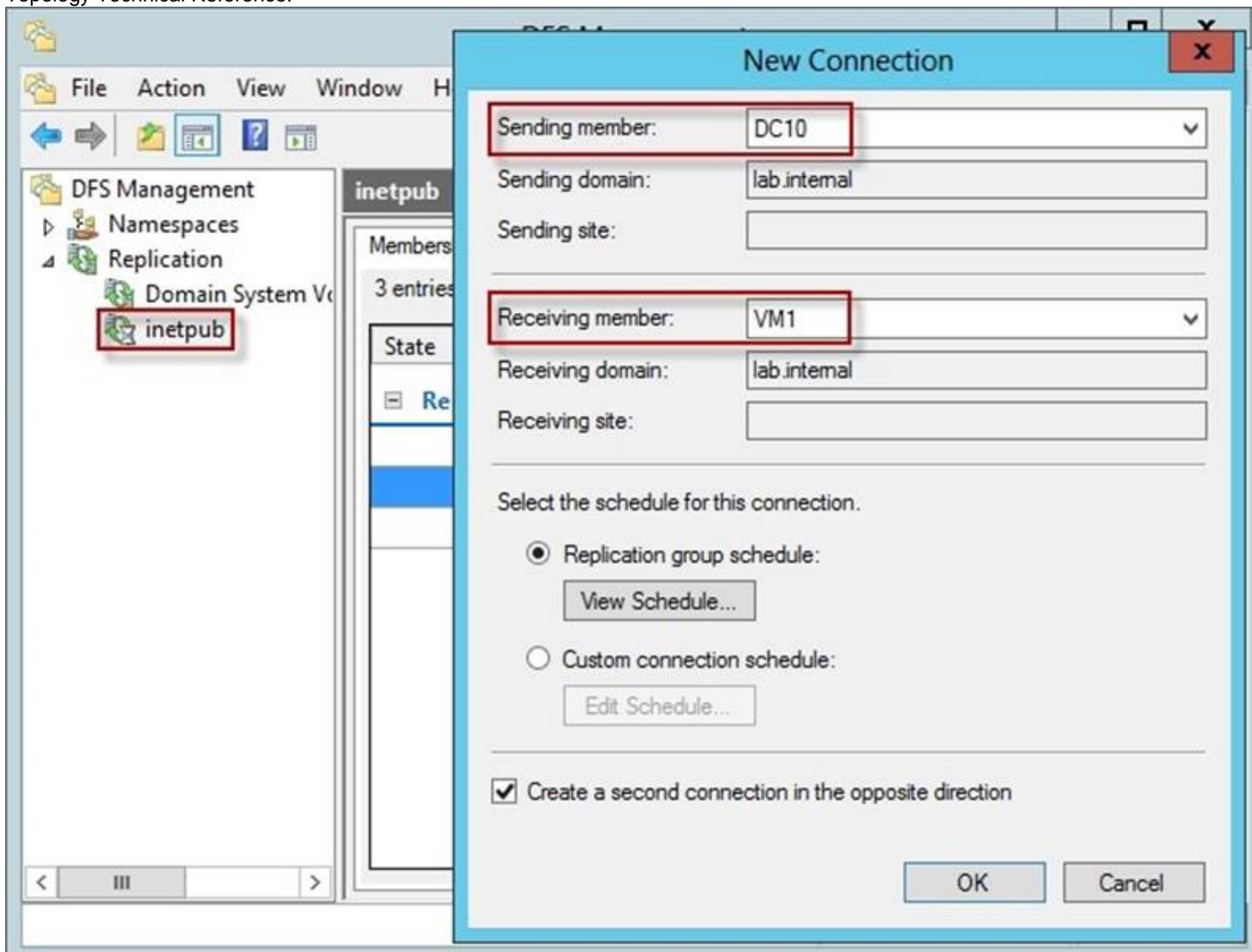
Unsure about this answer. D:



A:

The Bridge all site links option in Active Directory must be enabled. (This option is available in the Active Directory Sites and Services snap-in.) Turning off Bridge all site links can affect the ability of DFS to refer client computers to target computers that have the least expensive connection cost. An Intersite Topology Generator that is running Windows Server 2003 relies on the Bridge all site links option being enabled to generate the intersite cost matrix that DFS requires for its site-costing functionality. If you turn off this option, you must create site links between the Active Directory sites for which you want DFS to calculate accurate site costs.

Any sites that are not connected by site links will have the maximum possible cost. For more information about site link bridging, see "Active Directory Replication Topology Technical Reference."



Reference:

<http://faultbucket.ca/2012/08/fixing-a-dfs-r-connection-problem/>

<http://faultbucket.ca/2012/08/fixing-a-dfs-r-connection-problem/>

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

NEW QUESTION 4

- (Topic 1)

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

The domain is renamed to adatum.com. Group Policies no longer function correctly.

You need to ensure that the existing GPOs are applied to users and computers. You want to achieve this goal by using the minimum amount of administrative effort.

What should you use?

- A. Dcgpofix
- B. Get-GPOReport
- C. Gpfixup
- D. Gpresult
- E. Gpedi
- F. msc
- G. Import-GPO
- H. Restore-GPO
- I. Set-GPInheritance
- J. Set-GPLink
- K. Set-GPPermission
- L. Gpupdate
- M. Add-ADGroupMember

Answer: C

Explanation:

You can use the gpfixup command-line tool to fix the dependencies that Group Policy objects (GPOs) and Group Policy links in Active Directory Domain Services (AD DS) have on Domain Name System (DNS) and NetBIOS names after a domain rename operation.

Reference: [http://technet.microsoft.com/en-us/library/hh852336\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/hh852336(v=ws.10).aspx)

NEW QUESTION 5

- (Topic 1)

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

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

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

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

Which authentication method should you identify?

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

Answer: C

Explanation:

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

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

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

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

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

NEW QUESTION 6

- (Topic 1)

You have a server named WSUS1 that runs Windows Server 2012 R2. WSUS1 has the Windows Server Update Services server role installed and has one volume.

You add a new hard disk to WSUS1 and then create a volume on the hard disk.

You need to ensure that the Windows Server Update Services (WSUS) update files are stored on the new volume.

What should you do?

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

Answer: D

Explanation:

Local Storage Considerations

If you decide to store update files on your server, the recommended minimum disk size is 30 GB. However, depending on the synchronization options you specify, you might need to use a larger disk. For example, when specifying advanced synchronization options, as in the following procedure, if you select options to download multiple languages and/or the option to download express installation files, your server disk can easily reach 30 GB. Therefore if you choose any of

these options, install a larger disk (for example, 100 GB).

If your disk gets full, you can install a new, larger disk and then move the update files to the new location. To do this, after you create the new disk drive, you will need to run the WSUSutil.exetool (with the movecontent command) to move the update files to the new disk. For this procedure, see Managing WSUS from the Command Line.

For example, if D:\WSUS1 is the new path for local WSUS update storage, D:\move.log is the path to the log file, and you wanted to copy the old files to the new location, you would type: wsusutil.exe movecontent D:\WSUS1\ D:\move.log.

Note: If you do not want to use WSUSutil.exe to change the location of local WSUS update storage, you can also use NTFS functionality to add a partition to the current location of local WSUS update storage. For more information about NTFS, go to Help and Support Center in Windows Server 2003.

Syntax

At the command line %drive%\Program Files\Update Services\Tools>, type: wsusutilmovecontentcontentpathlogfile -skipcopy [/?]

The parameters are defined in the following table.

contentpath - the new root for content files. The path must exist. logfile - the path and file name of the log file to create.

-skipcopy - indicates that only the server configuration should be changed, and that the content files should not be copied.

/help or /? - displays command-line help for movecontent command.

References:

<http://blogs.technet.com/b/sus/archive/2008/05/19/wsus-how-to-change-the-location-where-wsus-stores-updates-locally.aspx>

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

<http://technet.microsoft.com/en-us/library/cc708480%28v=ws.10%29.aspx> [http://technet.microsoft.com/en-us/library/cc720466\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc720466(v=ws.10).aspx)

<http://technet.microsoft.com/en-us/library/cc708480%28v=ws.10%29.aspx>

NEW QUESTION 7

- (Topic 1)

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

Server1 has the following role services installed:

? DirectAccess and VPN (RRAS)

? Network Policy Server

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

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

What should you configure on Server1?

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

Answer: A

Explanation:

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

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

NEW QUESTION 8

- (Topic 1)

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

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

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

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

Which role should you identify?

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

Answer: C

Explanation:

Windows Deployment Services (WDS) is a server role that enables you to remotely deploy Windows operating systems. You can use it to set up new computers by using a network- based installation. This means that you do not have to install each operating system directly from a CD, USB drive or DVD. To use Windows Deployment Services, you should have a working knowledge of common desktop deployment technologies and networking components, including Dynamic Host

Configuration Protocol (DHCP), Domain Name System (DNS), and Active Directory Domain Services (AD DS). It is also helpful to understand the Preboot execution Environment (also known as Pre-Execution Environment).

NEW QUESTION 9

HOTSPOT - (Topic 1)

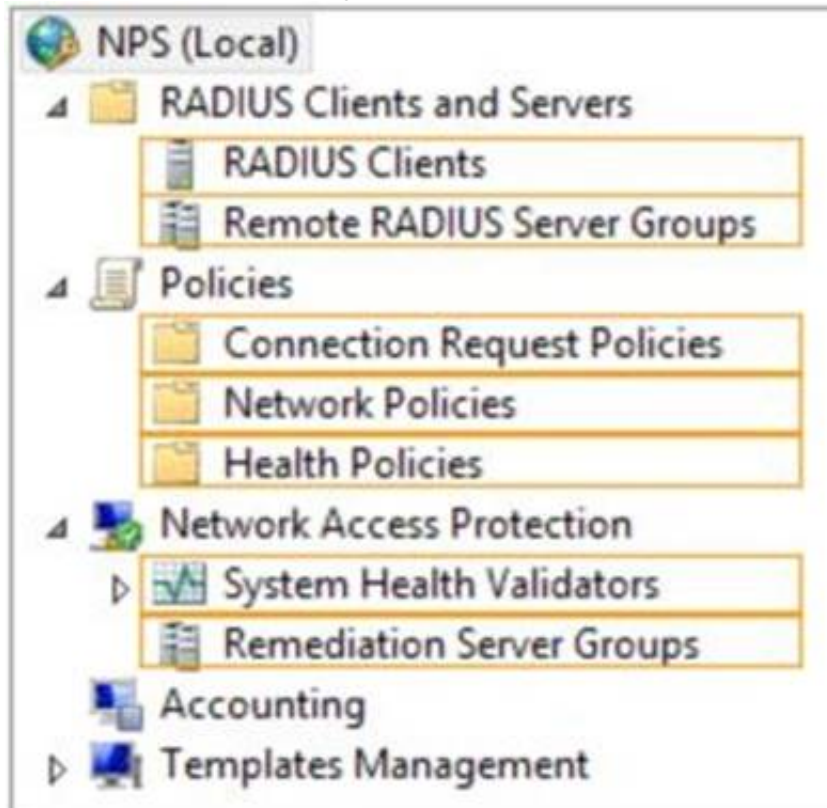
Your network contains a RADIUS server named Server1.

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

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

On Server2, you configure a Connection Request Policy.

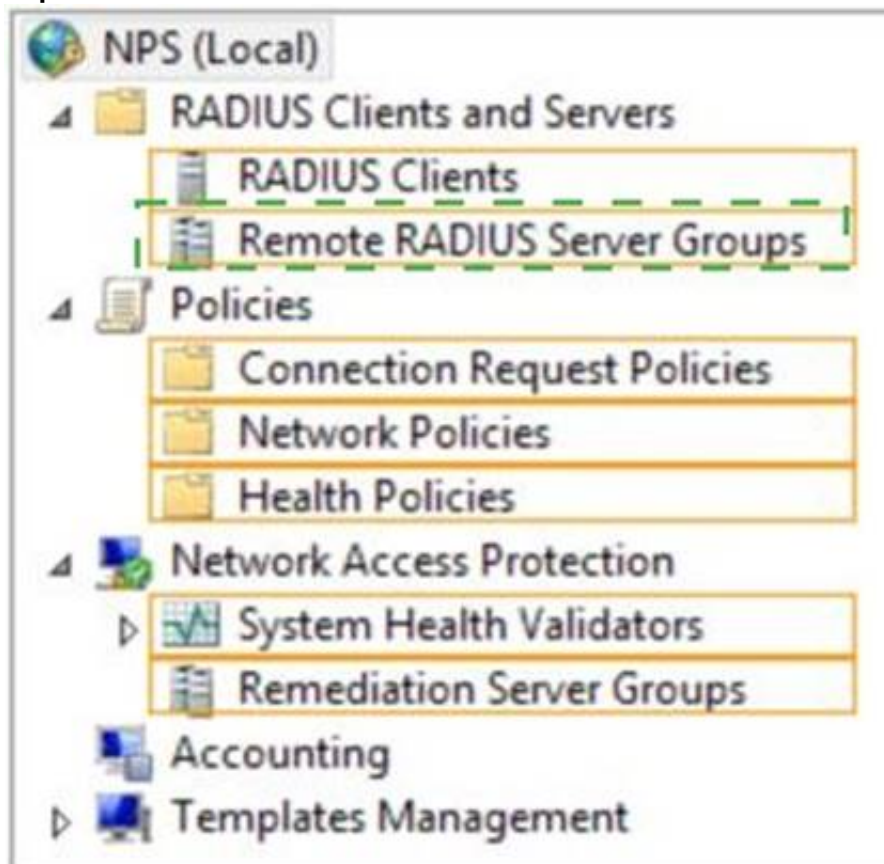
What else should you configure on Server2? To answer, select the appropriate node in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**NEW QUESTION 10**

- (Topic 1)

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

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 10

HOTSPOT - (Topic 1)

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

User name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

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

Answer Area

User1:

User2:

User3:

Answer Area

User1:
Policy1
Policy2
Policy3

User2:
Policy1
Policy2
Policy3

User3:
Policy1
Policy2
Policy3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Policies are processed in this order:

- Policy2 (applies only to members of Group1)
- Policy1 (applies to all users during specified time slot)
- Policy3 (applies only to members of Group2)

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

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

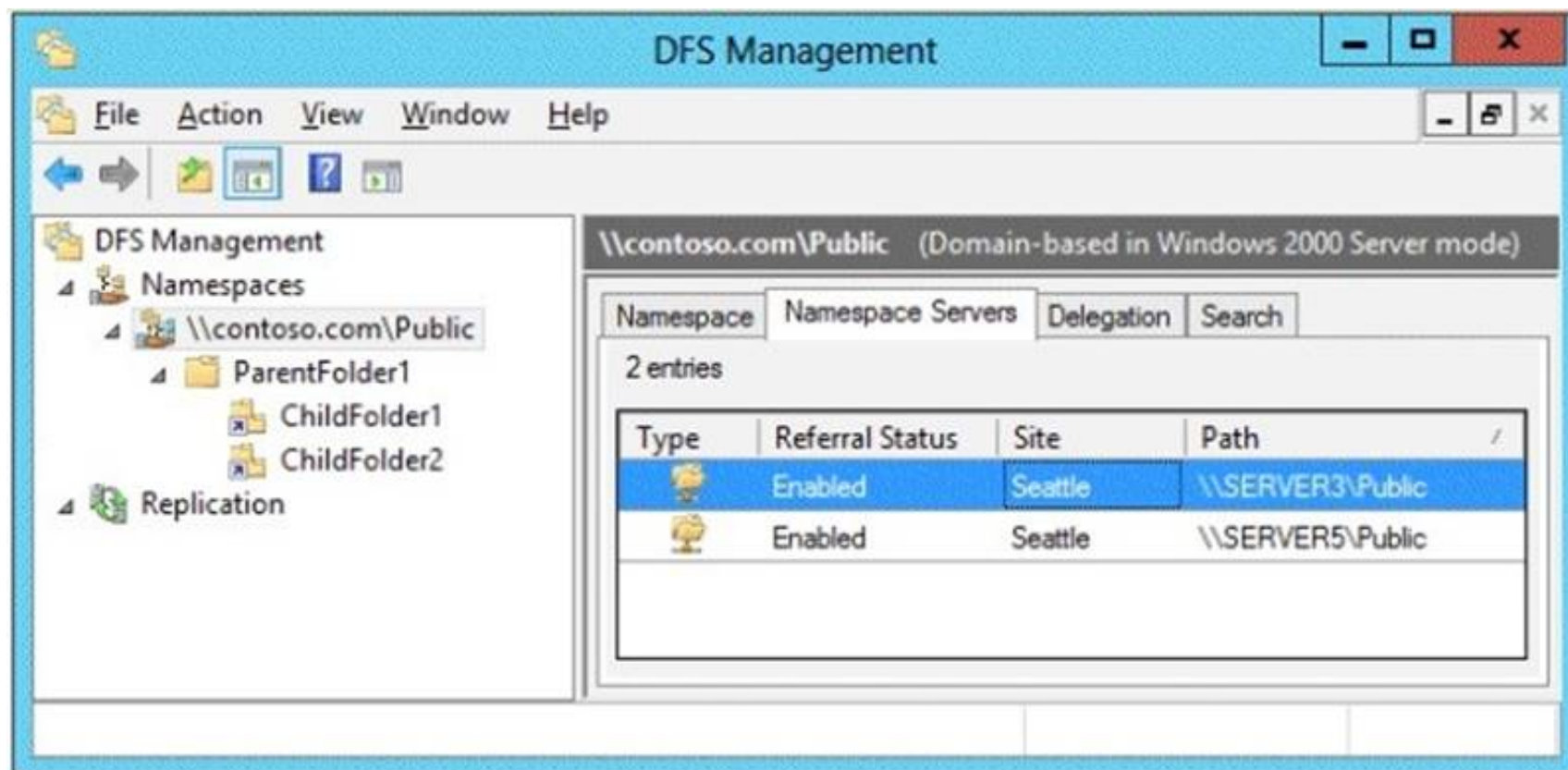
[https://technet.microsoft.com/en-us/library/cc732724\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732724(v=ws.10).aspx)

NEW QUESTION 15

- (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 20

- (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. All client computers run Windows 8 Enterprise.

DC1 contains a Group Policy object (GPO) named GPO1. You need to deploy a VPN connection to all users.

What should you configure from User Configuration in GPO1?

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

Answer: D

Explanation:

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

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

Reference: <http://technet.microsoft.com/en-us/library/cc772449.aspx>

NEW QUESTION 23

- (Topic 1)

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

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

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

What should you configure?

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

Answer: B

Explanation:

To configure data management for a Data Collector Set

1. In Windows Performance Monitor, expand Data Collector Sets and click User Defined.
2. In the console pane, right-click the name of the Data Collector Set that you want to configure and click Data Manager.
3. On the Data Manager tab, you can accept the default values or make changes according to your data retention policy. See the table below for details on each option.
When Minimum free disk or Maximum folders is selected, previous data will be deleted according to the Resource policy you choose (Delete largest or Delete oldest) when the limit is reached. When Apply policy before the data collector set starts is selected, previous data will be deleted according to your selections before the data collector set creates its next log file.
When Maximum root path size is selected, previous data will be deleted according to your selections when the root log folder size limit is reached.
4. Click the Actions tab. You can accept the default values or make changes. See the table below for details on each option.
5. When you have finished making your changes, click OK.

NEW QUESTION 24

- (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 28

- (Topic 1)

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

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

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

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

Answer: BC

Explanation:

To set up a Source-Initiated Subscription with Windows Server 2003/2008 so that events of interest from the Security event log of several domain controllers can be forwarded to an administrative workstation.

* Group Policy

The forwarding computer needs to be configured with the address of the server to which the events are forwarded. This can be done with the following group policy setting:

Computer configuration-Administrative templates-Windows components-Event forwarding- Configure the server address, refresh interval, and issue certificate authority of a target subscription manager.

* Edit the GPO and browse to Computer Configuration | Policies | Administrative Templates

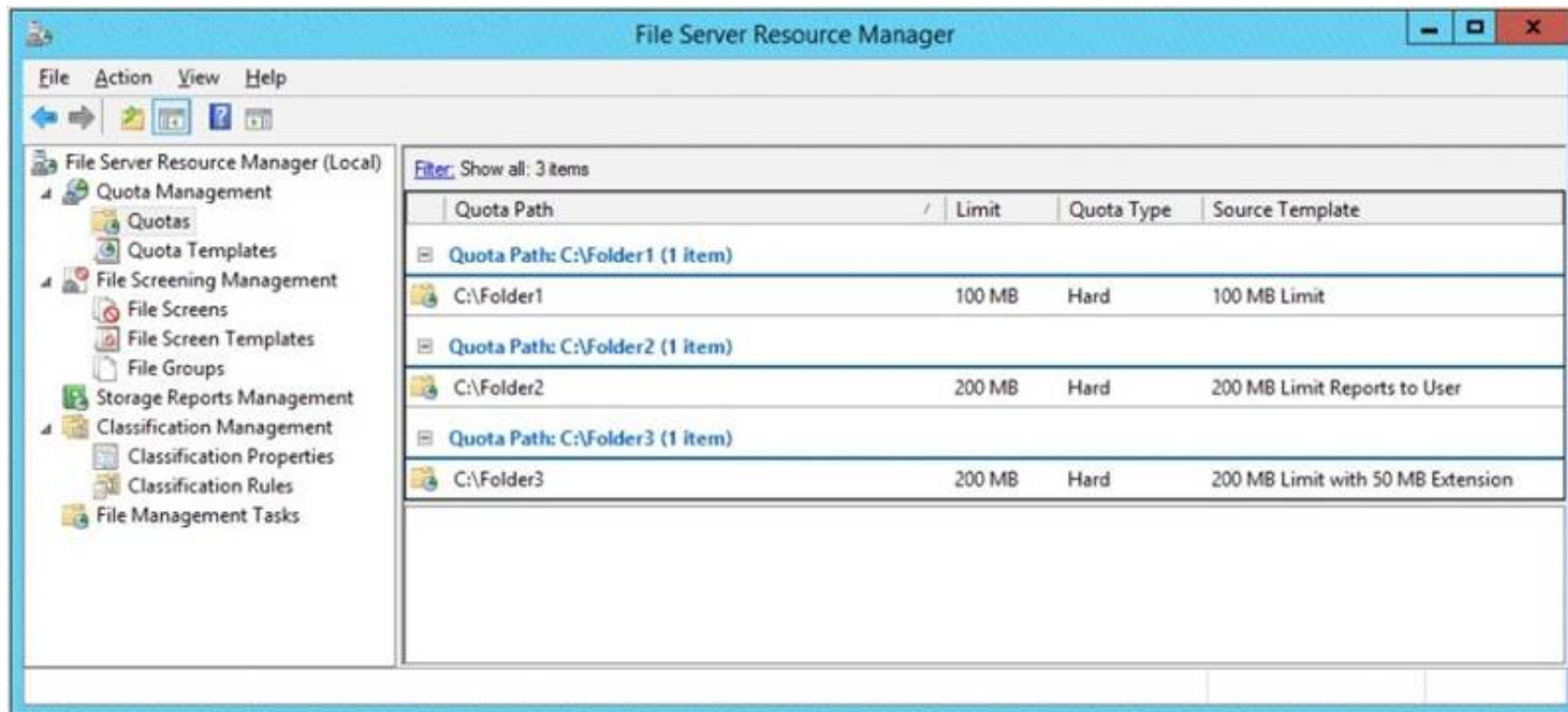
| Windows Components | Event Forwarding - Configure the server address, refresh interval, and issuer certificate authority of a target Subscription Manager.

NEW QUESTION 32

- (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.)



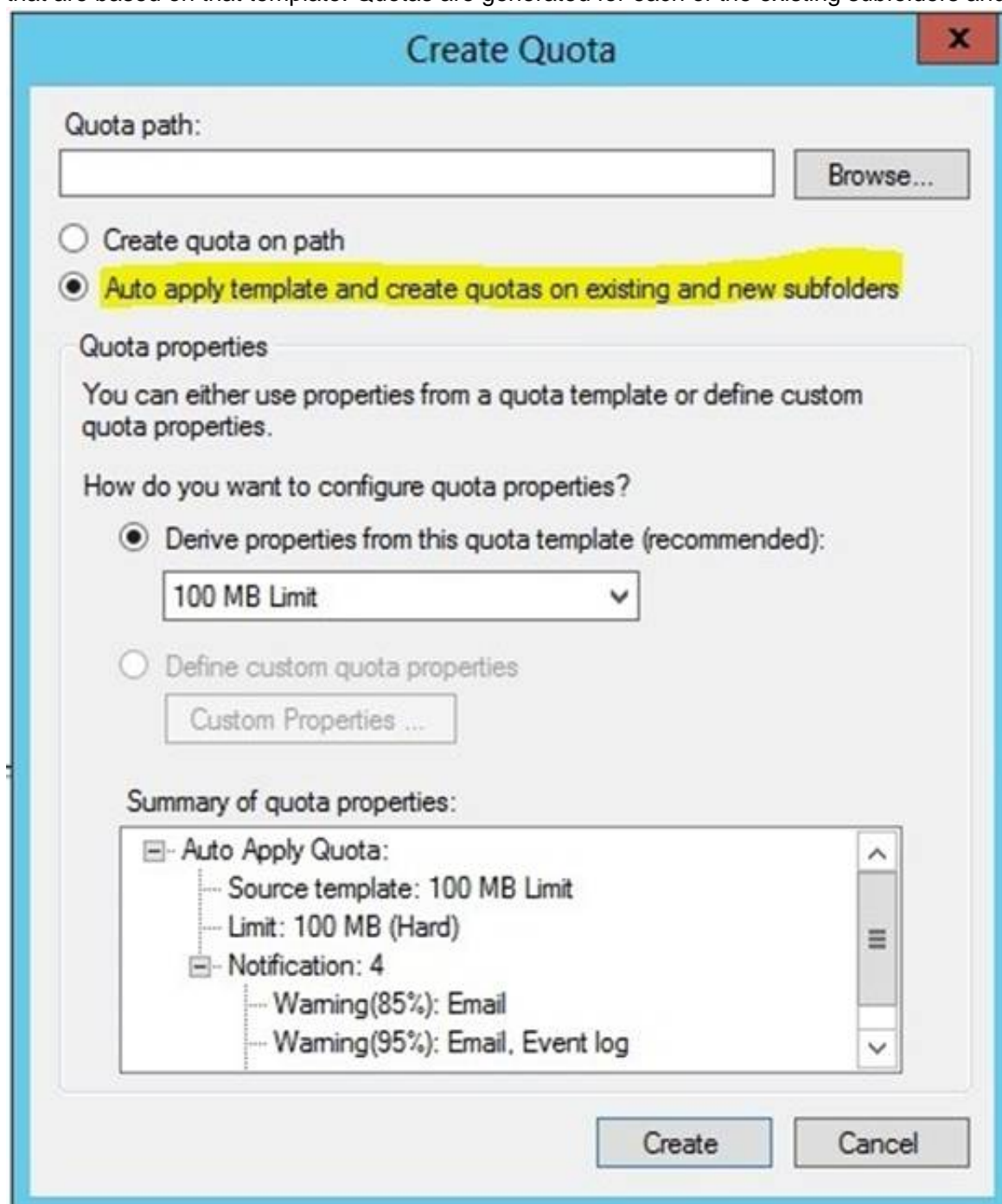
You need to ensure that all of the folders in Folder1 have a 100-MB quota limit. What should you do?

- 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 37

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 38

HOTSPOT - (Topic 1)

Your company has two offices. The offices are located in Montreal and Seattle.

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

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

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

Answer Area
<div> <input type="text"/> <input type="text"/> <input type="text"/> </div>

Answer Area

<input type="text"/> Add-WsusComputer Approve-WsusUpdate Set-WsusClassification Set-WsusProduct Set-WsusServerSynchronizatio	<input type="text"/> -ServerName Server1 -UpdateServer Server1 -UssServerName Server1	<input type="text"/> -Replica -SyncFromMu -UseSsl
---	--	--

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

<input type="text"/> Add-WsusComputer Approve-WsusUpdate Set-WsusClassification Set-WsusProduct Set-WsusServerSynchronizatio	<input type="text"/> -ServerName Server1 -UpdateServer Server1 -UssServerName Server1	<input type="text"/> -Replica -SyncFromMu -UseSsl
---	--	--

NEW QUESTION 40

HOTSPOT - (Topic 1)

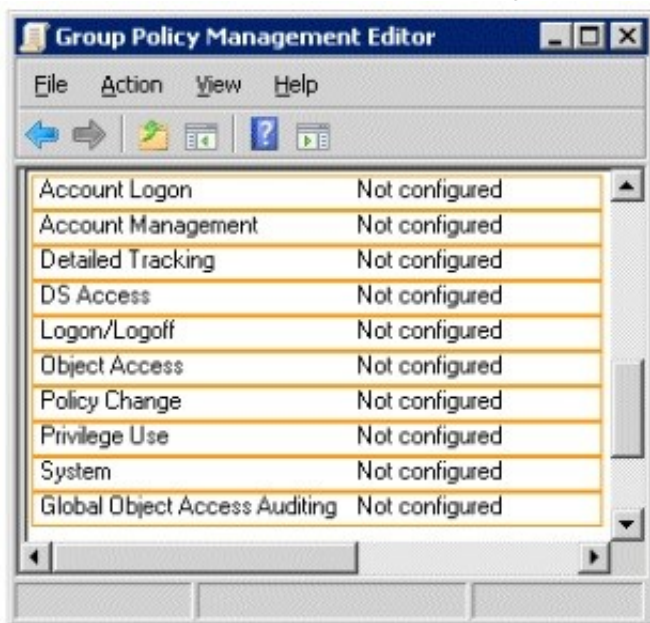
Your network contains an Active Directory domain named contoso.com.

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.

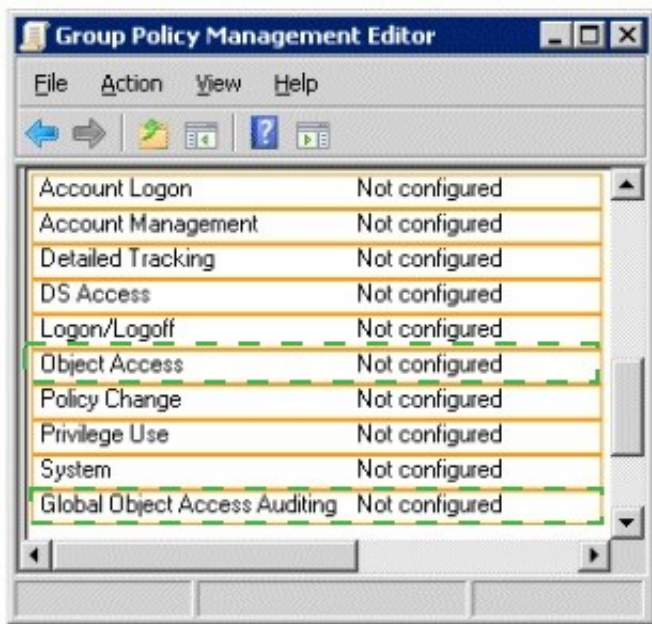
Which two audit policies should you configure in GPO1? To answer, select the appropriate two objects in the answer area.



- A. Mastered
B. Not Mastered

Answer: A

Explanation:

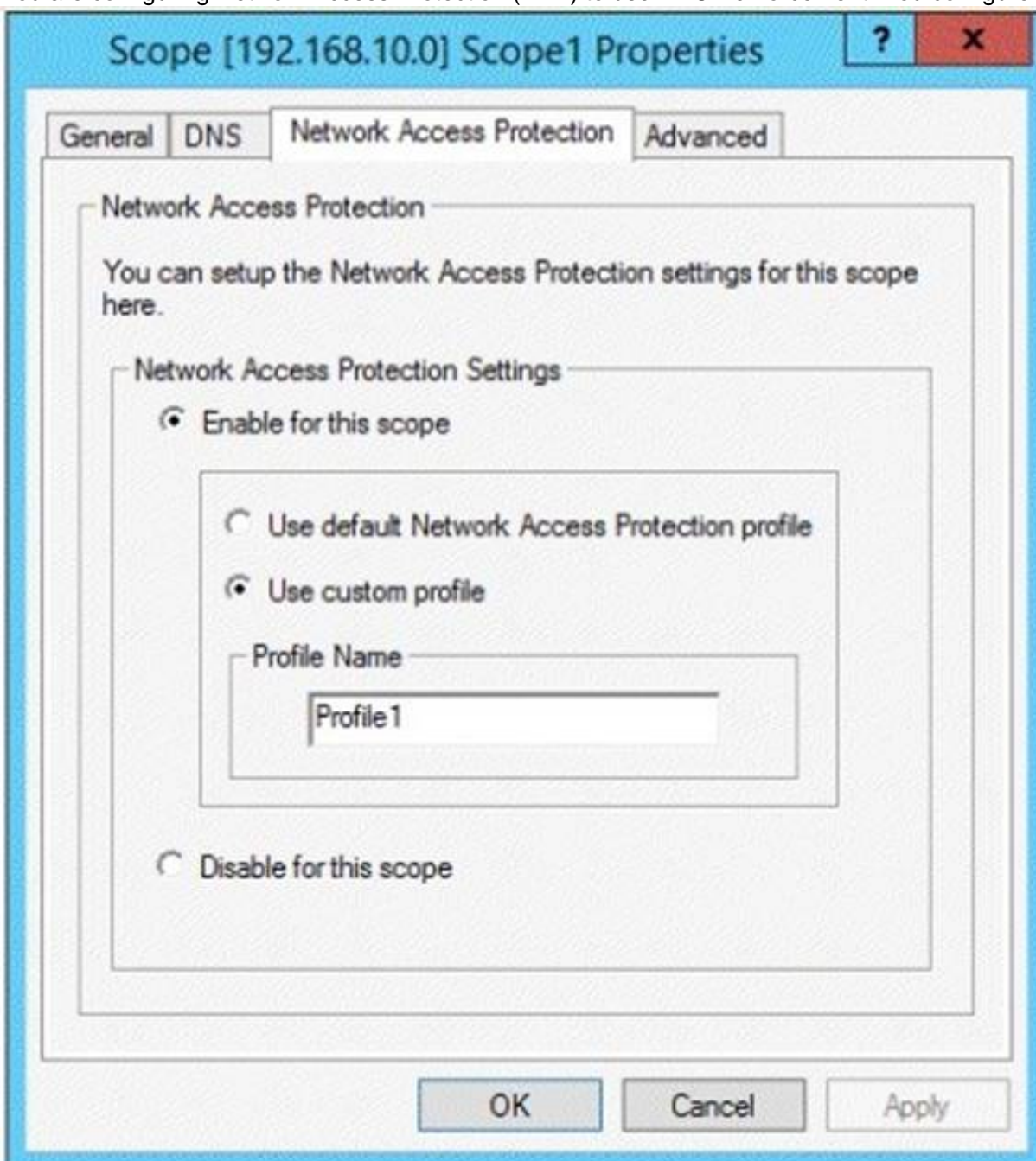


NEW QUESTION 43

HOTSPOT - (Topic 1)

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Server1 has the Network Policy Server server role installed. Server2 has the DHCP Server server role installed. Both servers run Windows Server 2012 R2.

You are configuring Network Access Protection (NAP) to use DHCP enforcement. You configure a DHCP scope as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that non-compliant NAP clients receive different DHCP options than compliant NAP clients.

What should you configure on each server? To answer, select the appropriate options for each server in the answer area.

Answer Area

Server1:

Server2:

Answer Area

Server1:

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

Server2:

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Health Policies Server Options

- * Health policy on the NAP server.
- * The DHCP server must be NAP enabled.

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

NEW QUESTION 44

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. You enable and configure Routing and Remote Access (RRAS) on Server1. You create a user account named User1. You need to ensure that User1 can establish VPN connections to Server1. What should you do?

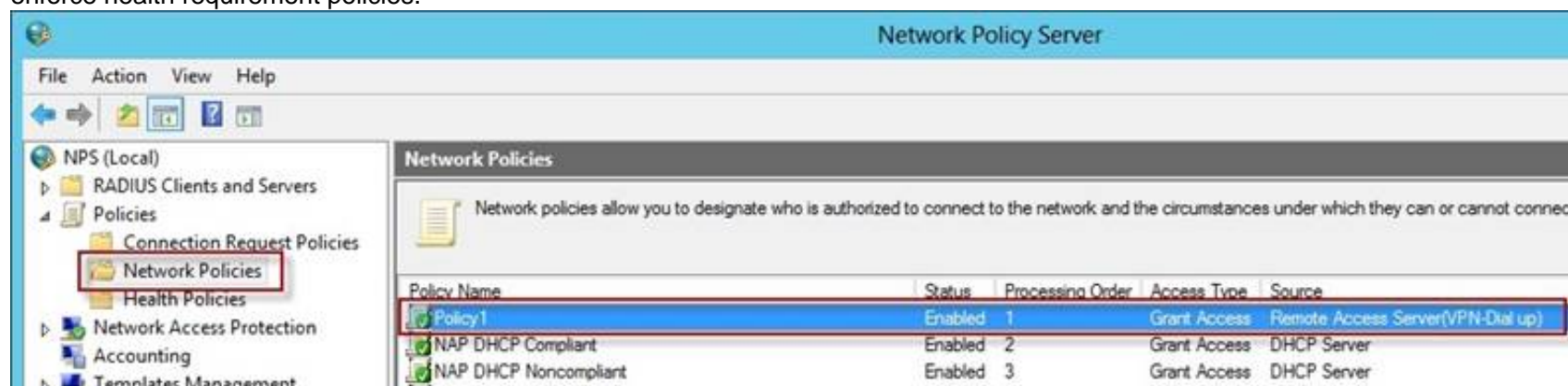
- A. Create a network policy.
B. Create a connection request policy.
C. Add a RADIUS client.
D. Modify the members of the Remote Management Users group.

Answer: A

Explanation:

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

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



References:

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

NEW QUESTION 49

- (Topic 2)

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

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

User1 Properties

Member Of: Remote control, Dial-in, Environment, Sessions, Remote Desktop Services Profile, COM+

General | Address | Account | Profile | Telephones | Organization

User1

First name: [] Initials: []

Last name: []

Display name: []

Description: []

Office: []

Telephone number: [] Other...

E-mail: []

Web page: [] Other...

OK Cancel Apply Help

You plan to use the User1 account as a service account. The service will forward authentication requests to other servers. You need to ensure that you can view the Delegation tab from the properties of the User1 account. What should you do first?

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

Answer: C

Explanation:

If you cannot see the Delegation tab, do one or both of the following:

Register a Service Principal Name (SPN) for the user account with the Setspn utility in the support tools on your CD. Delegation is only intended to be used by service accounts, which should have registered SPNs, as opposed to a regular user account which typically does not have SPNs.

Raise the functional level of your domain to Windows Server 2003. For more information, see Related Topics.

User1 Properties

Organization | Member Of | Dial-in | Environment | Sessions, Remote control, Remote Desktop Services Profile, COM+

General | Address | Account | Profile | Telephones | **Delegation**

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

☒ Do not trust this user for delegation

☐ Trust this user for delegation to any service (Kerberos only)

☐ Trust this user for delegation to specified services only

☒ Use Kerberos only

☐ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name

☐ Expanded Add... Remove

OK Cancel Apply Help

References:

<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>
<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>
[http://technet.microsoft.com/en-us/library/cc739474\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc739474(v=ws.10).aspx)
<http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx>

NEW QUESTION 51

- (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 54

- (Topic 2)

You have a DNS server named Server1.

Server1 has a primary zone named contoso.com.

Zone Aging/Scavenging is configured for the contoso.com zone.

One month ago, an administrator removed a server named Server2 from the network.

You discover that a static resource record for Server2 is present in contoso.com. Resource records for decommissioned client computers are removed automatically from contoso.com.

You need to ensure that the static resource records for all of the servers are removed automatically from contoso.com.

What should you modify?

- A. The Expires after value of contoso.com
- B. The Record time stamp value of the static resource records
- C. The time-to-live (TTL) value of the static resource records
- D. The Security settings of the static resource records

Answer: B

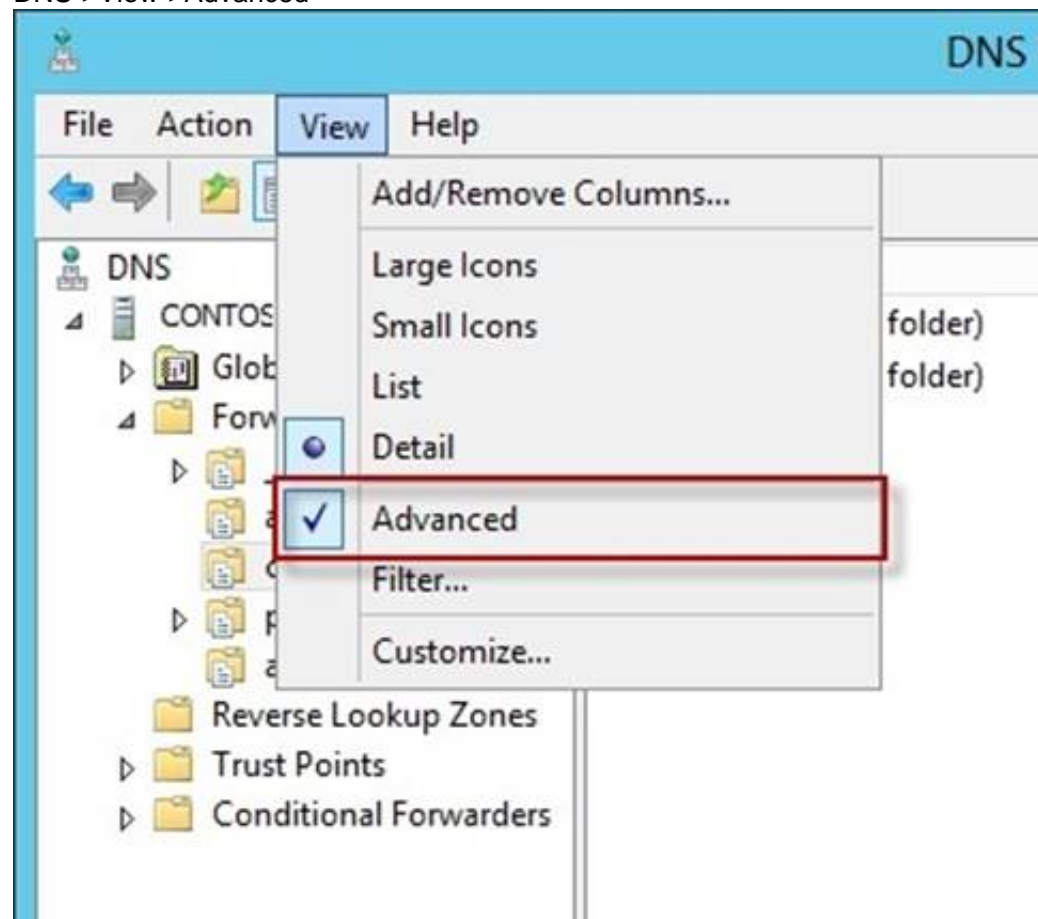
Explanation:

Reset and permit them to use a current (non-zero) time stamp value. This enables these records to become aged and scavenged.

You can use this procedure to change how a specific resource record is scavenged.

A stale record is a record where both the No-Refresh Interval and Refresh Interval have passed without the time stamp updating.

DNS->View->Advanced



Depending on the how the resource record was originally added to the zone, do one of the following:

If the record was added dynamically using dynamic update, clear the Delete this record when it becomes stale check box to prevent its aging or potential removal

during the scavenging process. If dynamic updates to this record continue to occur, the Domain Name System (DNS) server will always reset this check box so that the dynamically updated record can be deleted.

If you added the record statically, select the Delete this record when it becomes stale check box to permit its aging or potential removal during the scavenging process.

Server2 Properties

Host (A)

Host (uses parent domain if left blank):
Server2

Fully qualified domain name (FQDN):
server2.contoso.com

IP address:
10.56.12.10

☒ Update associated pointer (PTR) record

☒ Delete this record when it becomes stale

Record time stamp: 01.04.2013 02:00

Time to live (TTL): 0 :1 :0 (DDDDD:HH.MM.SS)

OK Cancel Apply

References:

<http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx>

Typically, stale DNS records occur when a computer is permanently removed from the network. Mobile users who abnormally disconnect from the network can also cause stale DNS records. To help manage stale records, Windows adds a time stamp to dynamically added resource records in primary zones where aging and scavenging are enabled. Manually added records are time stamped with a value of 0, and they are automatically excluded from the aging and scavenging process.

To enable aging and scavenging, you must do the following:

Resource records must be either dynamically added to zones or manually modified to be used in aging and scavenging operations.

Scavenging and aging must be enabled both at the DNS server and on the zone. Scavenging is disabled by default.

Zone Aging/Scavenging Properties

☐ Scavenge stale resource records

No-refresh interval

The time between the most recent refresh of a record timestamp and the moment when the timestamp may be refreshed again.

No-refresh interval: 7 days

Refresh interval

The time between the earliest moment when a record timestamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period.

Refresh interval: 7 days

The zone can be scavenged after:

Date and time: 01.01.1601 01:00:00

OK Cancel

DNS scavenging depends on the following two settings:

No-refresh interval: The time between the most recent refresh of a record time stamp and the moment when the time stamp can be refreshed again. When scavenging is enabled, this is set to 7 days by default.

Refresh interval: The time between the earliest moment when a record time stamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period. When scavenging is enabled, this is set to 7 days by default.

A DNS record becomes eligible for scavenging after both the no-refresh and refresh intervals have elapsed. If the default values are used, this is a total of 14 days.

References:

<http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx>

<http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx>

<http://technet.microsoft.com/en-us/library/cc771570.aspx>

<http://technet.microsoft.com/en-us/library/cc771677.aspx>

[http://technet.microsoft.com/en-us/library/cc758321\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc758321(v=ws.10).aspx)

NEW QUESTION 55

- (Topic 2)

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

Server1 stores update files locally in C:\Updates.

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 60

- (Topic 2)

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

You need to configure Server1 to create an entry in an event log when the processor usage exceeds 60 percent.

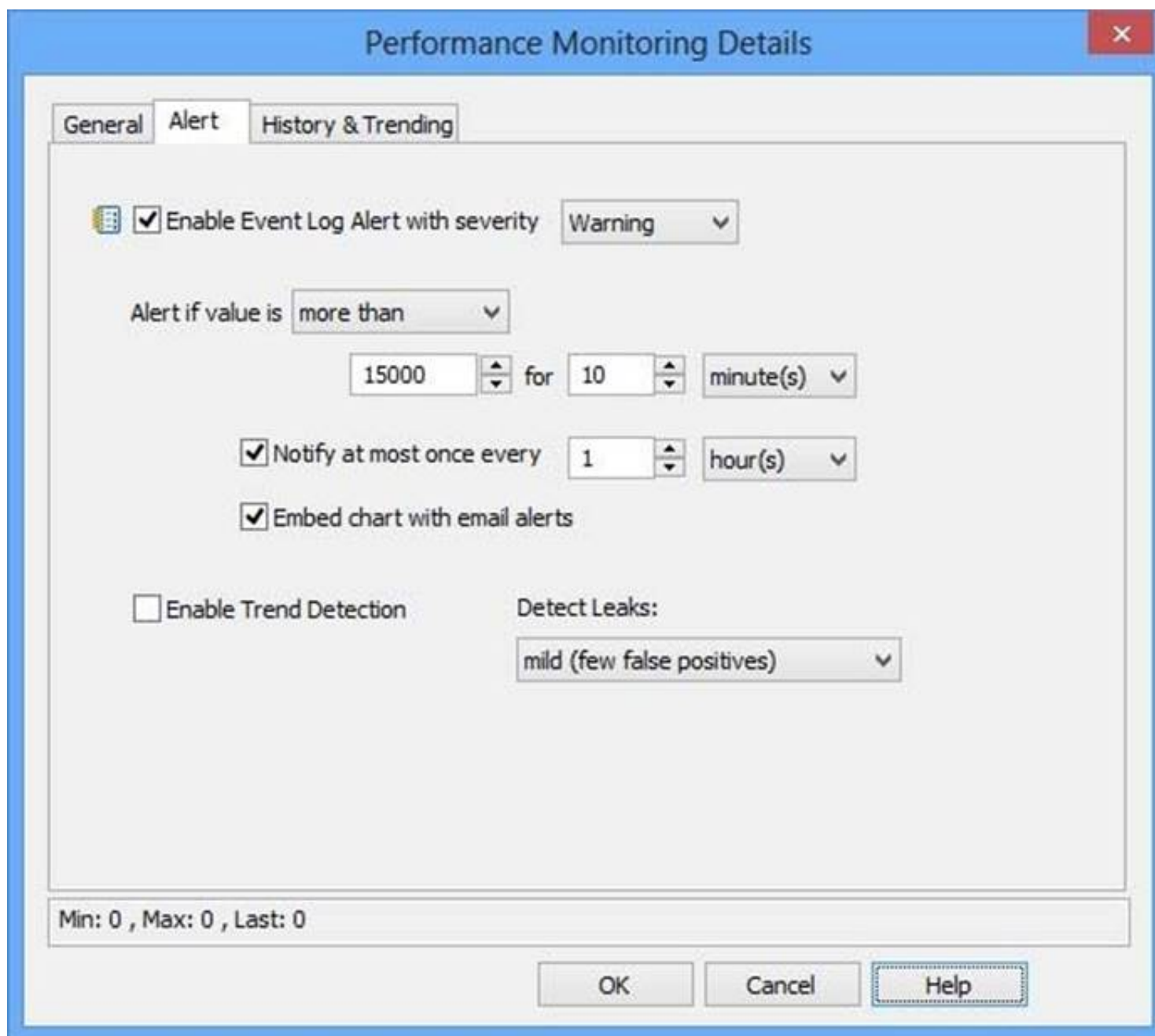
Which type of data collector should you create?

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

Answer: B

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" with a close button (X) in the top right corner. 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 64

- (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:

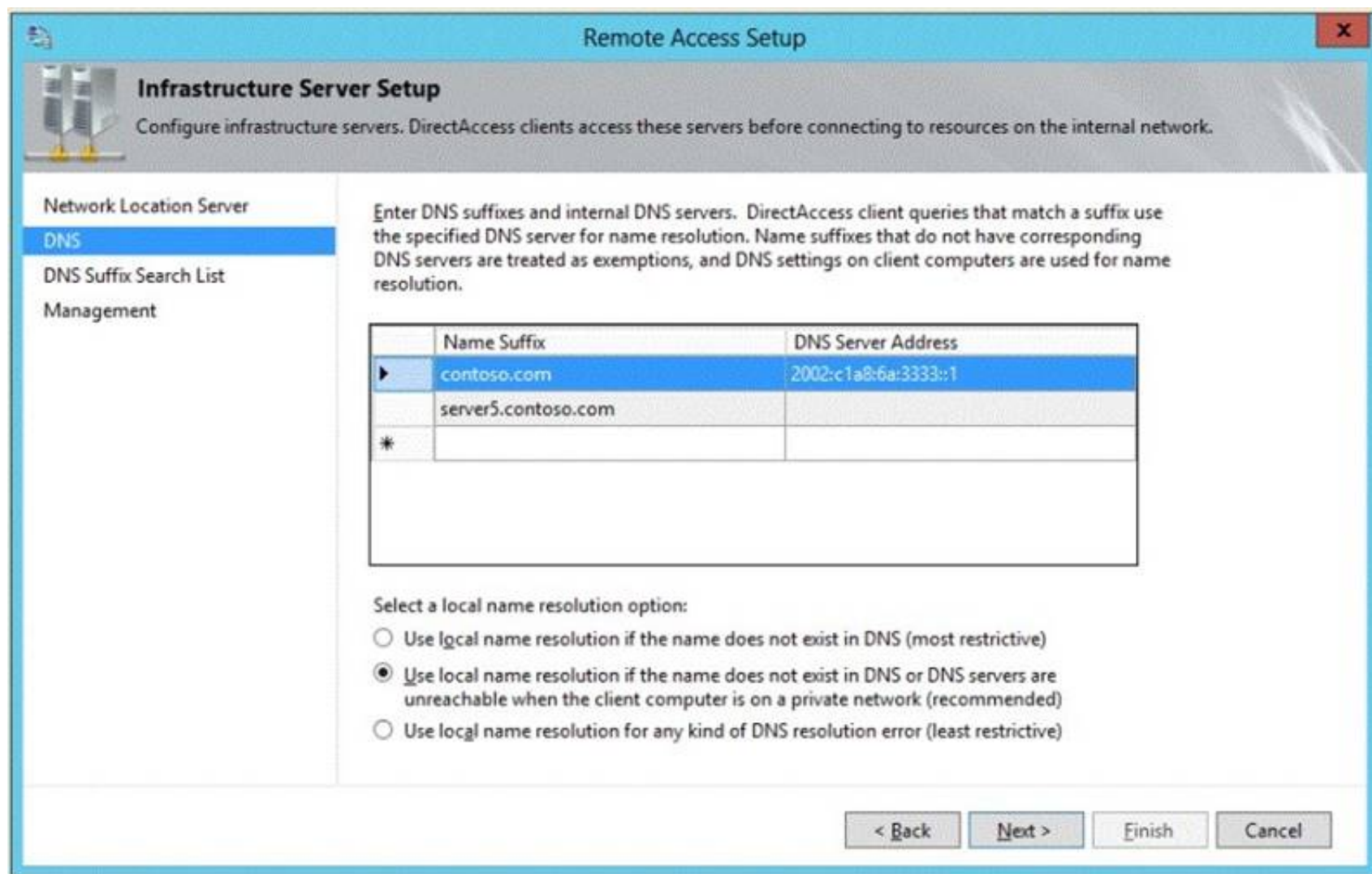
Internal DNS name: server1.contoso.com

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.)



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 66

- (Topic 2)

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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 68

DRAG DROP - (Topic 2)

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: ntdsutil

Box 2: snapshot

Box 3: activate instance ntds Box 4: create

Note:

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

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

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

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

NEW QUESTION 69

- (Topic 2)

Your network contains a single Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that hosts the primary DNS zone for contoso.com.

All servers dynamically register their host names.

You install three new Web servers that host identical copies of your company's intranet website. The servers are configured as shown in the following table.

Server name	IP address
WEB1.contoso.com	10.0.0.20
WEB2.contoso.com	10.0.0.21
WEB3.contoso.com	10.0.0.22

You need to use DNS records to load balance name resolution queries for intranet.contoso.com between the three Web servers.

What is the minimum number of DNS records that you should create manually?

- A. 1
- B. 3
- C. 4
- D. 6

Answer: B

Explanation:

To create DNS Host (A) Records for all internal pool servers

1. Click Start, click All Programs, click Administrative Tools, and then click DNS.

2. In DNS Manager, click the DNS Server that manages your records to expand it.

3. Click Forward Lookup Zones to expand it.

4. Right-click the DNS domain that you need to add records to, and then click New Host (A or AAAA).

5. In the Name box, type the name of the host record (the domain name will be automatically appended).

6. In the IP Address box, type the IP address of the individual Front End Server and then select Create associated pointer (PTR) record or Allow any authenticated user to update DNS records with the same owner name, if applicable.

7. Continue creating records for all member Front End Servers that will participate in DNS Load Balancing.

For example, if you had a pool named pool1.contoso.com and three Front End Servers, you would create the following DNS entries:

FQDN	Type	Data
Pool1.contoso.com	Host (A)	192.168.1.1
Pool1.contoso.com	Host (A)	192.168.1.2
Pool1.contoso.com	Host (A)	192.168.1.3

erence:

<http://technet.microsoft.com/en-us/library/cc772506.aspx>

<http://technet.microsoft.com/en-us/library/gg398251.aspx>

NEW QUESTION 74

HOTSPOT - (Topic 2)

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

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

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

Which two settings should you configure in GPO1?

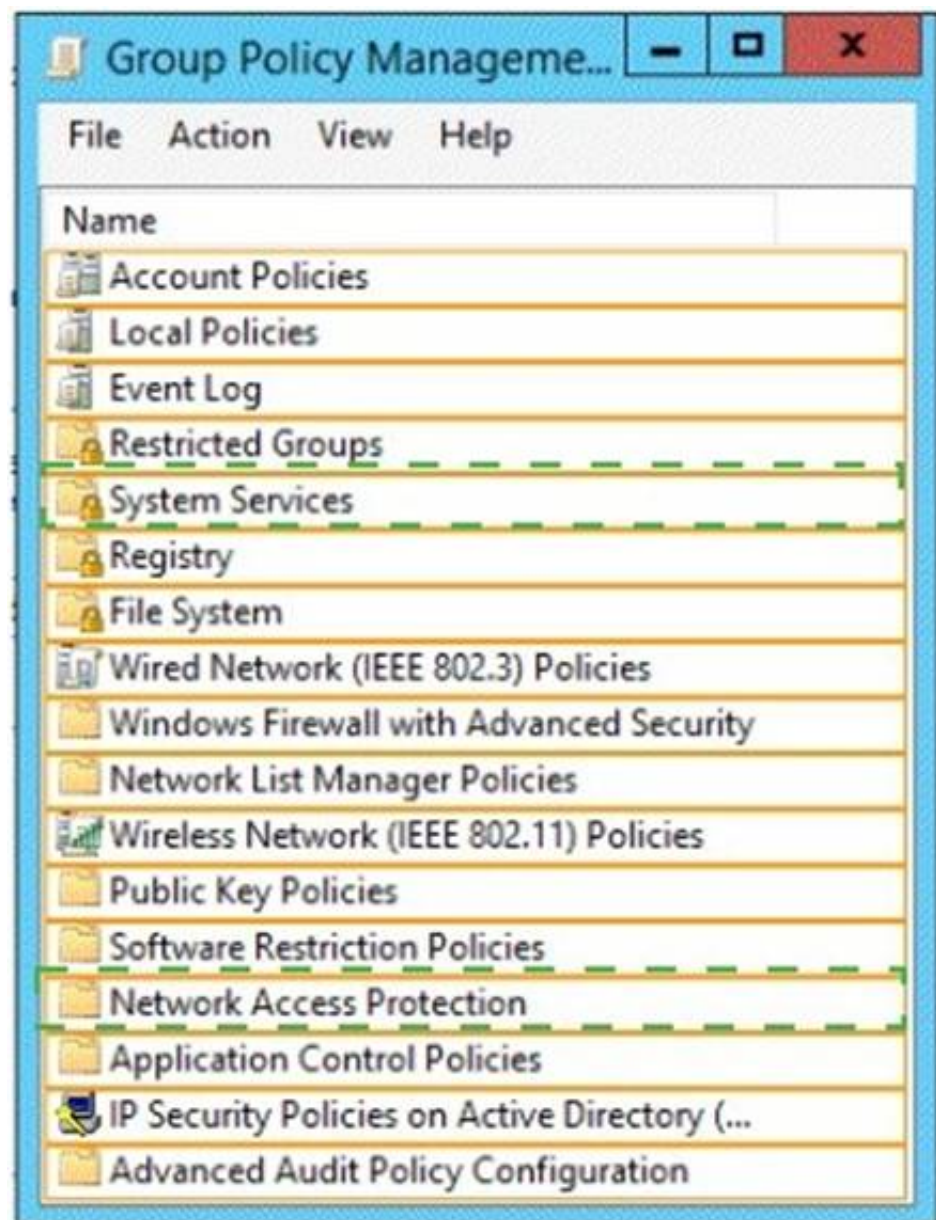
To answer, select the appropriate two settings in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**NEW QUESTION 75**

- (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 78

HOTSPOT - (Topic 2)

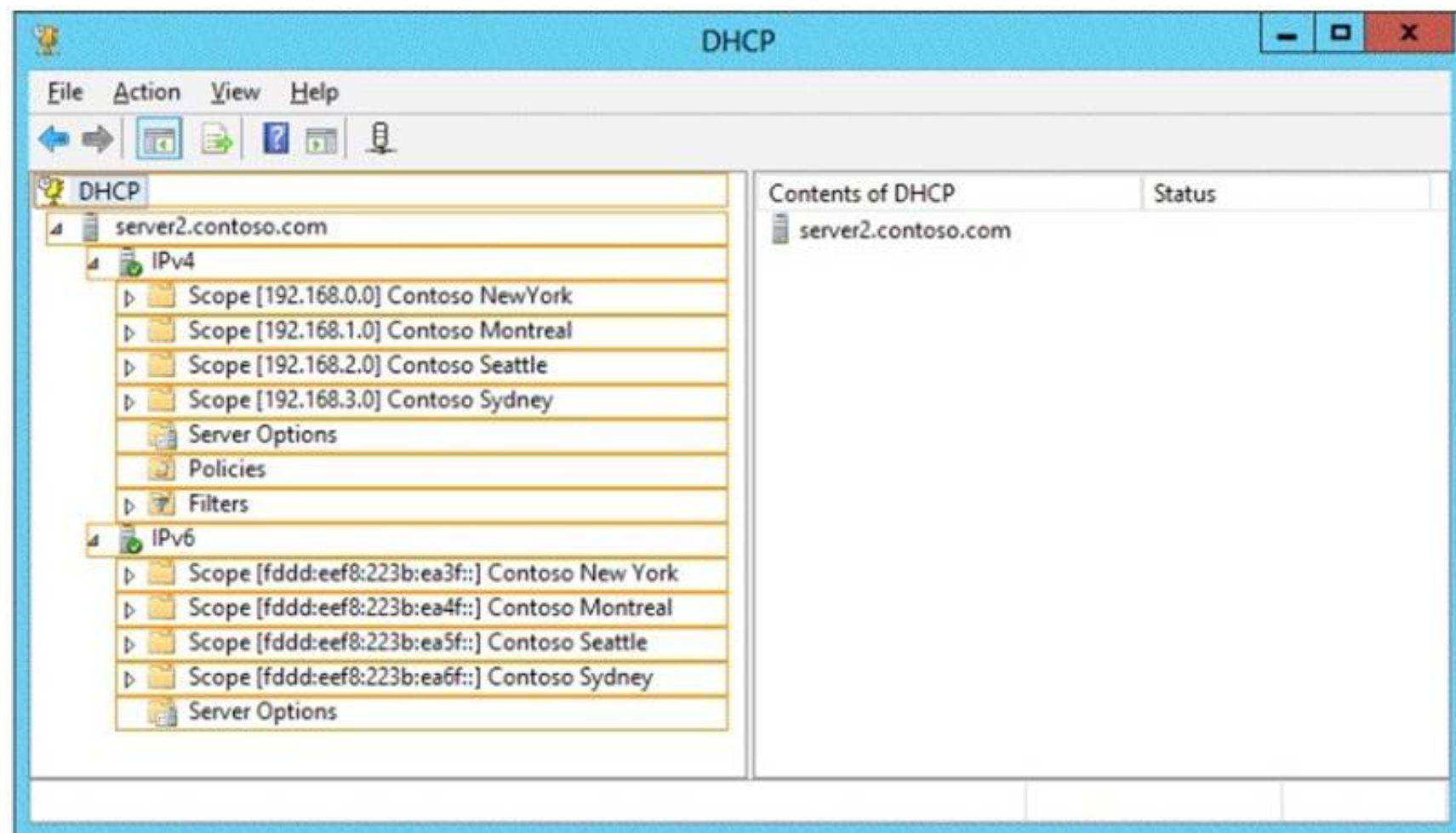
Your company has four offices. The offices are located in Montreal, Seattle, Sydney, and New York.

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

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

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

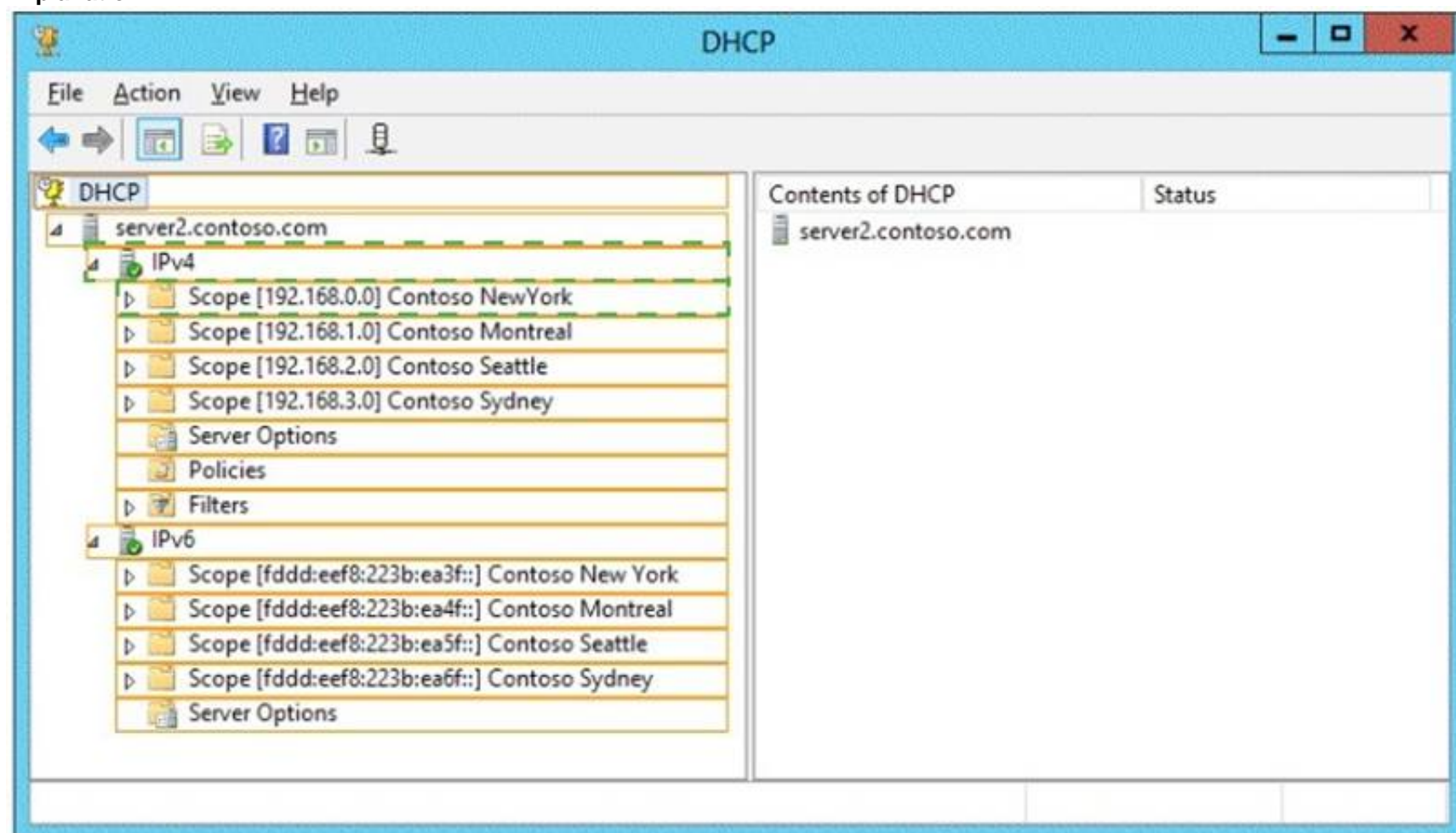
Which two nodes should you configure? To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 83

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 has the 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 84

DRAG DROP - (Topic 2)

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

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

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

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

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 87

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. You plan to use fine-grained password policies to customize the password policy settings of contoso.com.

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

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

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

Answer: AB

Explanation:

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

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

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

<http://technet.microsoft.com/en-us/library/cc731589%28v=ws.10%29.aspx>

<http://technet.microsoft.com/en-us/library/cc731589%28v=ws.10%29.aspx> <http://technet.microsoft.com/en-us/library/cc770848%28v=ws.10%29.aspx>

<http://www.brandonlawson.com/active-directory/creating-fine-grained-password-policies/>

NEW QUESTION 89

HOTSPOT - (Topic 2)

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

You change the IP address of Server2.

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

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

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

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

The screenshot shows the 'contoso.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The fields are as follows:

- Serial number:** 234 (with an 'Increment' button)
- Primary server:** server1.contoso.com. (with a 'Browse...' button)
- Responsible person:** hostmaster.contoso.com. (with a 'Browse...' button)
- Refresh interval:** 1 days (dropdown menu)
- Retry interval:** 1 days (dropdown menu)
- Expires after:** 1 days (dropdown menu)
- Minimum (default) TTL:** 1 days (dropdown menu)
- TTL for this record:** 1 :0 :0 :0 (format: DDDDD:HH.MM.SS)

At the bottom are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

Despite being the original defined meaning, the first of these, the minimum TTL value of all RRs in a zone, has never in practice been used and is hereby deprecated. The second, the default TTL of RRs which contain no explicit TTL in the master zone file, is relevant only at

the primary server. After a zone transfer all RRs have explicit TTLs and it is impossible to determine whether the TTL for a record was explicitly set or derived from the default after a zone transfer. Where a server does not require RRs to include the TTL value explicitly, it should provide a mechanism, not being the value of the

MINIMUM field of the SOA record, from which the missing TTL values are obtained. How this is done is implementation dependent.

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

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

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

Windows IP Configuration

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

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

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

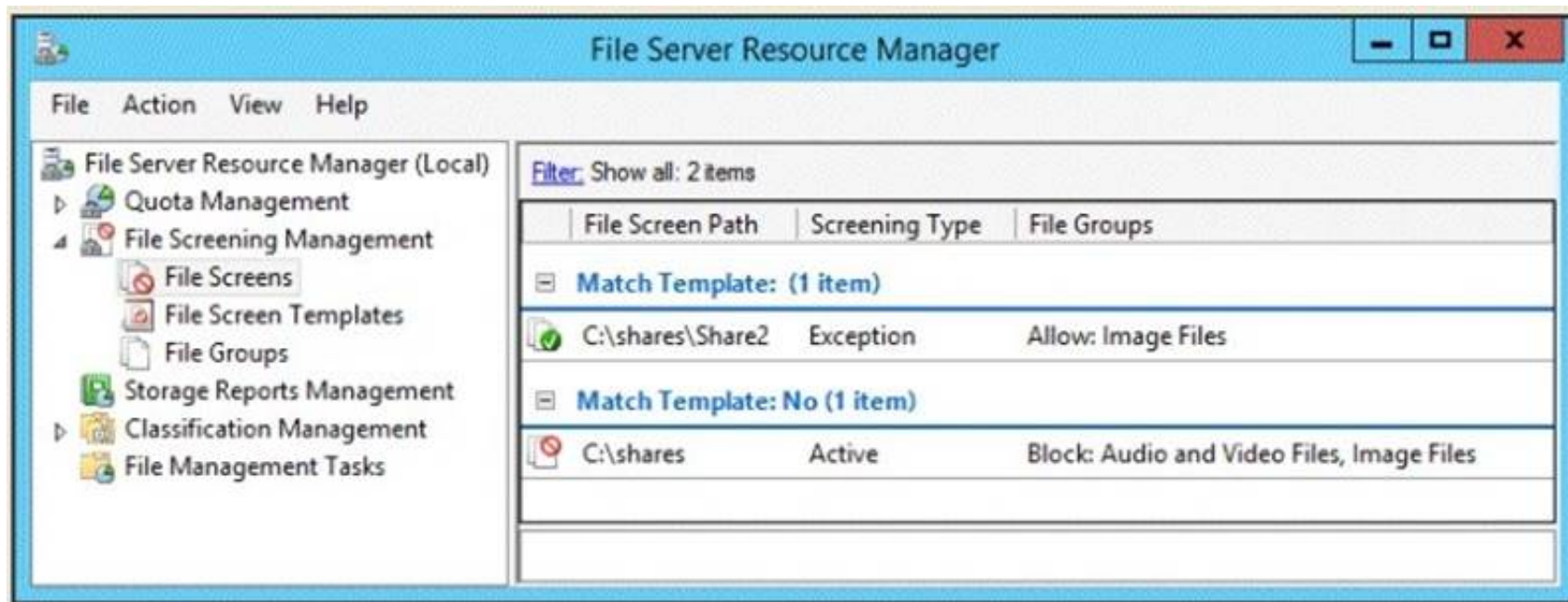
NEW QUESTION 90

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.

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

NEW QUESTION 95

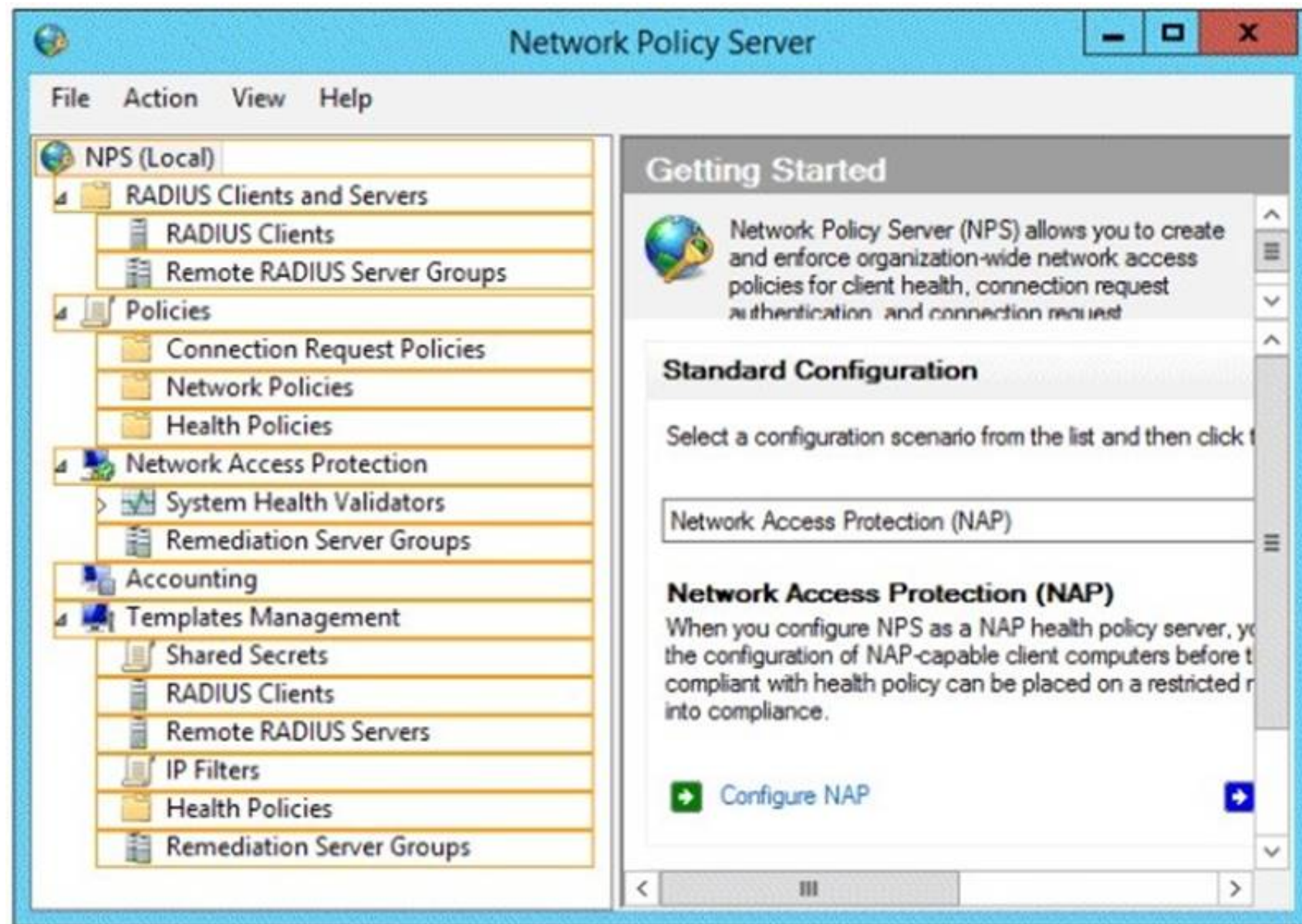
HOTSPOT - (Topic 2)

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

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

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

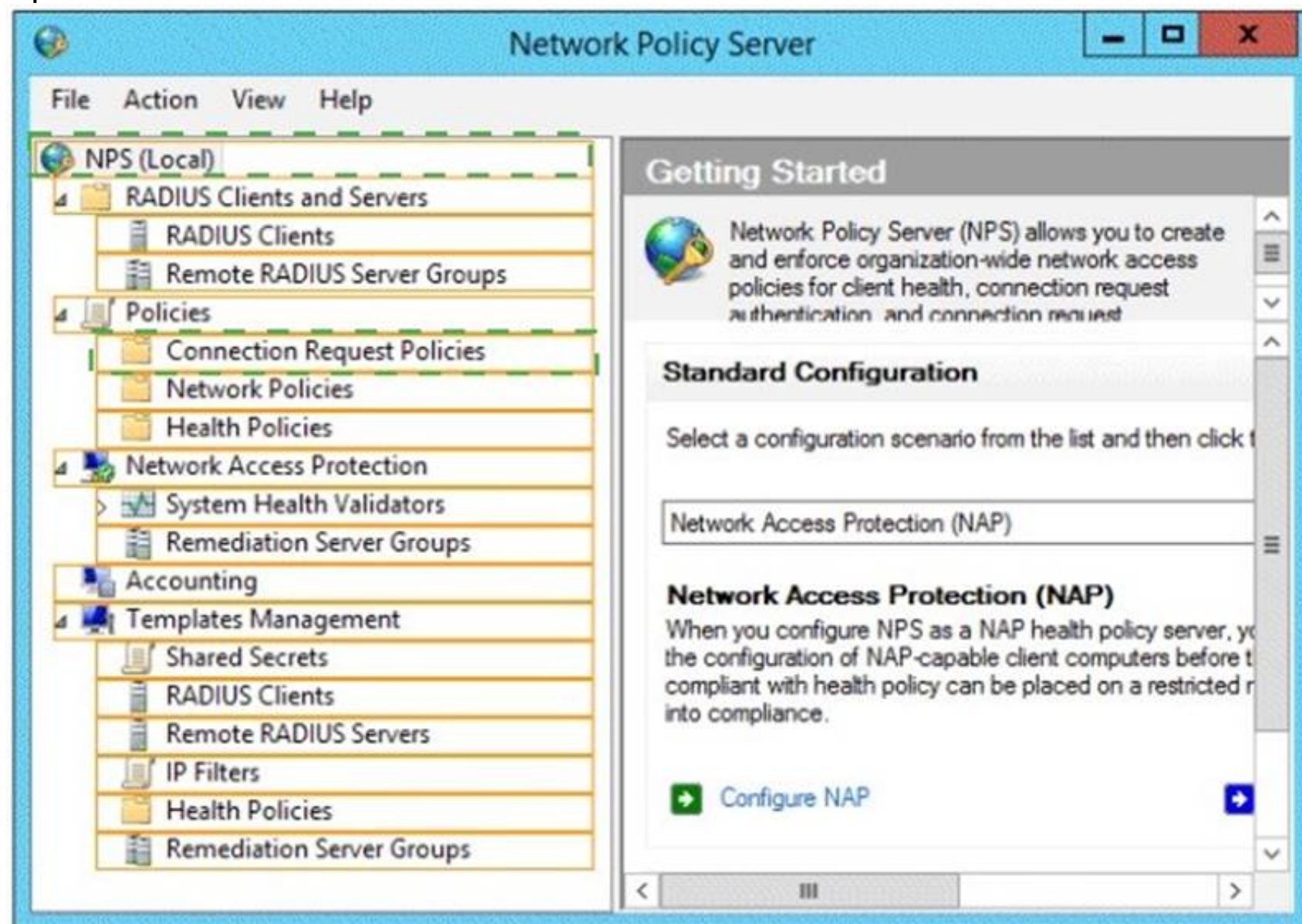
Which two nodes should you configure from the Network Policy Server console? To answer, select the appropriate two nodes in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 99

- (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 screenshot shows the 'Performance Monitoring Details' dialog box with the 'Alert' tab selected. The 'General' tab is also visible. The 'Alert' tab contains the following settings:

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

At the bottom, there is a status bar showing 'Min: 0 , Max: 0 , Last: 0' and buttons for 'OK', 'Cancel', and 'Help'.

NEW QUESTION 104

- (Topic 2)

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

All sales users have laptop computers that run Windows 8. The sales computers are joined to the domain. All user accounts for the sales department are in an organizational unit (OU) named Sales_OU.

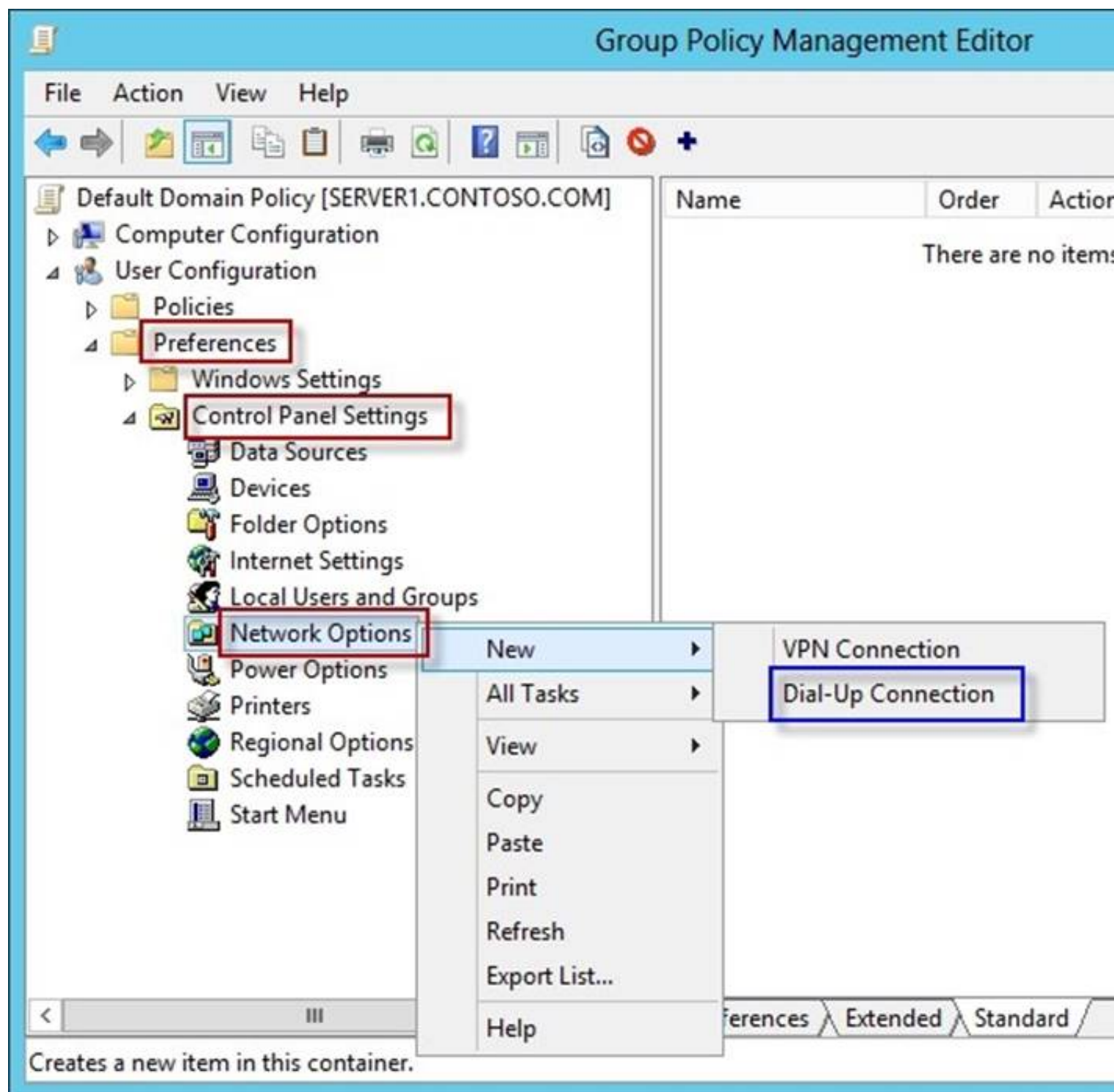
A Group Policy object (GPO) named GPO1 is linked to Sales_OU. You need to configure a dial-up connection for all of the sales users. What should you configure from User Configuration in GPO1?

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

Answer: B

Explanation:

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



To create a new Dial-Up Connection preference item

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

References:

<http://technet.microsoft.com/en-us/library/cc772107.aspx>

<http://technet.microsoft.com/en-us/library/cc772107.aspx>

<http://technet.microsoft.com/en-us/library/cc772449.aspx>

NEW QUESTION 109

- (Topic 2)

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

On all of the domain controllers, Windows is installed in C:\Windows and the Active

Directory database is located in D:\Windows\NTDS\.

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

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

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

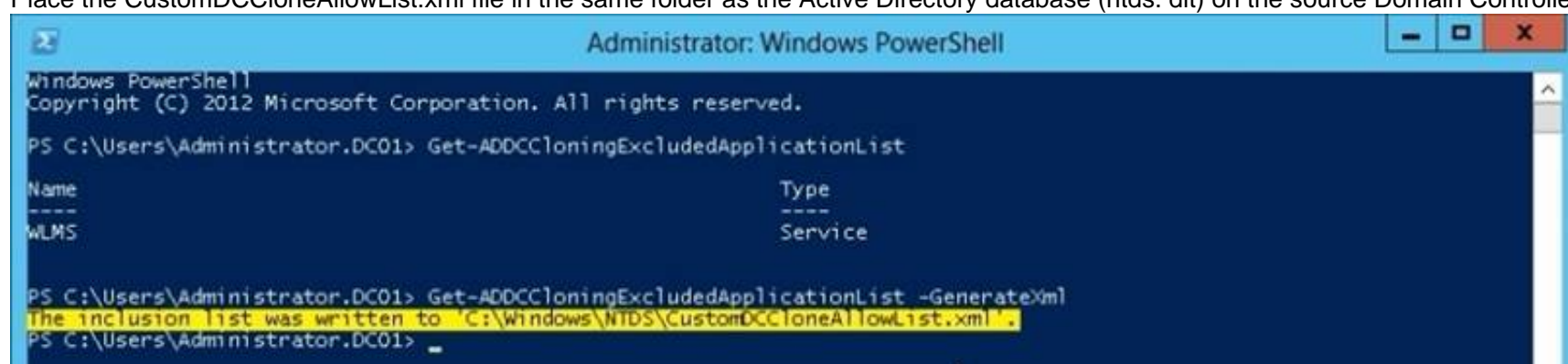
You need to prepare a domain controller for cloning. What should you do?

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

Answer: C

Explanation:

Place the CustomDCCloneAllowList.xml file in the same folder as the Active Directory database (ntds.dit) on the source Domain Controller.



References:

<http://blogs.dirteam.com/blogs/sanderberkouwer/archive/2012/09/10/new-features-in-active-directory-domain-services-in-windows-server-2012-part-13-domain-controller-cloning.aspx>
<http://www.thomasmaurer.ch/2012/08/windows-server-2012-hyper-v-how-to-clone-a-virtual-domain-controller>
<http://technet.microsoft.com/en-us/library/hh831734.aspx>

NEW QUESTION 113

- (Topic 2)

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

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

Answer: A

Explanation:

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

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

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

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

NEW QUESTION 114

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2. All client computers run Windows 8 Enterprise. DC1 contains a Group Policy object (GPO) named GPO1. You need to update the PATH variable on all of the client computers. Which Group Policy preference should you configure?

- A. Ini Files
- B. Services

- C. Data Sources
- D. Environment

Answer: D

Explanation:

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

NEW QUESTION 119

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2. Both servers have the File and Storage Services server role, the DFS Namespaces role service, and the DFS Replication role service installed. Server1 and Server2 are part of a Distributed File System (DFS) Replication group named Group1. Server1 and Server2 are separated by a low-speed WAN connection.

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

What should you modify?

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

Answer: D

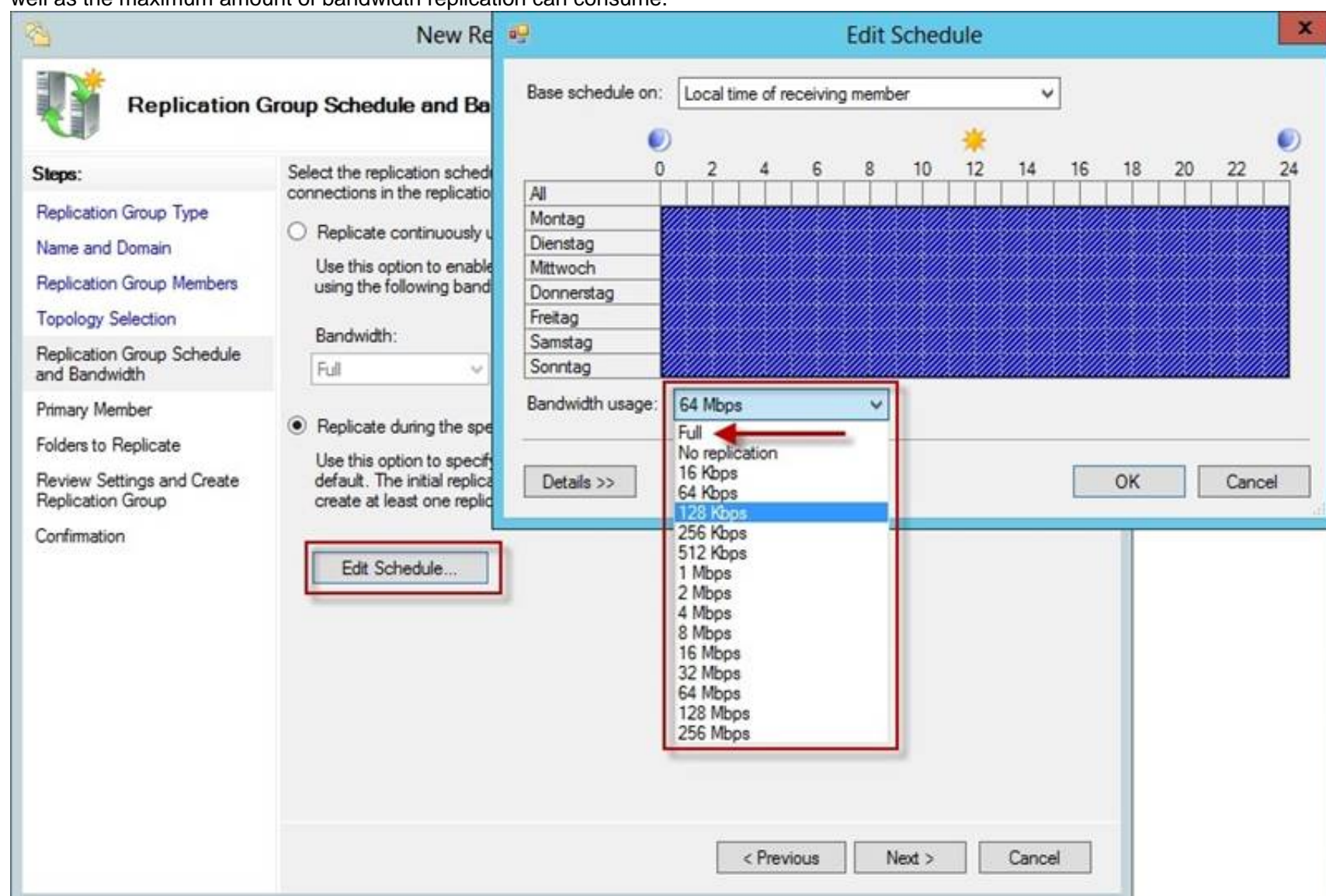
Explanation:

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

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

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

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



NEW QUESTION 120

- (Topic 2)

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

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

All client computers run Windows 8 Enterprise.

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

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

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

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

Answer: ABE

Explanation:

Requirements for HRA automatic discovery

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

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

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

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

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

NEW QUESTION 123

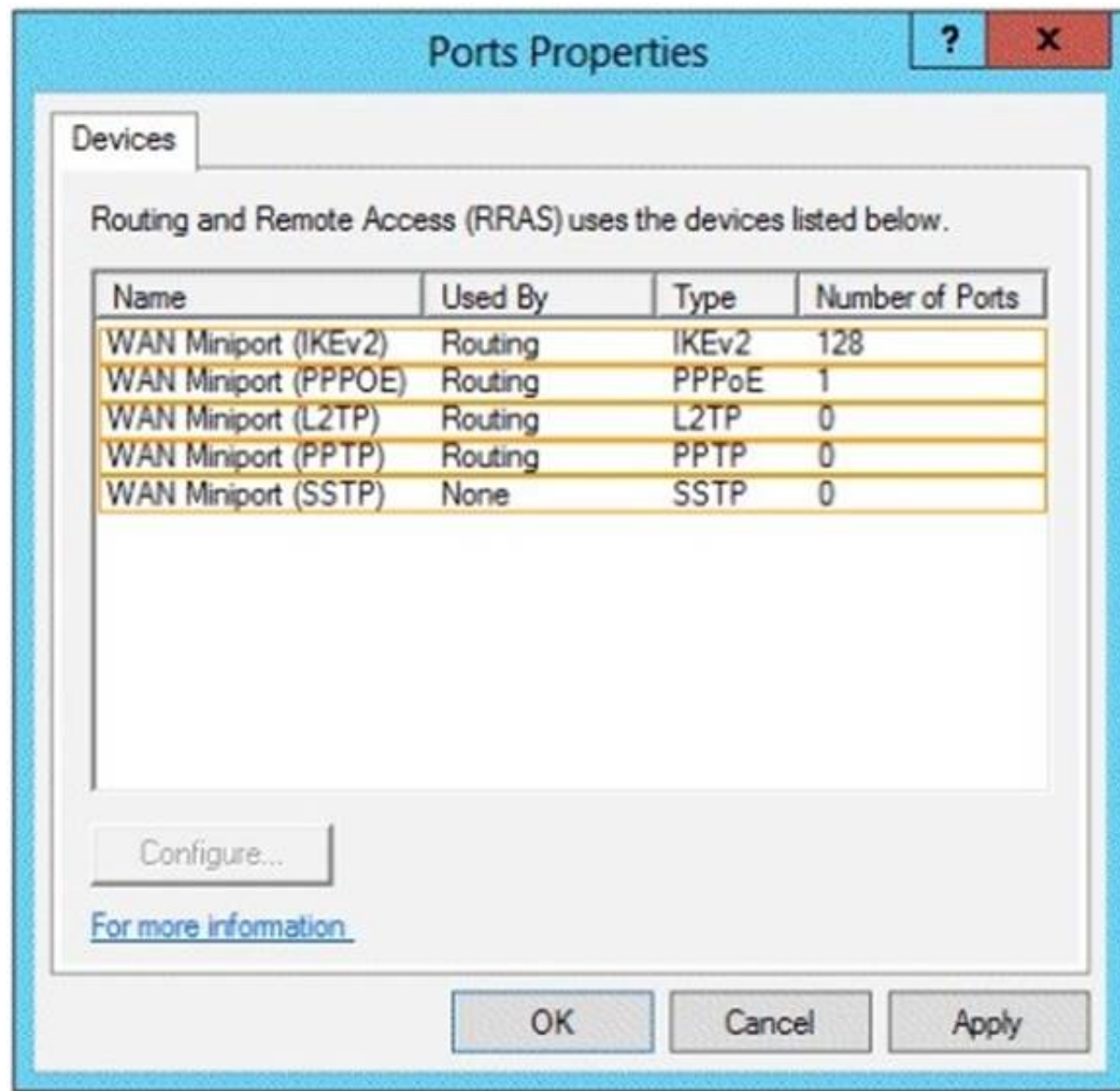
HOTSPOT - (Topic 2)

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

You need to configure the ports on Server1 to ensure that client computers can establish VPN connections to Server1. The solution must NOT require the use of certificates or pre-shared keys.

What should you modify?

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The four types of tunneling protocols used with a VPN/RAS server running on Windows Server 2012 include:

Point-to-Point Tunneling Protocol (PPTP): A VPN protocol based on the legacy Point-to-Point protocol used with modems. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality.

Layer 2 Tunneling Protocol (L2TP): Used with IPsec to provide security. L2TP supports either computer certificates or a preshared key as the authentication method for IPsec. IKEv2: IKE is short for Internet Key Exchange, which is a tunneling protocol that uses IPsec Tunnel Mode protocol. The message is encrypted with one of the following protocols by using encryption keys that are generated from the IKEv2 negotiation process.

Secure Socket Tunneling Protocol (SSTP): Introduced with Windows Server 2008, which uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls

References:

http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

NEW QUESTION 127

- (Topic 2)

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

You configure a custom service on VM1 named Service1.

You need to ensure that VM1 will be moved to a different node if Service1 fails. Which cmdlet should you run on Cluster1?

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

Answer: A

Explanation:

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

NEW QUESTION 131

- (Topic 3)

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

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

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

- A. Microsoft XPS Viewer
- B. Microsoft Report Viewer 2008 Redistributable Package

- C. Microsoft SQL Server 2008 R2 Report Builder 3.0
- D. Microsoft.NET Framework 2.0
- E. Microsoft SQL server 2012 Reporting Services (SSRS)

Answer: BD

NEW QUESTION 132

HOTSPOT - (Topic 3)

Your network contains one Active Directory domain named contoso.com. The domain contains two servers named Server01 and Server02 that run Windows Server 2012 R2.

Server01 is a member of a Distributed File System (DFS) replication group named RG01 that replicates to a folder named RF01.

You plan to replicate RF01 to Server02. RF01 will be pre-staged on Server02. You need export the DFS files and the DFS database from Server01.

Which tools should you use? To answer, select the appropriate options in the answer area.

Answer Area

Export DFS files:

	▼
Dfsrmig	
Export-BinaryMILog	
Export_DFSRClone	
Robocopy	
Sync-DFSRRReplicationGroup	

Export DFS database:

	▼
Dfsrmig	
Export-BinaryMILog	
Export_DFSRClone	
Robocopy	
Sync-DFSRRReplicationGroup	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

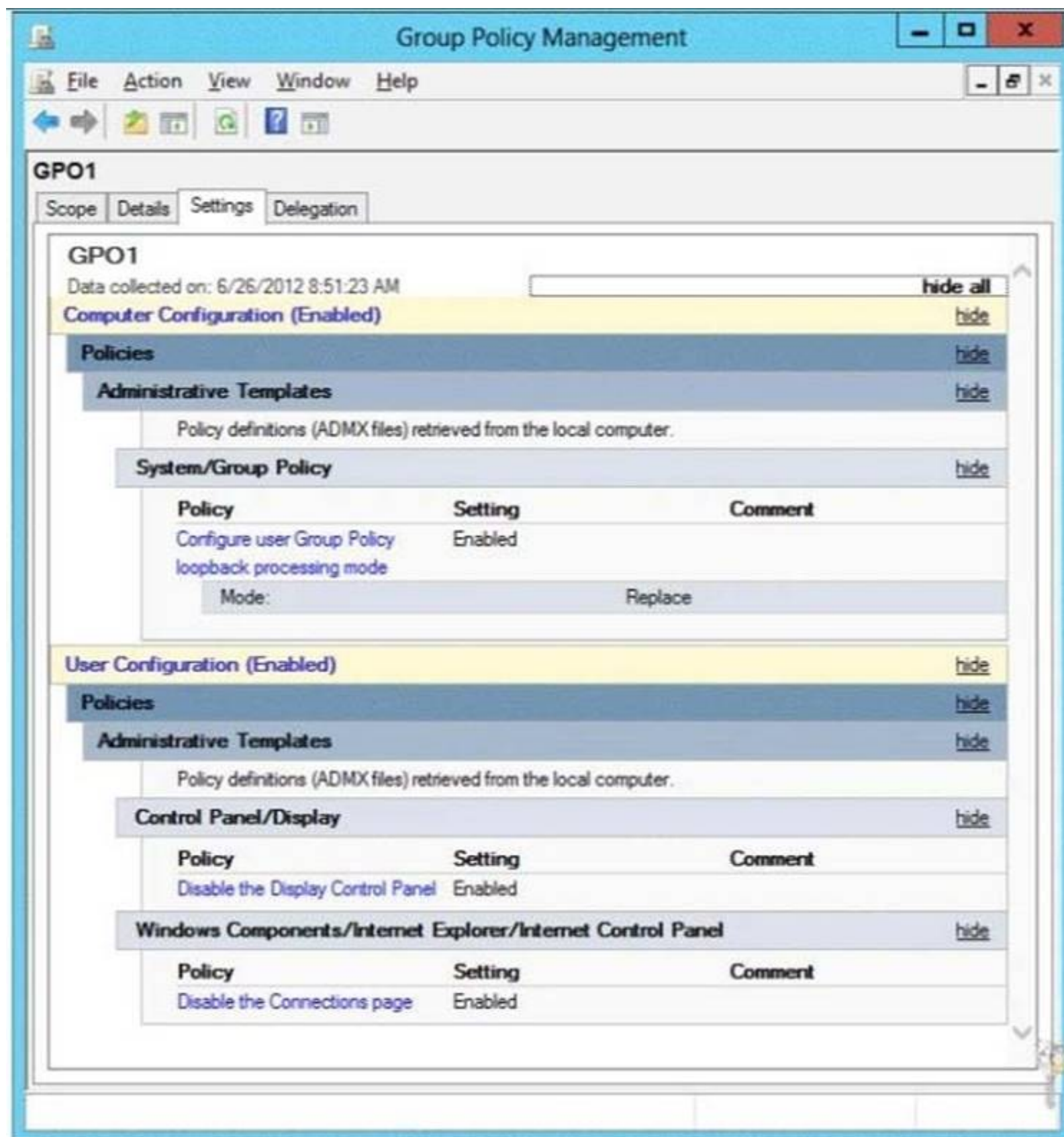
References: [https://technet.microsoft.com/en-us/library/dn495044\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn495044(v=ws.11).aspx) [https://technet.microsoft.com/en-us/library/dn482443\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn482443(v=ws.11).aspx)

NEW QUESTION 137

- (Topic 3)

Your network contains on Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named AllServers_OU.

You create and link a Group Policy object (GPO) named GPO1 to AllServer_OU. GPO1 is configured as shown in the exhibit. (Click the Exhibit button.)



You need to ensure that GPO1 only applies to servers that have Remote Desktop Services (RDS) installed
What should you configure?

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

Answer: D

Explanation:

If you need to configure a Remote Desktop Server farm and need to setup some group policies that only applied to computers that are Remote Desktop Servers, there are a couple of obvious ways you could achieve this.

- 1) You could put your Remote Desktop Servers in a specific Organisational Unit and link your Group Policies there
- 2) You could create a WMI Filter to filter by name i.e.

SELECT * FROM Win32_ComputerSystem WHERE ((Name = 'RDSERVER01') OR (Name = 'RDSERVER02'))

If you don't want to have to update the WMI Filter if you need to add more Remote Desktop Servers, you can use the following WMI Filter against the rootCIMV2TerminalServices Namespace:

Select * From Win32_TerminalServiceSetting Where TerminalServerMode=1

<http://www.focusedit.co.uk/54-group-policy-wmi-filter-for-remote-desktop-server/> <https://blogs.technet.microsoft.com/askds/2008/09/11/fun-with-wmi-filters-in-group-policy/>

NEW QUESTION 139

- (Topic 3)

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

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

You need to identify which domain controllers are authorized to be cloned by using virtual domain controller cloning.

Which cmdlet should you use?

- A. Get-ADGroupMember
- B. Get-ADDomainControllerPasswordReplicationPolicy

- C. Get-ADDomainControllerPasswordReplicationPolicyUsage
- D. Get-ADDomain
- E. Get-ADOptionalFeature
- F. Get-ADAccountAuthorizationGroup

Answer: D

Explanation:

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

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

Output would include a line such as: PDCEmulator : Fabrikam-DC1.Fabrikam.com Reference: Step-by-Step: Domain Controller Cloning

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

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

NEW QUESTION 142

- (Topic 3)

You have three Windows Server Update Services (WSUS) servers named Server01, Server02, Server03. Server01 synchronizes from Microsoft Update.

You need to ensure that only Server02 and Server03 can synchronize from Server01. What should you do on Server01?

- A. Modify %ProgramFiles%\Update Services\WebServices\serversyncweb service\Web.config.
- B. From the Update Services console, modify the Automatic Approvals options.
- C. Modify %ProgramFiles%\Update Services\WebServices\serversyncweb service\SimpleAuth.asmx.
- D. From the Update Services console, modify the Update Source and Proxy Server options.

Answer: D

Explanation:

References:

[https://technet.microsoft.com/en-us/library/hh852346\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh852346(v=ws.11).aspx)

NEW QUESTION 144

- (Topic 3)

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

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

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

Which cmdlet should you use?

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

Answer: D

Explanation:

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

NEW QUESTION 146

- (Topic 3)

Your network contains one Active Directory domain named contoso.com. You pilot DirectAccess on the network.

During the pilot deployment, you enable DirectAccess only for a group named Contoso\Test Computers.

Once the pilot is complete, you need to enable DirectAccess for all of the client computers in the domain.

What should you do?

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

Answer: B

Explanation:

References:

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

NEW QUESTION 150

- (Topic 3)

Your network contains two Active Directory forests named contoso.com and adatum.com. All domain controllers run Windows Server 2012 R2.

The adatum.com domain contains a Group Policy object (GPO) named GPO1. An administrator from adatum.com backs up GPO1 to a USB flash drive. You have a domain controller named dc1.contoso.com. You insert the USB flash drive in dc1.contoso.com. You need to identify the domain-specific reference in GPO1. What should you do?

- A. From the Migration Table Editor, click Populate from Backup.
- B. From Group Policy Management, run the Group Policy Modeling Wizard.
- C. From Group Policy Management, run the Group Policy Results Wizard.
- D. From the Migration Table Editor, click Populate from GPO.

Answer: A

NEW QUESTION 155

- (Topic 3)

Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1 that runs Windows Server 2012 R2. Server1 is configured as a Network Policy Server (NPS) server and as a DHCP server. The network contains two subnets named Subnet1 and Subnet2. Server1 has a DHCP scope for each subnet. You need to ensure that noncompliant computers on Subnet1 receive different network policies than noncompliant computers on Subnet2. Which two settings should you configure? (Each correct answer presents part of the solution. Choose two.)

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

Answer: CD

Explanation:

The NAP health policy server uses the NPS role service with configured health policies and system health validators (SHVs) to evaluate client health based on administrator-defined requirements. Based on results of this evaluation, NPS instructs the DHCP server to provide full access to compliant NAP client computers and to restrict access to client computers that are noncompliant with health requirements. If policies are filtered by DHCP scope, then MS-Service Class is configured in policy conditions.

NEW QUESTION 160

- (Topic 3)

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

- A. From Windows PowerShell, run the Set-DAServer cmdlet.
- B. From Remote Access Management Console, run the remote access Server Setup wizard.
- C. From Group Policy Management, modify the security filtering of an object named Direct Access Server Setting Group Policy
- D. From Group Policy Management, modify the security filtering of an object named Direct Access Client Setting Group Policy.

Answer: D

Explanation:

The simplified Direct Access wizard creates two GPOs and links them to the domain: "DirectAccess Server Settings" contains Connection Security Settings and Firewall inbound rules for Direct Access. "DirectAccess Clients Settings" sets name resolution policy for NLS validation. Both GPOs have security filtering applied, with DirectAccess Clients Settings applied only to the DirectAccess enabled clients.
http://www.windowsecurity.com/articles-tutorials/Windows_Server_2012_Security/windows-server-2012-simplified-directaccess-wizard-overview-Part1.html

NEW QUESTION 163

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012. You have a Group Policy object (GPO) named GPO1 that contains several custom Administrative templates. You need to filter the GPO to display only settings that will be removed from the registry when the GPO falls out of scope. The solution must only display settings that are either enabled or disabled and that have a comment. How should you configure the filter? To answer, select the appropriate options below. Select three.

Filter Options

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

Select the type of policy settings to display.

Managed:

Configured:

Commented:

Any

Any

Any

☐ Enable Keyword Filters

☒ Enable Keyword Filters

Filter for word(s):

Any

Within:

☒ Policy Setting Title

☒ Help Text

☒ Comment

☐ Enable Requirements Filters

Select the desired platform and application filter(s):

Include settings that match any of the selected platforms.

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

Select All

Clear All

OK

Cancel

Filter Options

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

Select the type of policy settings to display.

Managed:

Configured:

Commented:

Any

Any

Any

☐ Enable Keyword Filters

☒ Enable Keyword Filters

Filter for word(s):

Any

Within:

☒ Policy Setting Title

☒ Help Text

☒ Comment

☐ Enable Requirements Filters

Select the desired platform and application filter(s):

Include settings that match any of the selected platforms.

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

Select All

Clear All

OK

Cancel

- A. Set Managed to: Yes
- B. Set Managed to: No
- C. Set Managed to: Any
- D. Set Configured to: Yes
- E. Set Configured to: No
- F. Set Configured to: Any
- G. Set Commented to: Yes
- H. Set Commented to: No

The Leader of IT Certification

visit - <https://www.certleader.com>

I. Set Commented to: Any

Answer: AFG

NEW QUESTION 168

- (Topic 3)

Your network contains an Active Directory domain named contoso.com. You have a standard primary zone named contoso.com.

You need to ensure that only users who are members of a group named Group1 can create DNS records in the contoso.com zone. All other users must be prevented from creating, modifying, or deleting DNS records in the zone.

What should you do first?

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

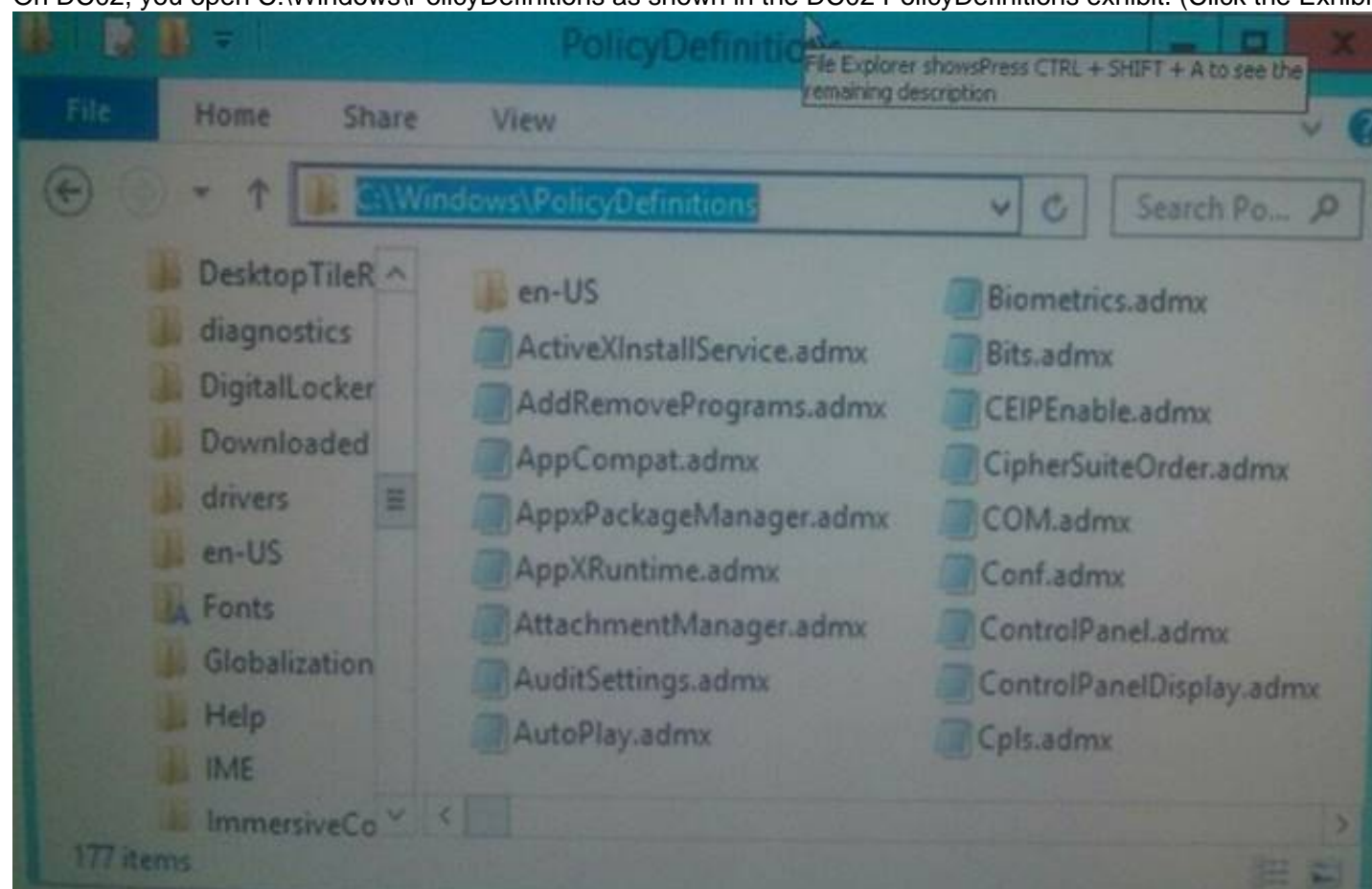
Answer: A

NEW QUESTION 169

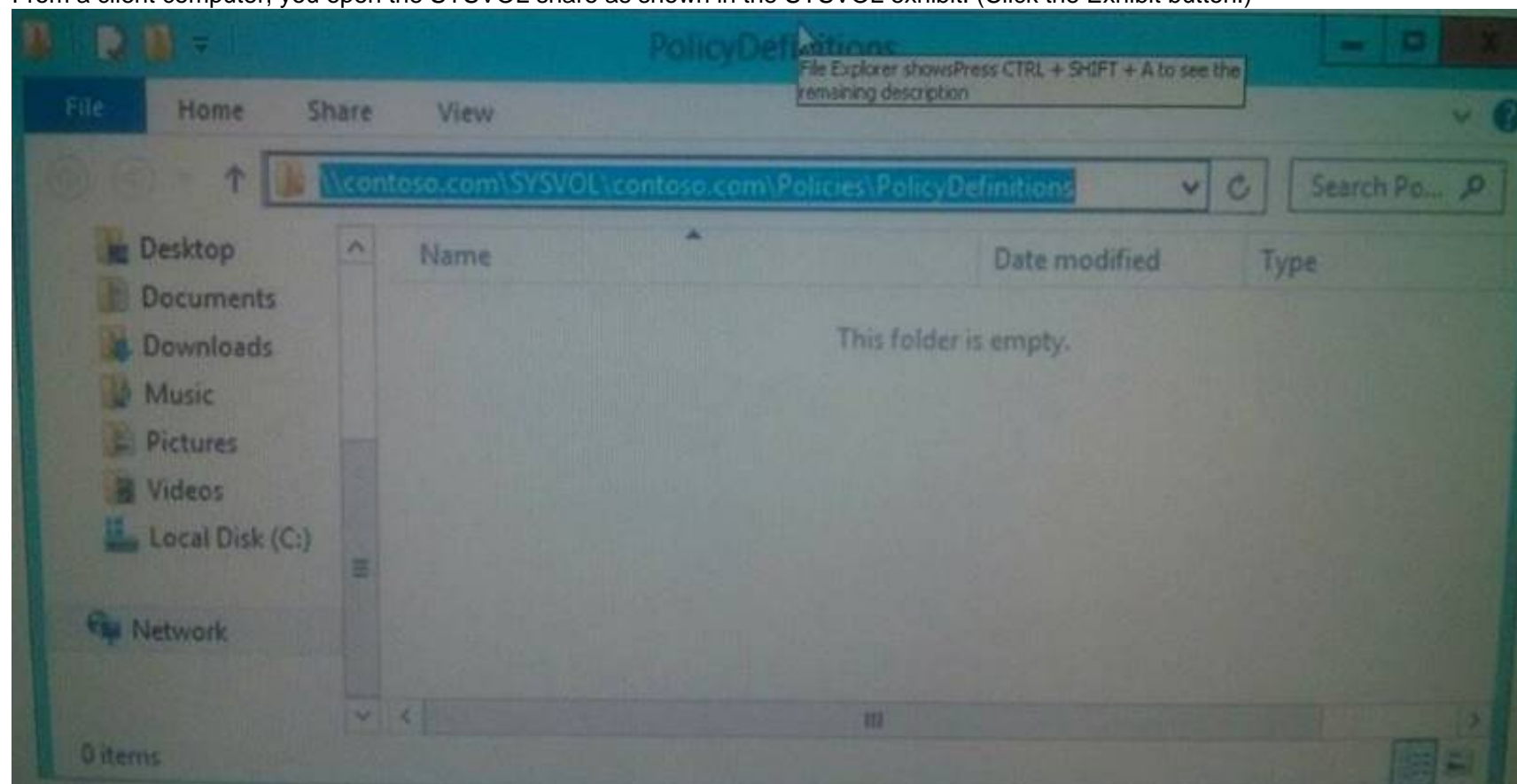
HOTSPOT - (Topic 3)

Your network contains one Active Directory domain named contoso.com. The domain contains two domain controllers named DC01 and DC02 that run Windows Server 2012 R2.

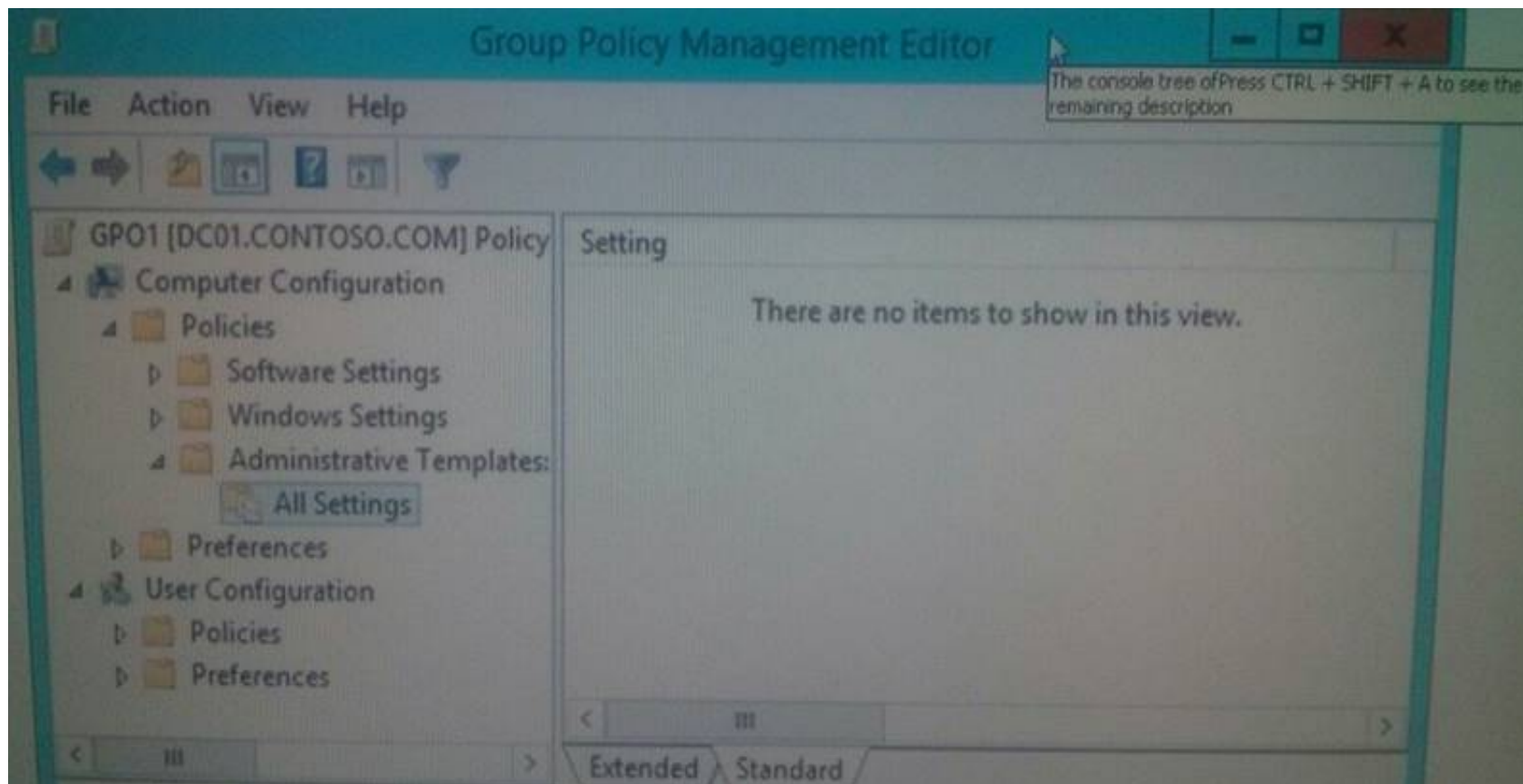
On DC02, you open C:\Windows\PolicyDefinitions as shown in the DC02 PolicyDefinitions exhibit. (Click the Exhibit button.)



From a client computer, you open the SYSVOL share as shown in the SYSVOL exhibit. (Click the Exhibit button.)



From DC01, you open a Group Policy object (GPO) named GPO1 as shown in the GPO1 exhibit. (Click the Exhibit button.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements

Yes No

A central store was created in the contoso.com domain.

☐☐

If you delete the %Systemroot%\SYSVOL\sysvol\contoso.com\Policies\PolicyDefinitions folder on DC01, settings will appear under the Administrative templates node of GPO1.

☐☐

If you create a new GPO on DC02, settings will appear under the Administrative Templates.

☐☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

Yes No

A central store was created in the contoso.com domain.

☒☐

If you delete the %Systemroot%\SYSVOL\sysvol\contoso.com\Policies\PolicyDefinitions folder on DC01, settings will appear under the Administrative templates node of GPO1.

☒☐

If you create a new GPO on DC02, settings will appear under the Administrative Templates.

☐☒

NEW QUESTION 170

DRAG DROP - (Topic 3)

Your network contains an Active Directory domain named contoso.com. The domain contains two member servers named Server1 and Server2. All servers run Windows Server 2012 R2.

You generalize Server2.

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

Which three actions should you perform?

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

Steps

- / create a capture image.
- / Create an install image.
- / Add the install image to the Windows Deployment Services server.

NEW QUESTION 174

HOTSPOT - (Topic 3)

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 JPG files can always be saved to a local computer, even when a file screen exists.

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

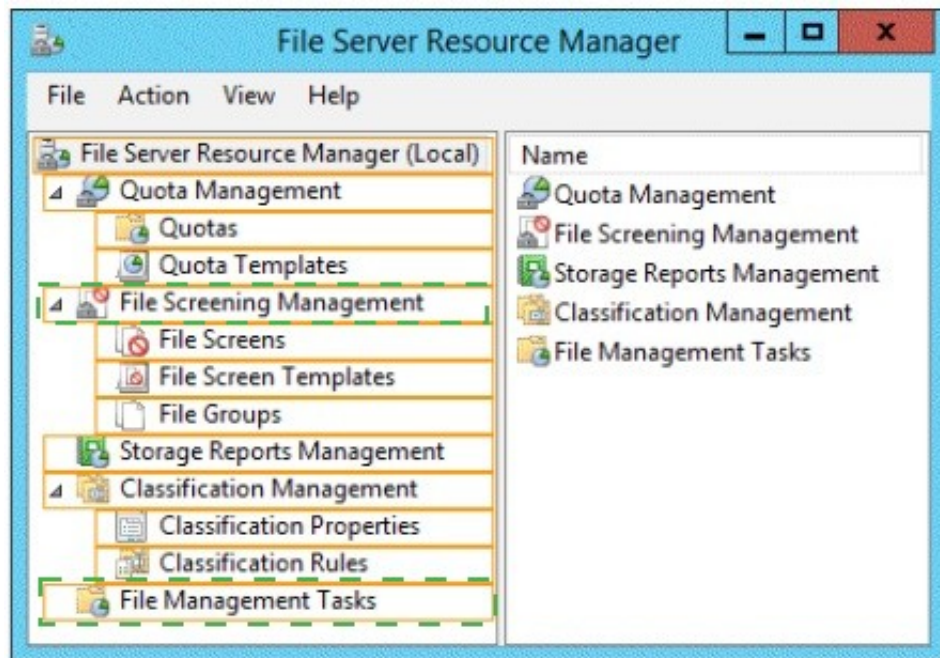
Answer Area



- A. Mastered
B. Not Mastered

Answer: A

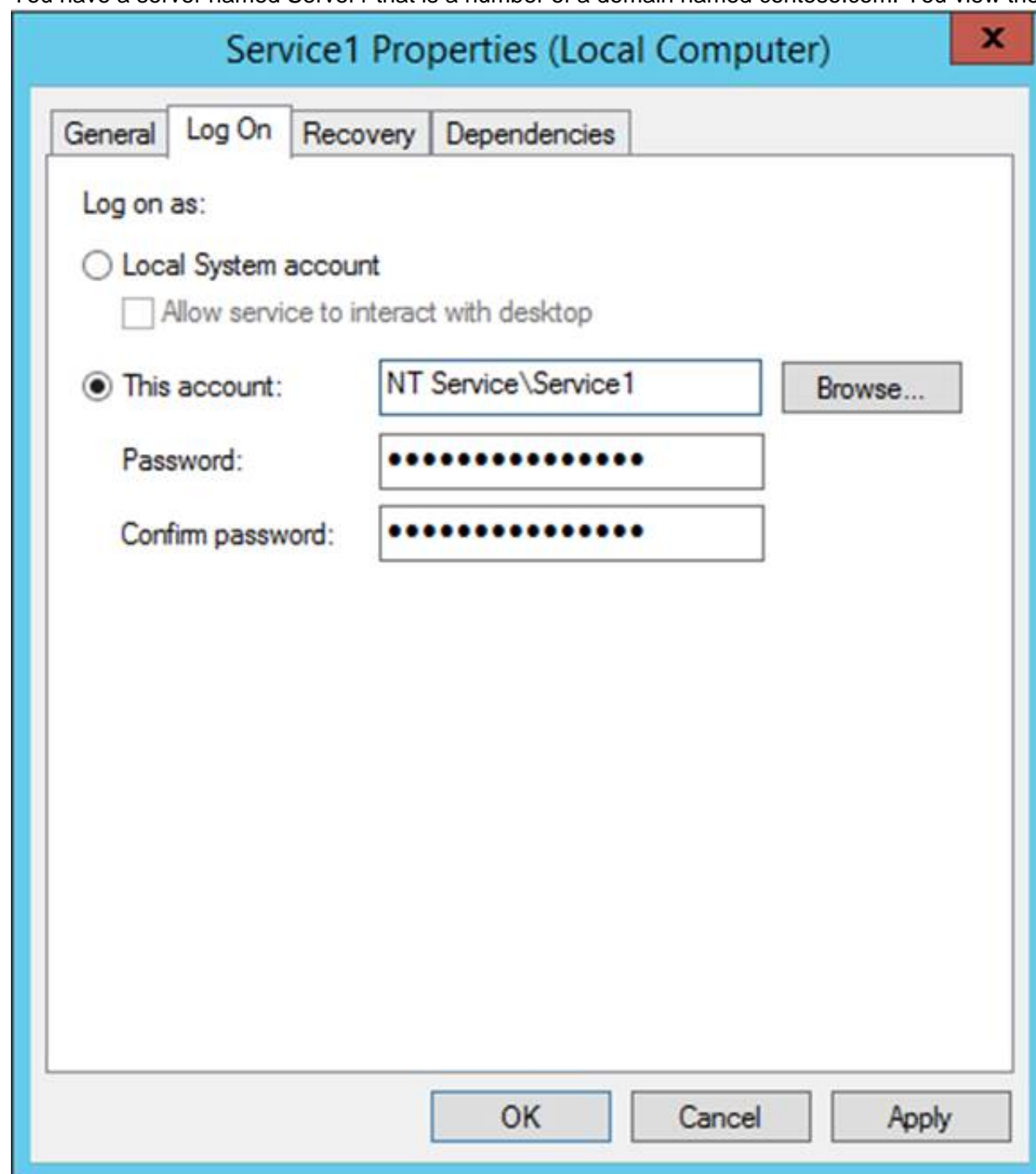
Explanation:



NEW QUESTION 175

CORRECT TEXT - (Topic 3)

You have a server named Server1 that is a member of a domain named contoso.com. You view the properties of a service on Server1 as shown in the graphic.



Use the drop-down menus to select the answer choice that completes each statement. NOTE: Each correct selection is worth one point.

Answer Area

Service1 is configured to use
[answere choice].

a local user account
a Managed Service Account
a virtual account

When accessing network
recources, Service1 will use the
identity of [answer choice].

the computer account
a domain user account
the Local System account
a local user account

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Service1 is configured to use
[answere choice].

a local user account
a Managed Service Account
a virtual account

When accessing network
recources, Service1 will use the
identity of [answer choice].

the computer account
a domain user account
the Local System account
a local user account

References:

[https://msdn.microsoft.com/en-us/library/ms677272\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms677272(v=vs.85).aspx) [https://msdn.microsoft.com/en-us/library/ms675915\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms675915(v=vs.85).aspx)

Service1 is configured to use [answer choice].

a virtual account

When accessing network resources, Service1
will use the identity of [answer choice].

the computer account

Virtual accounts are "managed local accounts" that provide the following features to simplify service administration:

- No password management is required.
- The ability to access the network with a computer identity in a domain environment.

Virtual accounts require very little management. They cannot be created or deleted, nor do they require any password management.

You must be a member of the Administrators group on the local computer to perform the following procedures. To configure a service to use a virtual account:

- Click Start, point to Administrative Tools, and then click Services.
- In the details pane, right-click the service that you want to configure, and then click Properties.
- Click the Log On tab, click This account, and then type NT SERVICE\ServiceName.

When you are finished, click OK.

- Restart the service for the change to take effect. [https://technet.microsoft.com/en-us/library/dd548356%20\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/dd548356%20(v=WS.10).aspx)

NEW QUESTION 179

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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