Microsoft.Passguide.70-411.v2013-11-13.by.Snowden.238q

Number: 70-411
Passing Score: 700
Time Limit: 120 min
File Version: 18.5

VCEplus.com

Exam Code: 70-411

Exam Name: Administering Windows Server 2012

Pass Guide
IT Certification • Exam Materials

Sections

1. Non Mobile VCE's
2. Configure and Manage Group Policy
3. Configure Network Services and Access Services
4. Configure file and print services
5. D-Deploy, manage and maintain servers
6. Configure a Network Policy infrastructure
7. Configure and manage AD
8. to review

VCEplus.com

Real Questions

QUESTION 1
Your network contains an Active Directory domain named contoso.com. The functional level of the forest is Windows Server 2008 R2.
Computer accounts for the marketing department are in an organizational unit (OU) named Departments\Marketing\Computers.
User accounts for the marketing department are in an OU named Departments\Marketing\Users.
All of the marketing user accounts are members of a global security group named MarketingUsers.
All of the marketing computer accounts are members of a global security group named MarketingComputers.
In the domain, you have Group Policy objects (GPOs) as shown in the exhibit. (Click the Exhibit button.)
You create two Password Settings objects named PSO1 and PSO2. PSO1 is applied to MarketingUsers. PSO2 is applied to MarketingComputers.
The minimum password length is defined for each policy as shown in the following table.

Location	Minimum password length
Default Domain Policy	7
GPO1	5
GPO2	6
PSO1	10
PSO2	12

You need to identify the minimum password length required for each marketing user.

What should you identify?

Exhibit:

Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: contoso.com
Domains
contoso.com
Default Domain Policy
Departments
Marketing
Computers
GPO1
Users
GPO2
Sales
Domain Controllers
Group Policy Objects
Group Policy Management
Contents
Name
Forest: contoso.com

A. 5
B. 6
C. 7
D. 10
E. 12

Correct Answer: D
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Password Setting Object (PSO) is another name for Fine Grain Password Policies. These PSOs allowed us to set up a different password policy based on security group membership. For example, an employee who is working on a multi billion dollar drug might need to have more characters in their password and more frequent password changes than someone who does not handle critical company data. PSOs allow us to do that.
Precedence:
In the case of a conflict in which a user is a member of more than one group with different PSOs assigned to each group, the one with the Precedence number that is lower will be the effective PSO

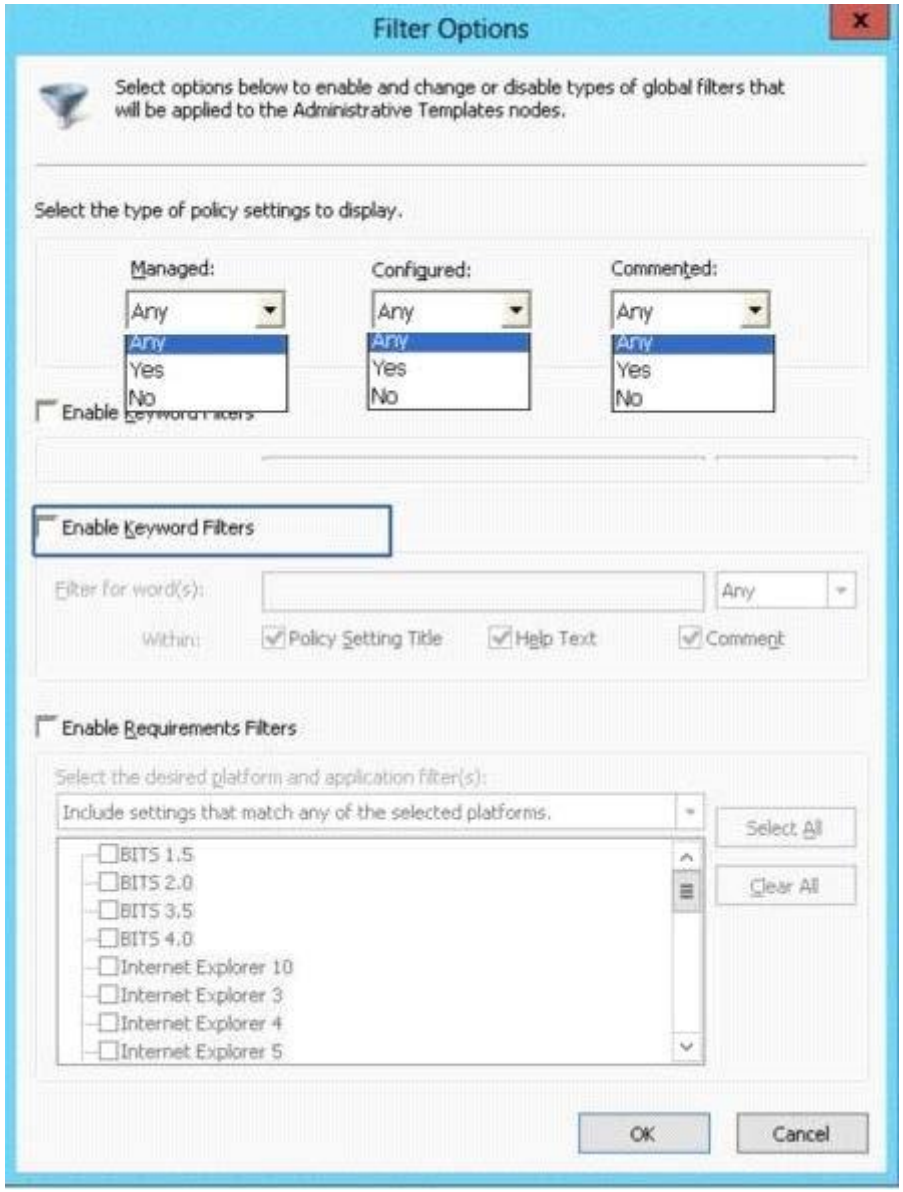
Applying fine-grained password policies: Fine-grained password policies **apply only to user objects** (or inetOrgPerson objects if they are used instead of user objects) and **global security groups**. **They cannot be applied to Computer objects**.

PSOs cannot be applied to organizational units (OUs) directly.
The PSO with the lowest priority takes precedence
If two PSOs have the same priority, the PSO with the smallest globally unique identifier (GUID) takes precedence.

http://technet.microsoft.com/en-us/library/cc770842%28v=ws.10%29.aspx

QUESTION 2
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.



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
I. Set Commented to: Any

Correct Answer: AFG
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Filter with Property Filters
The Local Group Policy Editor allows you to change the criteria for displaying Administrative Template policy settings. By default, the editor displays all policy settings, including unmanaged policy settings. However, you can use property filters to change how the Local Group Policy Editor displays Administrative Template policy settings.

http://technet.microsoft.com/en-us/library/cc732634.aspx
Administrative Templates are registry-based policy settings that appear under the Administrative Templates node of both the Computer and User Configuration nodes. This hierarchy is created when the Group Policy Management Console reads XML-based Administrative Template files (.admx).

http://technet.microsoft.com/en-us/library/cc731054.aspx

The Group Policy Management Console allows you to change the criteria for displaying Administrative Template policy settings. By default, the editor displays all policy settings, including unmanaged policy settings. However, you can use property filters to change how the Group Policy Management Console displays Administrative Template policy settings.

There are three inclusive property filters that you can use to filter Administrative Templates. These property filters include:
1. Managed
2. Configured
3. Commented

Managed

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

The Group Policy service does not govern unmanaged policy settings. These policy settings are persistent. The Group Policy service does not remove unmanaged

policy settings, even if the policy setting is not within scope of the user or computer. Typically, you use these types of policy settings to set preferences for operating system components that are not policy enabled. You can also use unmanaged policy settings for application settings.

The Managed property filter has three states: Any , Yes , and No . Setting this property filter to Any causes the Group Policy Management Console to display all Administrative Template policy settings. Setting this property filter to Yes causes the editor to show only managed Administrative Template policy settings, hiding all unmanaged Administrative Template policy settings. Setting this property filter to No causes the editor to show only unmanaged Administrative Template policy settings, hiding all managed Administrative Template policy settings.

Configured

You can configure Administrative Template policy settings to one of three states: Not Configured , Enabled , and Disabled . Not Configured is the default state for all policy settings. Policy settings set to Not Configured do not affect users or computers. Enabling an Administrative Template policy setting activates the policy setting. When Enabled , the action described in the title of the policy setting applies to the user or computer. When Disabled , the opposite action described in the title of the policy setting applies to the user or computer. Usually Not Configured and Disabled policy settings produce the same results. The difference is that Not Configured policy settings do not apply to the user, but Disabled policy settings apply to a user.

Each Administrative Template policy setting provides detailed information about its Enabled , Disabled , and Not Configured states. You can view this information in the Help pane of each Administrative Template policy setting. Or, you can view this information for the selected policy setting in the Extended View of the editor.

The Configured property filter has three states: Any , Yes , and No . Setting this property filter to Any causes the Group Policy Management Console to display all Administrative Template policy settings and is the default setting for this filter. Setting this property filter to Yes causes the editor to show only configured Administrative Template policy settings, hiding not configured policy settings. Setting this property filter to No causes the editor to show only not configured Administrative Template policy settings, hiding configured policy settings.

Commented

Each Administrative Template policy setting has a comment property. The Commented property allows you to enter text associated with a specific policy setting.

The Commented property filter has three states: Any , Yes , and No . Setting this property filter to Any causes the Group Policy Management Editor to display all Administrative Template policy settings and is the default setting for this filter. Setting this proper filter to Yes causes the editor to show only commented Administrative Template policy settings, hiding policy settings without comments. Setting this property filter to No causes the editor to show only Administrative Template policy settings without comments, hiding commented policy settings.

Additional considerations

- Filters are inclusive; therefore, select items you want to display rather than items you want to be removed.
- Filters do not work with Classic Administrative Templates.

A: Set Managed to: Yes

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

The Group Policy Client service does not govern *unmanaged* policy settings. These policy settings are persistent. The Group Policy Client service does not remove *unmanaged* policy settings, even if the policy setting is not within scope of the user or computer. Typically, you use these types of policy settings to configure options for operating system components that are not policy enabled. You can also use unmanaged policy settings for application settings.

F: Set Configured to: Any
We want to display both settings that are enable and disabled.

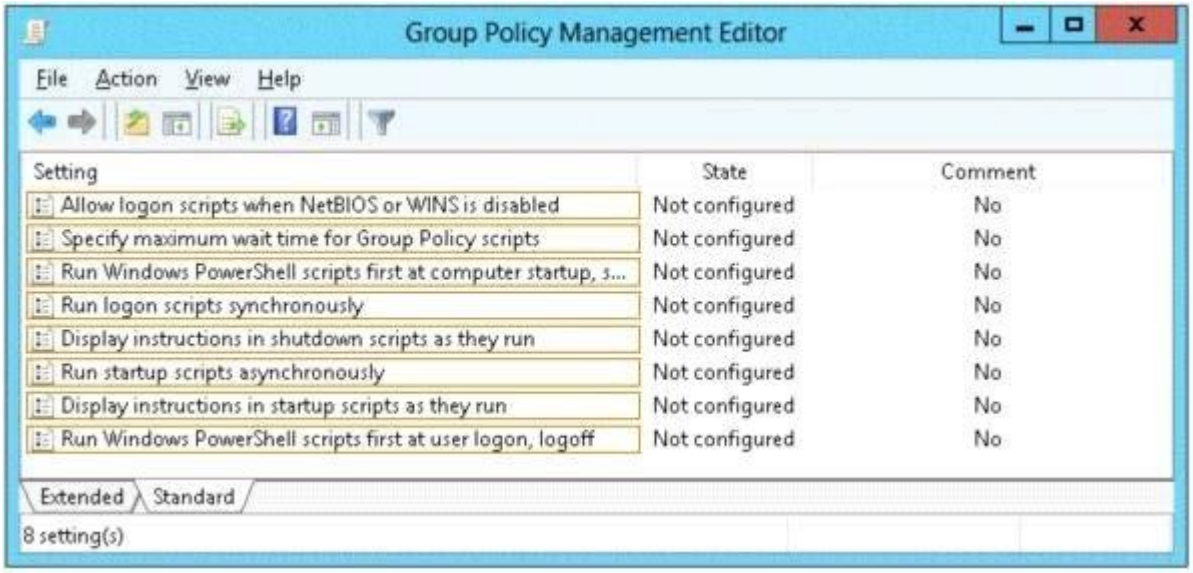
G: Set Commented to: Yes
Only settings that are commented should be displayed.

http://technet.microsoft.com/en-us/library/dd759104.aspx

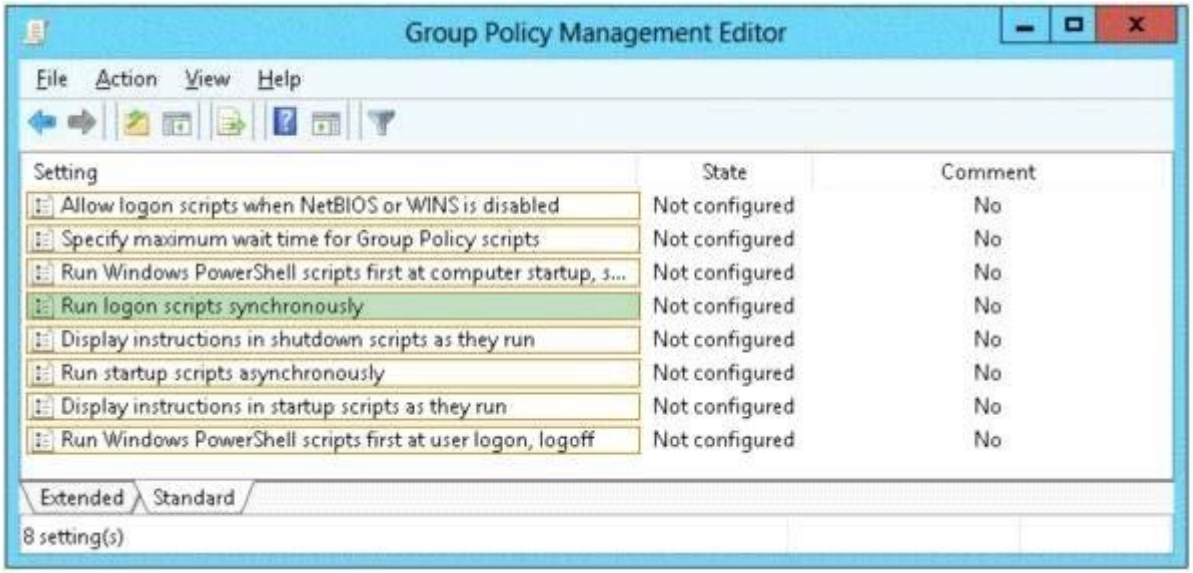
QUESTION 3
Your network contains an Active Directory domain named contoso.com. You have several Windows PowerShell scripts that execute when users log on to their client computer.
You need to ensure that all of the scripts execute completely before the users can access their desktop.

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

Hot Area:



Correct Answer:



Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Run logon scripts synchronously

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

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

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

http://technet.microsoft.com/en-us/library/cc958585.aspx

QUESTION 4
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named dc1.contoso.com.
You discover that the Default Domain Policy Group Policy objects (GPOs) and the Default Domain Controllers Policy GPOs were deleted.
You need to recover the Default Domain Policy and the Default Domain Controllers Policy GPOs.

What should you run?

A. dcgpofix.exe /target:domain
B. gpfixup.exe /dc:dc1.contoso.com
C. dcgpofix.exe /target:both
D. gptixup.exe /oldnb:contoso /newnb:dc1

Correct Answer: C
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

```
DCGPOFix [/ignoreschema] [/target: {Domain | DC | Both}] [/?]
```

Dcgpofix - Recreates the default Group Policy Objects (GPOs) for a domain. You will lose any changes that you have made to this GPOs

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Dcgpofix /Target:Both

Microsoft(R) Windows(R) Operating System Default Group Policy Restore Utility v5.1

Copyright (C) Microsoft Corporation. 1981-2003

Description: Recreates the Default Group Policy Objects (GPOs) for a domain

Syntax: DcGPOFix [/ignoreschema] [/Target: Domain | DC | BOTH]


This utility can restore either or both the Default Domain Policy or the
Default Domain Controllers Policy to the state that exists immediately after
domain creation. You must be a domain administrator to perform this operation.

WARNING: YOU WILL LOSE ANY CHANGES YOU HAVE MADE TO THESE GPOs. THIS UTILITY
IS INTENDED ONLY FOR DISASTER RECOVERY PURPOSES.

You are about to restore Default Domain Policy and Default Domain Controller Policy for the following domain
home.local
Do you want to continue: <Y/N>? y
WARNING: This operation will replace all 'User Rights Assignments' made in the chosen GPOs. This might cause some server
 applications to fail. Do you want to continue: <Y/N>? y
The Default Domain Policy was restored successfully
Note: Only the contents of the Default Domain Policy were restored. Group Policy links to this Group Policy Object were
not altered.
By default, the Default Domain Policy is linked to the domain.

The Default Domain Controller Policy was restored successfully
Note: Only the contents of the Default Domain Controller Policy were restored. Group Policy links to this Group Policy O
bject were not altered.
By default, the Default Domain Controller Policy is linked to the domain controllers OU.

PS C:\Users\Administrator>
```

http://technet.microsoft.com/en-us/library/hh875588(v=ws.10).aspx

QUESTION 5
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.
You have a Password Settings object (PSOs) named PSO1.
You need to view the settings of PSO1.

Which tool should you use?

A. Group Policy Management

B. Server Manager
C. Get-ADAccountResultantPasswordReplicationPolicy
D. Active Directory Administrative Center

Correct Answer: D
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

Active Directory Administrative Center

home (local) ‣ System ‣ Password Settings Container

PSO1

TASKS SECTIONS

Password Settings

Directly Applies To

Extensions

Password Settings

Name: PSO1

Precedence: 4

☑ Enforce minimum password length

Minimum password length (cha... 7

☑ Enforce password history

Number of passwords rememb... 24

☑ Password must meet complexity requirem...

☐ Store password using reversible encryption

☑ Protect from accidental deletion

Password age options:

☑ Enforce minimum password age

User cannot change the pass... 1

☑ Enforce maximum password age

User must change the passw... 42

☐ Enforce account lockout policy:

Number of failed logon attempt...

Reset failed logon attempts cou... 30

Account will be locked out

◉ For a duration of (mins): 30

○ Until an administrator manually unloc...

Description:

Directly Applies To

Name	Mail
AdminOU-PRT	

Add...

Remove

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

http://technet.microsoft.com/en-us/library/cc770848(v=ws.10).aspx

QUESTION 6
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs).
Currently, there are no enforced GPOs. You need to prevent all of the GPOs at the site level and at the domain level from being applied to users and computers in an organizational unit (OU) named OU1.
You want to achieve this goal by using the minimum amount of Administrative effort.

What should you use?

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

Correct Answer: I
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Set-GPInheritance - Blocks or unblocks inheritance for a specified domain or organizational unit (OU).

GPOs are applied according to the Group Policy hierarchy in the following order: local GPO, GPOs linked to the site, GPOs linked to the domain, GPOs linked to OUs. By default, an Active Directory container inherits settings from GPOs that are applied at the next higher level in the hierarchy. Blocking inheritance prevents the settings in GPOs that are linked to higher-level sites, domains, or organizational units from being automatically inherited by the specified domain or OU, unless the link (at the higher-level container) for a GPO is enforced.

```
C:\PS>

Set-GPinheritance -Target "ou=MyOU,dc=contoso,dc=com" -IsBlocked Yes


Name                  : myou

ContainerType         : OU

Path                  : ou=myou,dc=contoso,dc=com

GpoInheritanceBlocked : Yes

GpoLinks              : {TestGPO-1, TestGPO-2}

InheritedGpoLinks     : {TestGPO-1, TestGPO-2}
```

http://technet.microsoft.com/en-us/library/ee461032.aspx
http://technet.microsoft.com/en-us/library/cc757050.aspx

QUESTION 7
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. You have two GPOs linked to an organizational unit (OU) named OU1.
You need to change the precedence order of the GPOs.

What should you use?

A. dcgpofix
B. Get-GPOReport
C. Gpfixup
D. Gpresult
E. Gptedit.msc
F. Import-GPO

G. Restore-GPO
H. Set-GPInheritance
I. Set-GPLink
J. Set-GPPermission
K. Gpupdate
L. Add-ADGroupMember

Correct Answer: I
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

```
C:\PS>

Set-GPLink -Name TestGPO -Domain north.contoso.com -Target "dc=south, dc=contoso, dc=com" -LinkEnabeled Yes -Enforced Yes -Order 1
```

Set-GPLink - Sets the properties of the specified GPO link.

You can set the following properties:
-- Enabled. If the GPO link is enabled, the settings of the GPO are applied when Group Policy is processed for the site, domain or OU.
-- Enforced. If the GPO link is enforced, it cannot be blocked at a lower-level (in the Group Policy processing hierarchy) container.
-- Order. The order specifies the precedence that the settings of the GPO take over conflicting settings in other GPOs that are linked (and enabled) to the same site, domain, or OU.

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

QUESTION 8
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. You need to provide an Administrator named Admin1 with the ability to create GPOs in the domain. The solution must not provide Admin1 with the ability to link GPOs.

What should you use?

A. dcgpofix
B. Get-GPOReport
C. Gpfixup
D. Gpresult

E. Gptedit.msc
F. Import-GPO
G. Restore-GPO
H. Set-GPInheritance
I. Set-GPLink
J. Set-GPPermission
K. Gpupdate
L. Add-ADGroupMember

Correct Answer: J
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

```
C:\PS>

Set-GPPermissions -All -TargetName "Marketing Admins" -TargetType Group -PermissionLevel GpoEdit -Replace
```

Set-GPPermissions - Grants a level of permissions to a security principal for one GPO or all the GPOs in a domain.

Grants a level of permissions to a security principal (**user**, security group, or computer) for one GPO or all the GPOs in a domain. You use the TargetName and TargetType parameters to specify a user, security group, or computer for which to set the permission level. You can use the Name or the Guid parameter to set the permission level for the security principal on a single GPO, or you can use the All parameter to set the permission level for the security principal on all GPOs in the domain.

By default, if the security principal already has a higher permission level than the specified permission level, the change is not applied. You can specify the Replace parameter, to remove the existing permission level from the GPO before the new permission level is set. This ensures that the existing permission level is replaced by the new permission level.

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

QUESTION 9
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. The domain contains a GPO named GPO1. GPO1 contains several Group Policy preferences. You need to view all of the preferences configured in GPO1.

What should you use?

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

Correct Answer: B
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Get-GPOReport - Generates a report either in XML or HTML format for a specified GPO or for all GPOs in a domain.

```
Get-GPOReport [-Name] <string> -ReportType {<Xml> | <Html>} [-Domain <string>] [-Path <string>] [-Server <string>] [<CommonParameters>]
```

```
Get-GPOReport -Guid <Guid> -ReportType {<Xml> | <Html>} [-Domain <string>] [-Path <string>] [-Server <string>] [<CommonParameters>]
```

```
Get-GPOReport -All -ReportType {<Xml> | <Html>} [-Domain <string>] [-Path <string>] [-Server <string>] [<CommonParameters>]
```

The Get-GPOReport cmdlet generates a report in either XML or HTML format that describes properties and policy settings for a specified GPO or for all GPOs in a domain. The information that is reported for each GPO includes: details, links, security filtering, WMI filtering, delegation, and computer and user configurations.

You can specify the All parameter to generate a report for every GPO in the domain, or you can specify either the Name or Guid parameter to generate a report for a single GPO. You can also pipe GPO objects into this cmdlet. If you specify a file by using the Path parameter, the report is written to a file; otherwise, it is printed to the display.

http://technet.microsoft.com/en-us/library/ee461057.aspx
http://cmdlet.wordpress.com/2011/08/24/episode-3-get-gporeport/

QUESTION 10
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs).
Currently, there are no enforced GPOs. A network Administrator accidentally deletes the Default Domain Policy GPO.
You do not have a backup of any of the GPOs.
You need to recreate the Default Domain Policy GPO.

What should you use?

A. dcgpofix
B. Get-GPOReport
C. Gpfixup
D. Gptedit.msc
E. Import-GPO
F. Restore-GPO
G. Set-GPInheritance
H. Set-GPLink
I. Set-GPPermission
J. Gpupdate
K. Add-ADGroupMember

Correct Answer: A
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

```
DCGPOFix [/ignoreschema] [/target: {Domain | DC | Both}] [/?]
```

Dcgpofix - Recreates the default Group Policy Objects (GPOs) for a domain.

Restores the default Group Policy objects to their original state (that is, the default state after initial installation).

http://technet.microsoft.com/pt-pt/library/hh875588%28v=ws.10%29.aspx

QUESTION 11
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. Gptedit.msc
F. Import-GPO
G. Restore-GPO
H. Set-GPInheritance
I. Set-GPLink
J. Set-GPPermission
K. Gpupdate
L. Add-ADGroupMember

Correct Answer: C
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

```
gpfixup /olddns: MyOldDnsName /newdns:MyNewDnsName /oldnb:MyOldNetBIOSName /newnb:MyNewNetBIOSName /dc:MyDcDnsName 2>&1 >gpfixup.log
```

Gpfixup - Fix domain name dependencies in Group Policy Objects (GPOs) and Group Policy links after a domain rename operation.

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.

http://technet.microsoft.com/en-us//library/hh852336%28v=ws.10%29.aspx

QUESTION 12
Your network contains an Active Directory domain named contoso.com. The domain contains more than 100 Group Policy objects (GPOs). Currently, there are no enforced GPOs. The domain contains a top-level organizational unit (OU) for each department.
A group named Group1 contains members from each department. You have a GPO named GPO1 that is linked to the domain.
You need to configure GPO1 to apply settings to Group1 only.

What should you use?

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

Correct Answer: J
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

```
C:\PS>

Set-GPPermissions -All -TargetName "Marketing Admins" -TargetType Group -PermissionLevel GpoEdit -Replace
```

Set-GPPermissions - Grants a level of permissions to a security principal for one GPO or all the GPOs in a domain.

Grants a level of permissions to a security principal (user, **security group**, or computer) for one GPO or all the GPOs in a domain. You use the TargetName and

TargetType parameters to specify a user, security group, or computer for which to set the permission level. You can use the Name or the Guid parameter to set the permission level for the security principal on a single GPO, or you can use the All parameter to set the permission level for the security principal on all GPOs in the domain.

By default, if the security principal already has a higher permission level than the specified permission level, the change is not applied. You can specify the Replace parameter, to remove the existing permission level from the GPO before the new permission level is set. This ensures that the existing permission level is replaced by the new permission level.

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

QUESTION 13
Your network contains an Active Directory domain named contoso.com.
A user named User1 creates a central store and opens the Group Policy Management Editor as shown in the exhibit. (Click the Exhibit button.)

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

Exhibit:

A. Link a WMI filter to GPO1.
B. Add User1 to the Group Policy Creator Owners group.

C. Configure Security Filtering in GPO1.
D. Copy files from %Windir%\PolicyDefinitions to the central store.

Correct Answer: D
Section: Configure and Manage Group Policy
Explanation

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

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

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

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

http://support.microsoft.com/kb/929841/en-us

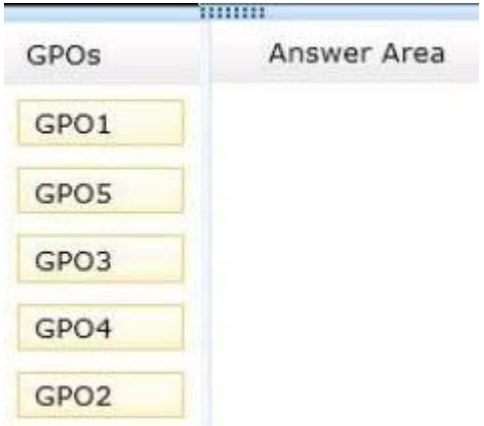
QUESTION 14
Your network contains a single Active Directory domain named contoso.com. The domain contains an Active Directory site named Site1 and an organizational unit (OU) named OU1.
The domain contains a client computer named Client1 that is located in OU1 and Site1. You create five Group Policy objects (GPO).
The GPOs are configured as shown in the following table.

GPO name	Linked to	Enforced setting
GPO1	Contoso.com	Disabled
GPO2	Contoso.com	Enabled
GPO3	Site1	Enabled
GPO4	OU1	Disabled
GPO5	OU1	Enabled

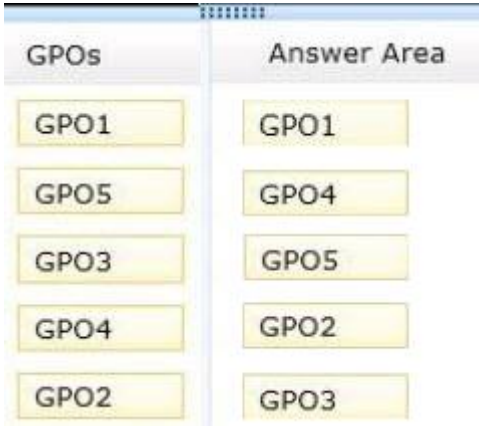
You need to identify in which order the GPOs will be applied to Client1.

In which order should you arrange the listed GPOs? To answer, move all GPOs from the list of GPOs to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Section: Configure and Manage Group Policy
Explanation

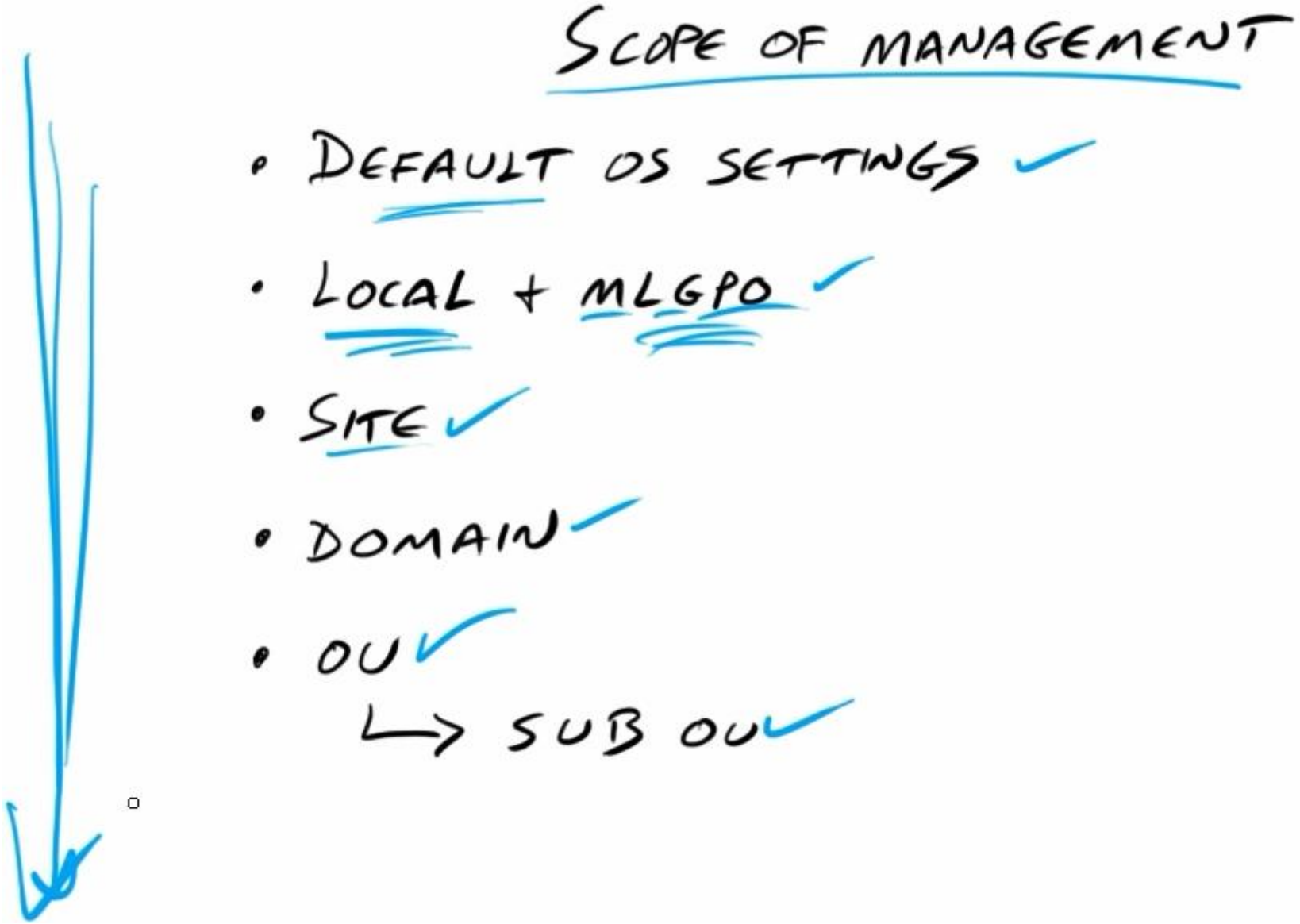
Explanation/Reference:
With enforcement, the parent GPO link always has precedence.

VCEplus.com

Applied by order:

domain
OU
OU enforcement
domain enforcement
site enforcement

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



GPOs are applied according to the Group Policy hierarchy in the following order:

1. **local GPO**
2. **GPOs linked to the site**

3. **GPOs linked to the domain**
4. **GPOs linked to OUs.**

By default, an Active Directory container inherits settings from GPOs that are applied at the next higher level in the hierarchy. Blocking inheritance prevents the settings in GPOs that are linked to higher-level sites, domains, or organizational units from being automatically inherited by the specified domain or OU, unless the link (at the higher-level container) for a GPO is enforced.

Links to a specific site, domain, or organizational unit are applied in reverse sequence based on link order. For example, a GPO with Link Order 1 has highest precedence over other GPOs linked to that container.

By default settings in Group Policy Objects (GPOs) get applied in the following order: Local system policies first, then policies on the Active Directory Domain level, then policies on the Active Directory Site level and then the policies for all the Organization Units the computer and user are members of, starting at the root of the domain. The settings that are last applied are the settings in effect.

http://blogs.technet.com/b/musings_of_a_technical_tam/archive/2012/02/15/understanding-the-structure-of-a-group-policy-object-part-2.aspx
http://technet.microsoft.com/en-us/library/cc757050.aspx

QUESTION 15
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.
You have a Password Settings object (PSOs) named PSO1.
You need to view the settings of PSO1.

Which tool should you use?

A. Get-ADFineGrainedPasswordPolicy
B. Get-ADAccountResultantPasswordReplicationPolicy
C. Get-ADDomainControllerPasswordReplicationPolicy
D. Get-ADDefaultDomainPasswordPolicy

Correct Answer: A
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Get-ADFineGrainedPasswordPolicy - Gets one or more Active Directory fine grained password policies

The Identity parameter specifies the Active Directory fine grained password policy to get. You can identify a fine grained password policy by its distinguished name (DN), GUID or name. You can also set the parameter to a fine grained password policy object variable, such as $<localFineGrainedPasswordPolicyObject> or pass a fine grained password policy object through the pipeline to the Identity parameter.

To search for and retrieve more than one fine grained password policies, use the Filter or LDAPFilter parameters. The Filter parameter uses the PowerShell

Expression Language to write query strings for Active Directory. PowerShell Expression Language syntax provides rich type conversion support for value types received by the Filter parameter. For more information about the Filter parameter syntax, see about_ActiveDirectory_Filter. If you have existing LDAP query strings, you can use the LDAPFilter parameter.

This cmdlet retrieves a default set of fine grained password policy object properties. To retrieve additional properties use the Properties parameter. For more information about the how to determine the properties for FineGrainedPasswordPolicy objects, see the Properties parameter description.

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

Command Prompt: C:\PS>

```
Get-ADFineGrainedPasswordPolicy AdminsPSO
```

```
Name : AdminsPSO
ComplexityEnabled : True
LockoutThreshold : 0
ReversibleEncryptionEnabled : True
LockoutDuration : 00:30:00
LockoutObservationWindow : 00:30:00
MinPasswordLength : 10
Precedence : 200
ObjectGUID : ba1061f0-c947-4018-a399-6ad8897d26e3
ObjectClass : msDS-PasswordSettings
PasswordHistoryCount : 24
MinPasswordAge : 1.00:00:00
MaxPasswordAge : 15.00:00:00
AppliesTo : {}
DistinguishedName : CN=AdminsPSO,CN=Password Settings Container,CN=System,DC=FABRIKAM,DC=COM

Description

-----------

Get the Fine Grained Password Policy named 'AdminsPSO'.
```

http://technet.microsoft.com/en-us/library/ee617231.aspx

QUESTION 16
Your network contains a production Active Directory forest named contoso.com and a test Active Directory forest named test.contoso.com. There is no network connectivity between contoso.com and test.contoso.com.

The test.contoso.com domain contains a Group Policy object (GPO) named GPO1.

You need to apply the settings in GPO1 to the contoso.com domain.

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

Select and Place:

Actions	Answer Area
Run the **Copy-GPO** cmdlet in test.contoso.com.	
Run the **Restore-GPO** cmdlet in contoso.com.	
Use removable media to transfer the contents of test.contoso.com to contoso.com.	
Run the **Copy-GPO** cmdlet in contoso.com.	
Run the **Backup-GPO** cmdlet in test.contoso.com.	
Run the **New-GPO** cmdlet in contoso.com.	
Run the **Import-GPO** cmdlet in contoso.com.	

Correct Answer:

Actions	Answer Area
Run the **Copy-GPO** cmdlet in test.contoso.com.	Run the **Backup-GPO** cmdlet in test.contoso.com.
Run the **Restore-GPO** cmdlet in contoso.com.	Use removable media to transfer the contents of test.contoso.com to contoso.com.
	Run the **New-GPO** cmdlet in contoso.com.
Run the **Copy-GPO** cmdlet in contoso.com.	Run the **Import-GPO** cmdlet in contoso.com.

Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
The correct answer is Backup/Import. Copy is an wrong answer because there is no trust relationship.

Backup. Backing up a GPO copies the data in the GPO to the file system. **The backup function also serves as the export capability for GPOs**. A GPO backup can be used to restore the GPO to the backed-up state, or to import the settings in the backup to another GPO.

Import. The Import operation transfers settings **into an existing GPO in Active Directory using a backed-up GPO in the file system location as its source**. Import operations can be used to transfer settings from one GPO to another GPO within the same domain, to a GPO in another domain in the same forest, or to a GPO in a domain in a different forest. The import operation always places the backed-up settings into an existing GPO. It erases any pre-existing settings in the destination GPO. **Import does not require trust between the source domain and destination domain**. Therefore it is useful for transferring settings across forests and domains that don't have trust. Importing settings into a GPO does not affect its DACL, links on sites domains or organizational units to that GPO, or a link to a WMI filter.

http://technet.microsoft.com/en-us/library/cc785343%28v=ws.10%29.aspx

QUESTION 17
Your network contains an Active Directory domain named contoso.com.

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

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

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

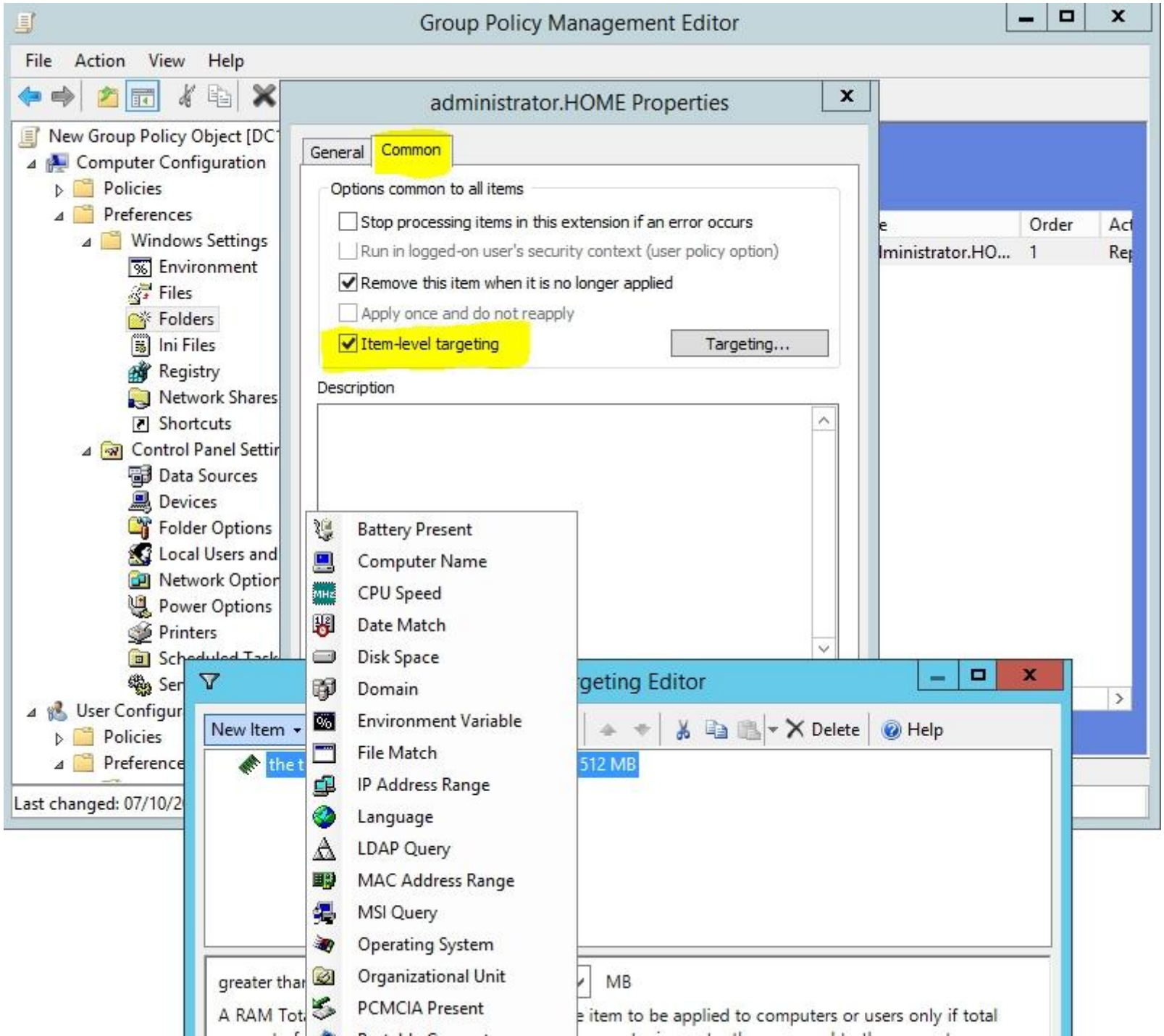
What should you configure?

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

Correct Answer: A
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

VCEplus.com


Group Policy Management Editor
File
Action
View
Help
administrator.HOME Properties
General
Common
Options common to all items
Stop processing items in this extension if an error occurs
Run in logged-on user's security context (user policy option)
Remove this item when it is no longer applied
Apply once and do not reapply
Item-level targeting
Targeting...
Description
New Group Policy Object [DC
Computer Configuration
Policies
Preferences
Windows Settings
Environment
Files
Folders
Ini Files
Registry
Network Shares
Shortcuts
Control Panel Settin
Data Sources
Devices
Folder Options
Local Users and
Network Optior
Power Options
Printers
User Configur
Policies
Preference
Last changed: 07/10/2
Order
Act
Iministrator.HO...
1
Rep
Battery Present
Computer Name
CPU Speed
Date Match
Disk Space
Domain
Environment Variable
File Match
IP Address Range
Language
LDAP Query
MAC Address Range
MSI Query
Operating System
Organizational Unit
PCMCIA Present
geting Editor
New Item
Delete
Help
512 MB
MB
greater than
A RAM Tot
item to be applied to computers or users only if total

A. You can use item-level targeting to change the scope of individual preference items, so they **apply only to selected users or computers**. Within a single Group Policy object (GPO), you **can include multiple preference items, each customized for selected users or computers and each targeted to apply settings only to the relevant users or computers**.
http://technet.microsoft.com/en-us/library/cc733022.aspx

B. You can further control precedence and how GPO links are applied to specific domains, sites, or organizational units by doing the following
Changing the link order
-Blocking Group Policy inheritance
-Enforcing a GPO link
-Disabling a GPO link

The settings deployed by GPOs linked to higher containers (parent container) in Active Directory are inherited by default to child containers and combine with any settings deployed in GPOs linked to child containers. If multiple GPOs attempt to set a setting to conflicting values, the GPO with the highest precedence sets the setting. GPO processing is based on a last writer wins model, and GPOs that are processed later have precedence over GPOs that are processed sooner.

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

D. Windows Management Instrumentation (WMI) filters allow you to dynamically determine the scope of Group Policy objects (GPOs) based on attributes of the target computer.
When a GPO that is linked to a WMI filter is applied on the target computer, the filter is evaluated on the target computer.
http://technet.microsoft.com/en-us/library/cc779036%28v=ws.10%29.aspx

QUESTION 18
Your network contains a single Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

The domain contains 400 desktop computers that run Windows 8 and 10 desktop computers that run Windows XP Service Pack 3 (SP3). All new desktop computers that are added to the domain run Windows 8.
All of the desktop computers are located in an organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1. GPO1 contains startup script settings. You link GPO1 to OU1.

You need to ensure that GPO1 is applied only to computers that run Windows XP SP3.

What should you do?

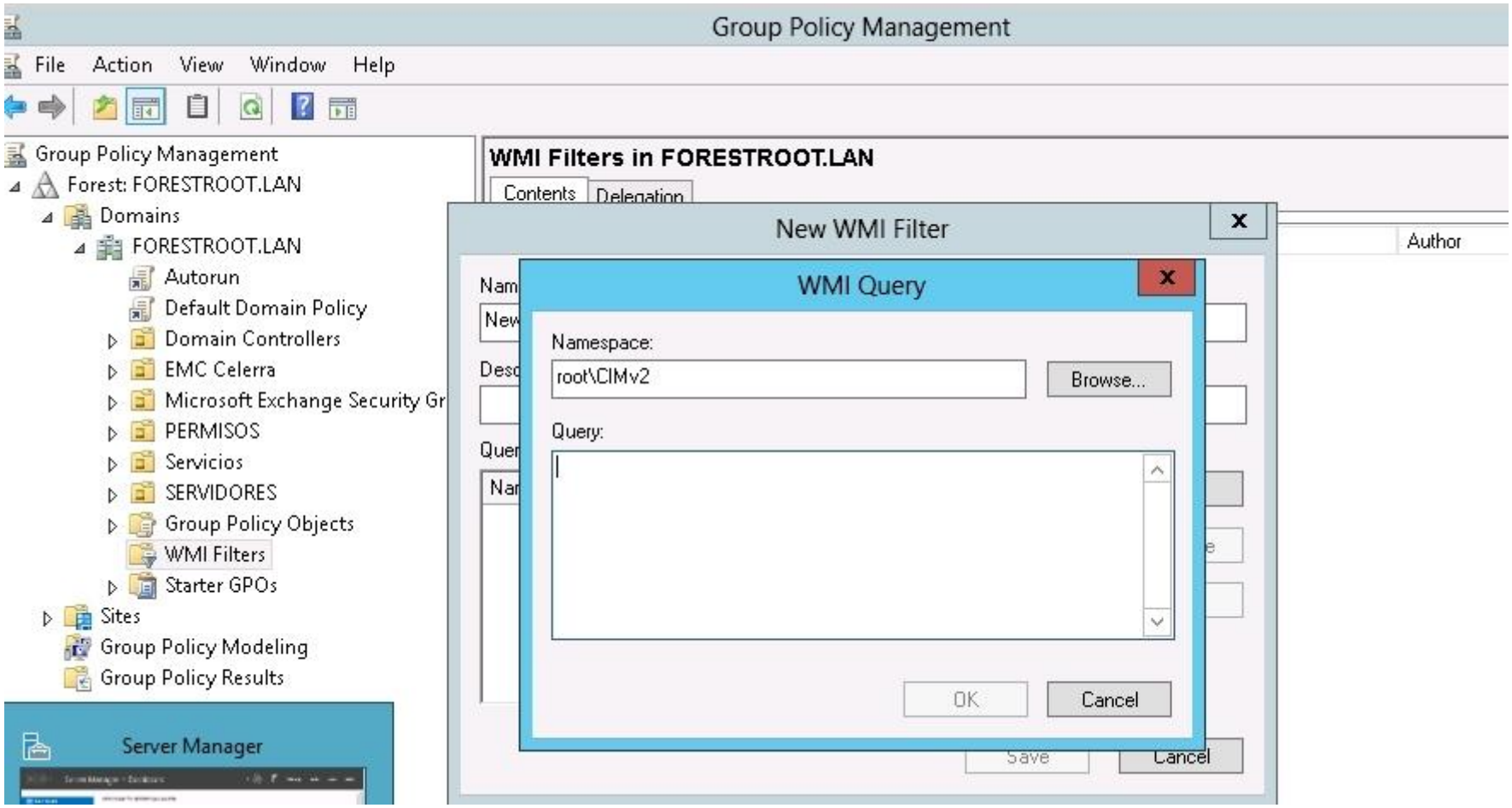
A. Modify the Security settings of OU1.
B. Run the Set-GPLink cmdlet and specify the -target parameter.
C. Create and link a WMI filter to GPO1.

D. Run the Set-GPInheritance cmdlet and specify the -target parameter.

Correct Answer: C
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Windows Management Instrumentation (WMI) filters allow you to dynamically determine the scope of Group Policy objects (GPOs) based on attributes of the target computer.
When a GPO that is linked to a WMI filter is applied on the target computer, the filter is evaluated on the target computer.

select * from Win32_OperatingSystem where Version = "5.1.2600" AND CSDversion = "Service Pack 3"



http://technet.microsoft.com/en-us/library/cc779036%28v=ws.10%29.aspx

QUESTION 19

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

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

Security setting	Requirement
Minimum password length	20
Account is sensitive and cannot be delegated	Disabled
User cannot change password	Disabled
Enforce password history	30

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

What should you identify?

To answer, configure the appropriate settings in the dialog box in the answer area.

Security setting	Configured by using
Minimum password length	
Account is sensitive and cannot be delegated	
User cannot change password	
Enforce password history	

Hot Area:

VCEplus.com

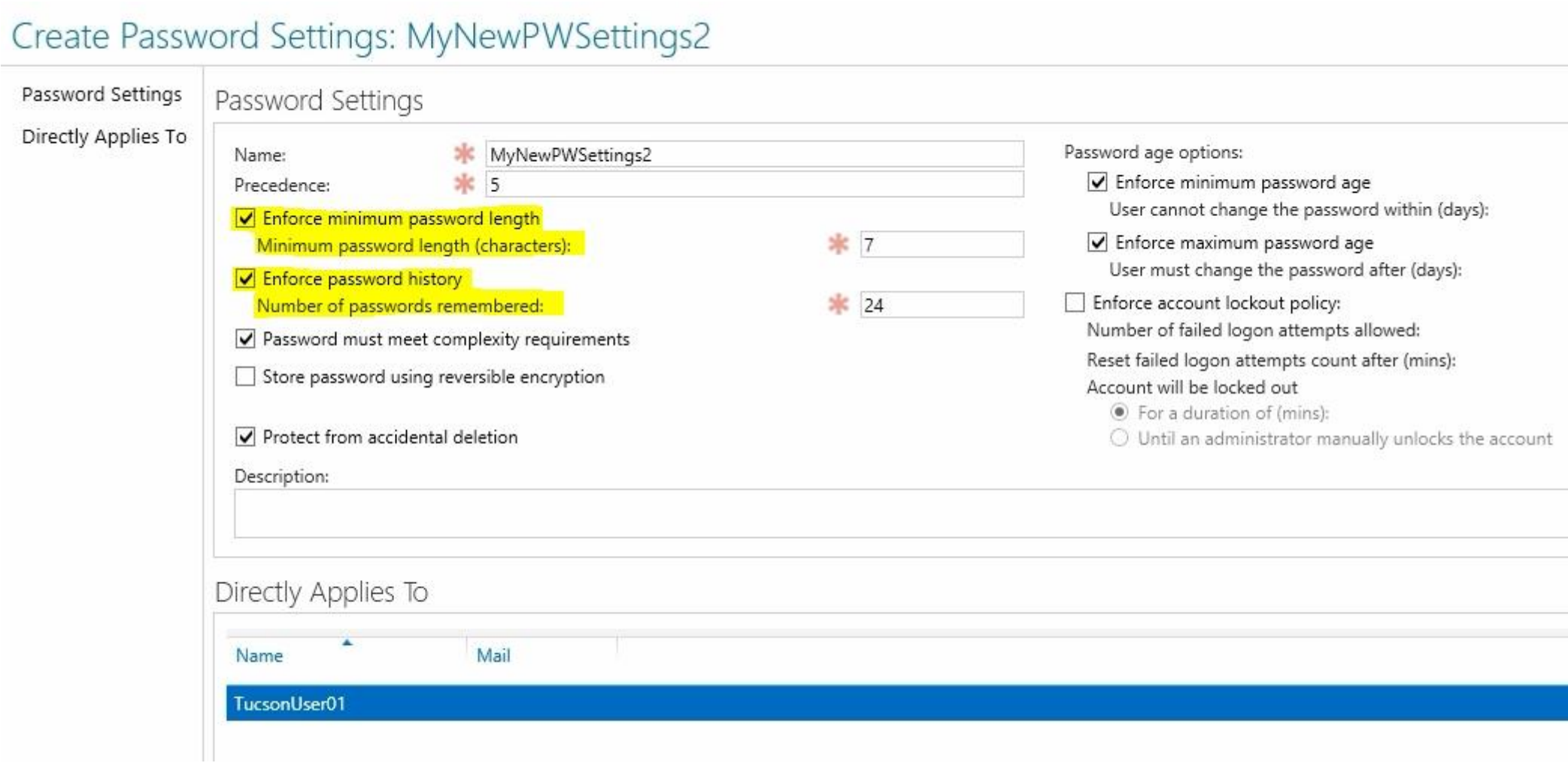
Security setting	Configured by using
Minimum password length	PSO User account properties
Account is sensitive and cannot be delegated	PSO User account properties
User cannot change password	PSO User account properties
Enforce password history	PSO User account properties

Correct Answer:

Security setting	Configured by using
Minimum password length	PSO User account properties
Account is sensitive and cannot be delegated	PSO User account properties
User cannot change password	PSO User account properties
Enforce password history	PSO User account properties

Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:



http://technet.microsoft.com/en-us/library/cc770842%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/dd145547.aspx

QUESTION 20
Computer1 is located in an OU, and the GPO1, User1 is another OU, and as GPO2, to ensure you can apply GPO1 to User1 should be how to do?

A. Security filtering

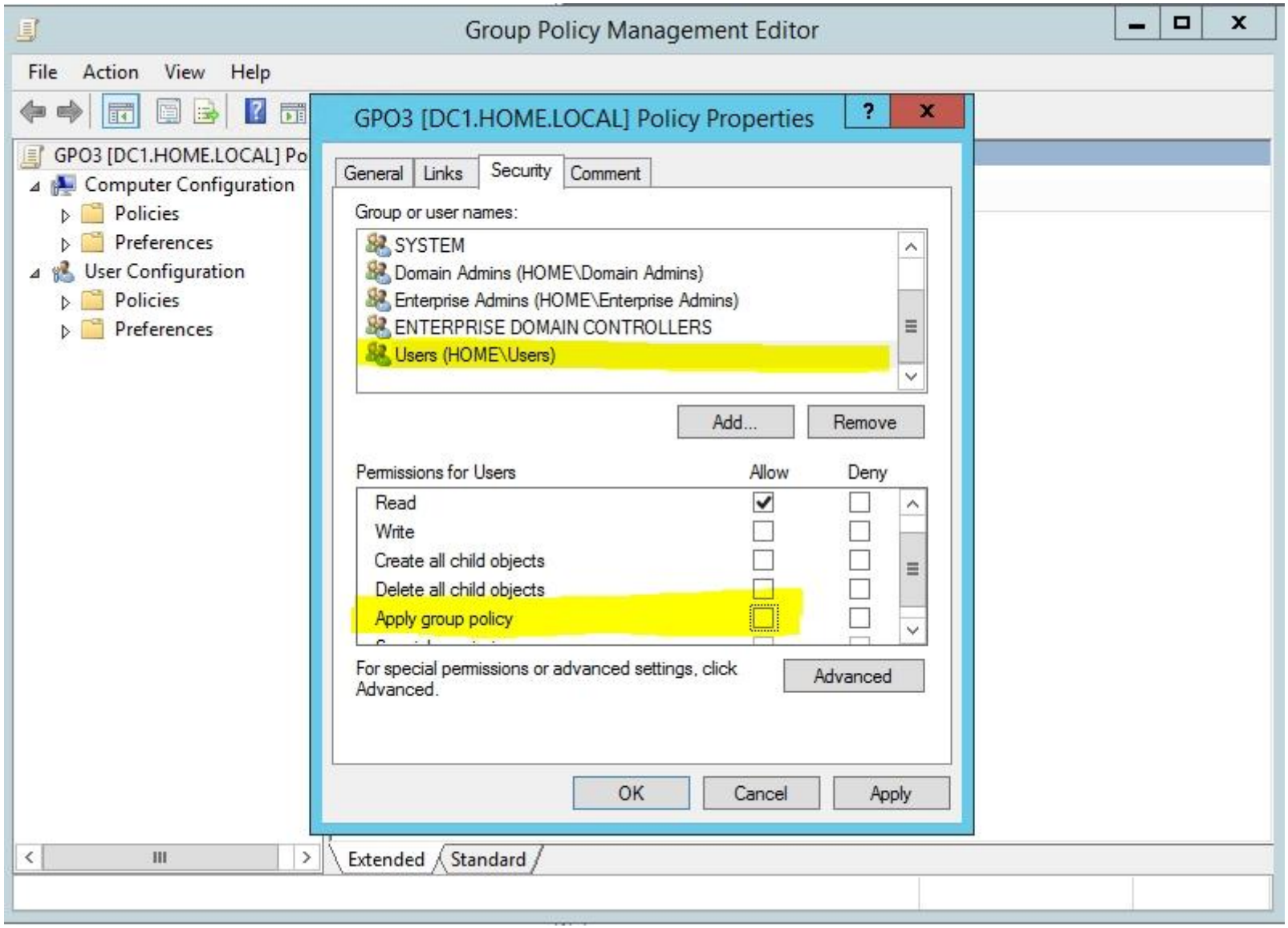
B. Inheritance
C. Gpupdate
D. GPO

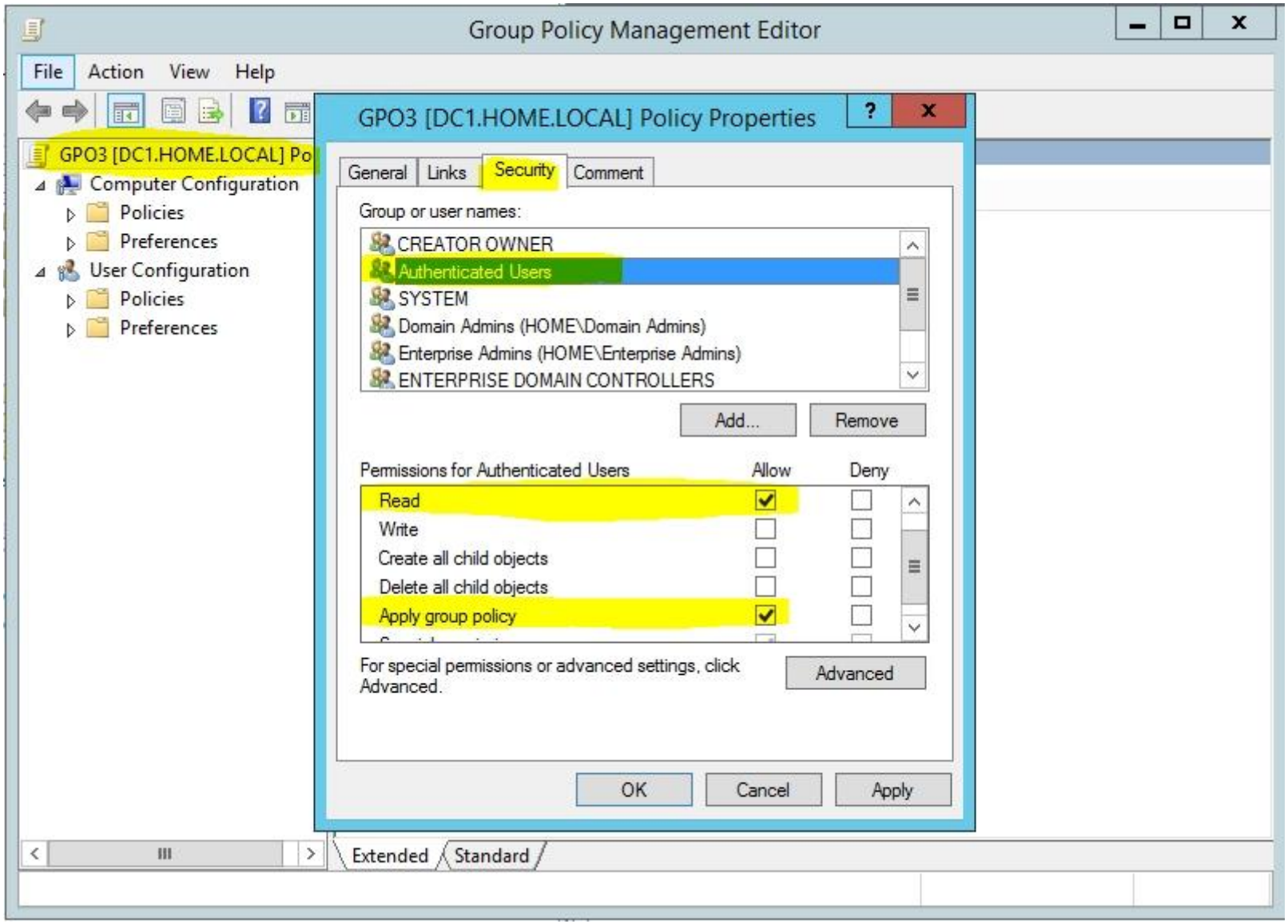
Correct Answer: A
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Security Filtering: this is simply tweaking permission on the Group Policy Object for a subset of targets (targets = users and computers in the scope of a policy). Users and Computers need both “Read” and “Apply Group Policy” permission on the object to successfully apply the GPO. If we had a “LockDown” GP that restricts the desktop to a minimum and we would apply that to the “ManufacturingOU”, all objects in that OU would be affected. To only apply the LockDown-GP to a number of targets, we can create an Active Directory group, put the target objects into the group and modify the security filtering settings in the “Scope” tab of the GP as shown in the screenshot:

GPOs cannot be linked directly to users, computers, or security groups. They can only be linked to sites, domains and organizational units. However, by using security filtering, you can narrow the scope of a GPO so that it applies only to a single group, user, or computer.

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


Group Policy Management Editor
File
Action
View
Help
GPO3 [DC1.HOME.LOCAL] Po
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
GPO3 [DC1.HOME.LOCAL] Policy Properties
General
Links
Security
Comment
Group or user names:
SYSTEM
Domain Admins (HOME\Domain Admins)
Enterprise Admins (HOME\Enterprise Admins)
ENTERPRISE DOMAIN CONTROLLERS
Users (HOME\Users)
Add...
Remove
Permissions for Users
Allow
Deny
Read
Write
Create all child objects
Delete all child objects
Apply group policy
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Extended
Standard



http://technet.microsoft.com/en-us/library/cc779291%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc781988%28v=ws.10%29.aspx
http://blogs.technet.com/b/grouppolicy/archive/2009/07/30/security-filtering-wmi-filtering-and-item-level-targeting-in-group-policy-preferences.aspx

QUESTION 21
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.
You have a Group Policy object (GPO) named GPO1 that contains hundreds of settings. GPO1 is linked to an organizational unit (OU) named OU1.
OU1 contains 200 client computers. You plan to unlink GPO1 from OU1.
You need to identify which GPO settings will be removed from the computers after GPO1 is unlinked from OU1.

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

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

Correct Answer: AD
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
There are two kinds of Administrative Template policy settings: **Managed** and **Unmanaged** .

An unmanaged policy setting makes a change that is persistent in the registry. If the GPO no longer applies, the setting remains. This is often called "tattooing" the registry—making a permanent change. To reverse the effect of the policy setting, you must deploy a change that reverts the configuration to the desired state.
By default, the GPME hides unmanaged policy settings to discourage you from implementing a configuration that is difficult to revert. However, you can make many useful changes with unmanaged policy settings, particularly for custom administrative templates to manage configuration for applications.
To control which policy settings are visible, right-click Administrative Templates and click Filter Options, and then make a selection from the Managed drop-down list.

The Group Policy service governs Managed policy settings and removes a policy setting when it is no longer within scope of the user or computer.
The Group Policy service does not govern unmanaged policy settings. These policy settings are **persistent**.
The Group Policy service does not remove unmanaged policy settings, even if the policy setting is not within scope of the user or computer.

Event Viewer: The Event Viewer has a wealth of information regarding Group Policy. Unfortunately, it requires you to look at all of the different log files to find entries for Group Policy. There you'll find entries related to policy application, policy replication, and policy refresh, all of which can be useful when trying to track down a problem. There is not always a lot of information on specific Group Policy errors in the event logs, but remember that you can always search TechNet if you find errors you can't identify.

http://technet.microsoft.com/en-us/library/cc731054.aspx
http://technet.microsoft.com/en-us/magazine/2007.02.troubleshooting.aspx

http://www.web-foro.com/wl/CompanionContent/course/crse6425b_00_06_04_02.htm

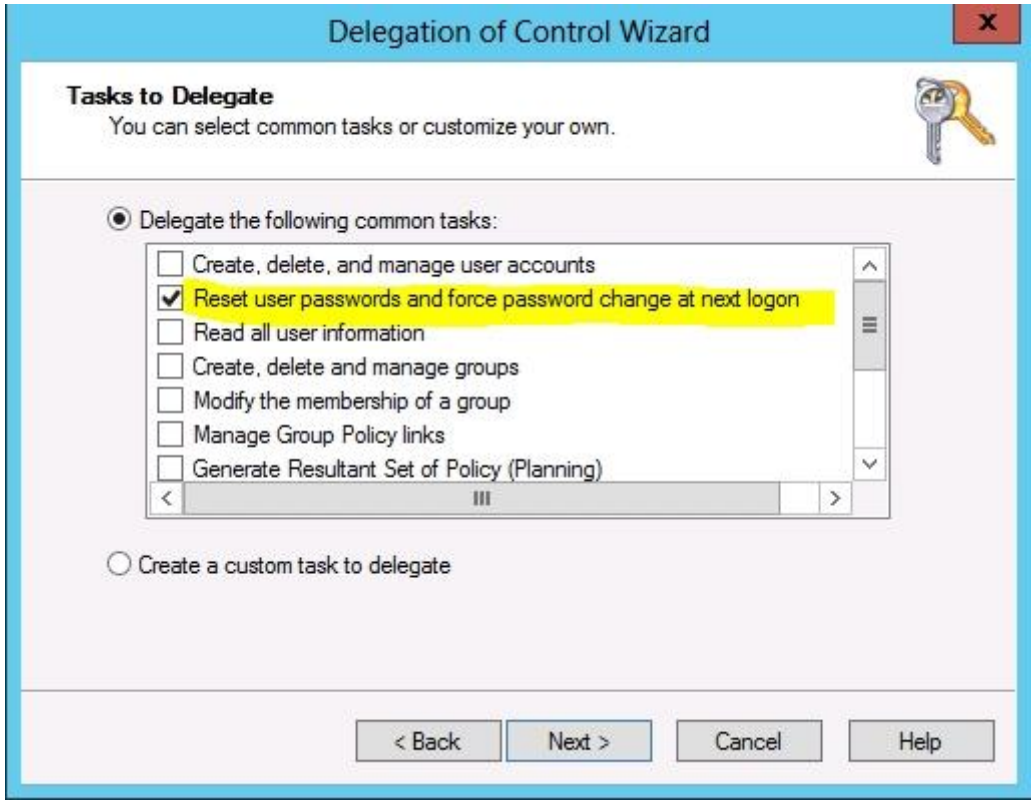
QUESTION 22
Your network contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named IT and a OU named Sales.
All of the help desk user accounts are located in the IT OU. All of the sales user accounts are located in the Sales OU.
The Sales OU contains a global security group named G_Sales. The IT OU contains a global security group named G_HelpDesk.
You need to ensure that members of G_HelpDesk can perform the following tasks:
· Reset the passwords of the sales users.
· Force the sales users to change their password at their next logon.

What should you do?

A. Run the Set-ADFinecrainedPasswordPolicy cmdlet and specify the -identity parameter.
B. Right-click the IT OU and select Delegate Control.
C. Right-click the Sales OU and select Delegate Control.
D. Run the Set-ADAccountPassword cmdlet and specify the -identity parameter.

Correct Answer: C
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
You can use the Delegation of Control Wizard to delegate the Reset Password permission to the delegated user.



http://support.microsoft.com/kb/296999/en-us

QUESTION 23
Your network contains an Active Directory domain named contoso.com. The domain contains 30 organizational units (OUs).
You need to ensure that a user named User1 can link Group Policy Objects (GPOs) in the domain.

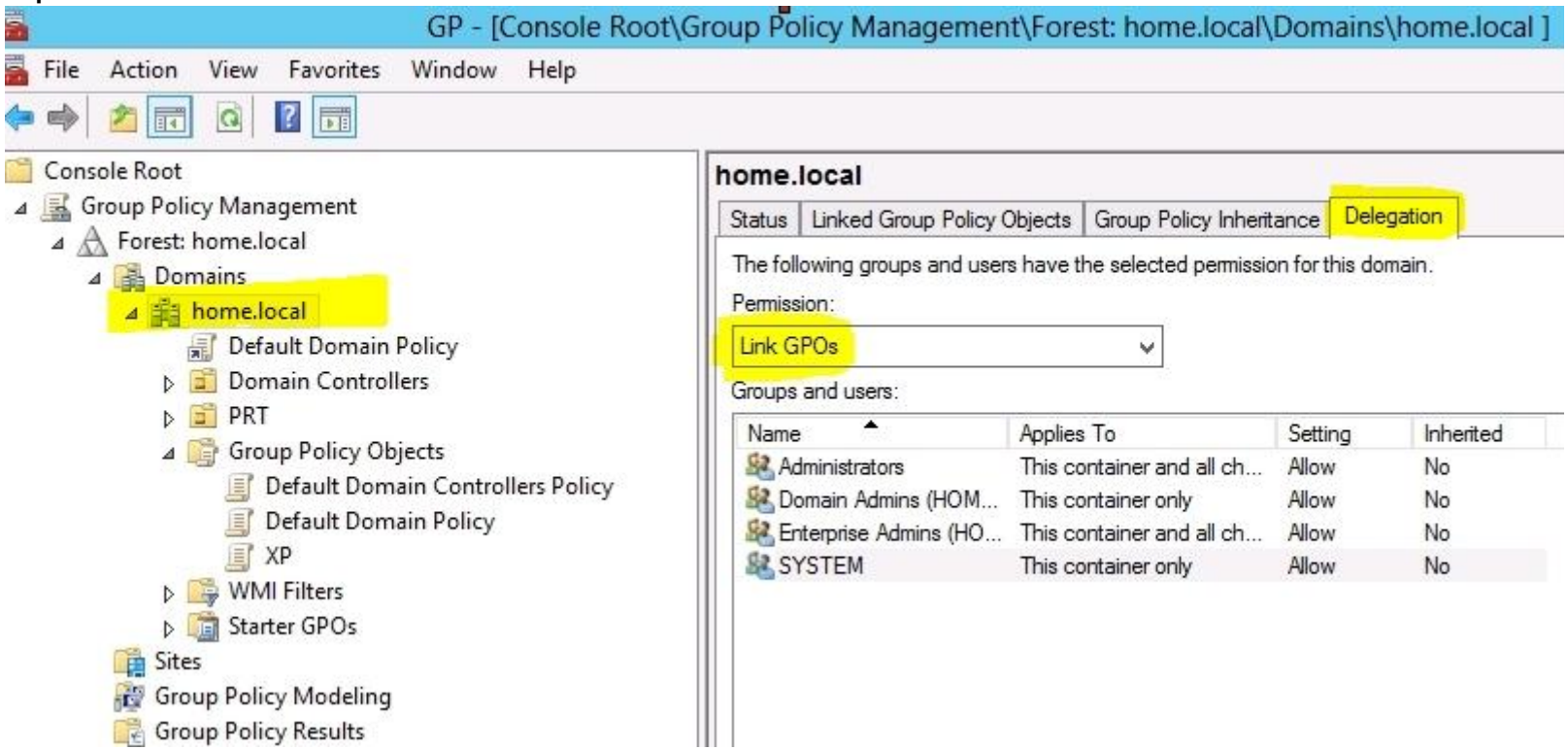
What should you do?

A. From the Active Directory Users and Computers, add User1 to the Network Configuration Operators group.
B. From the Group Policies Management, click the contoso.com node and modify the Delegation settings.
C. From the Group Policies Management, click the Group policy Objects node and modify the Delegation settings.
D. From the Active Directory Users and Computers, add User1 to the Group Policy Creator Owners group.

Correct Answer: B

Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:



http://technet.microsoft.com/en-us/library/cc755086(v=ws.10).aspx

QUESTION 24
DRAG DROP

Your network contains an Active Directory domain named contoso.com. All client computers run Windows 7.

Group Policy objects (GPOs) are linked to the domain as shown in the exhibit. (Click the Exhibit button.)

GP02 contains user configurations only and GP03 contains computer configurations only.

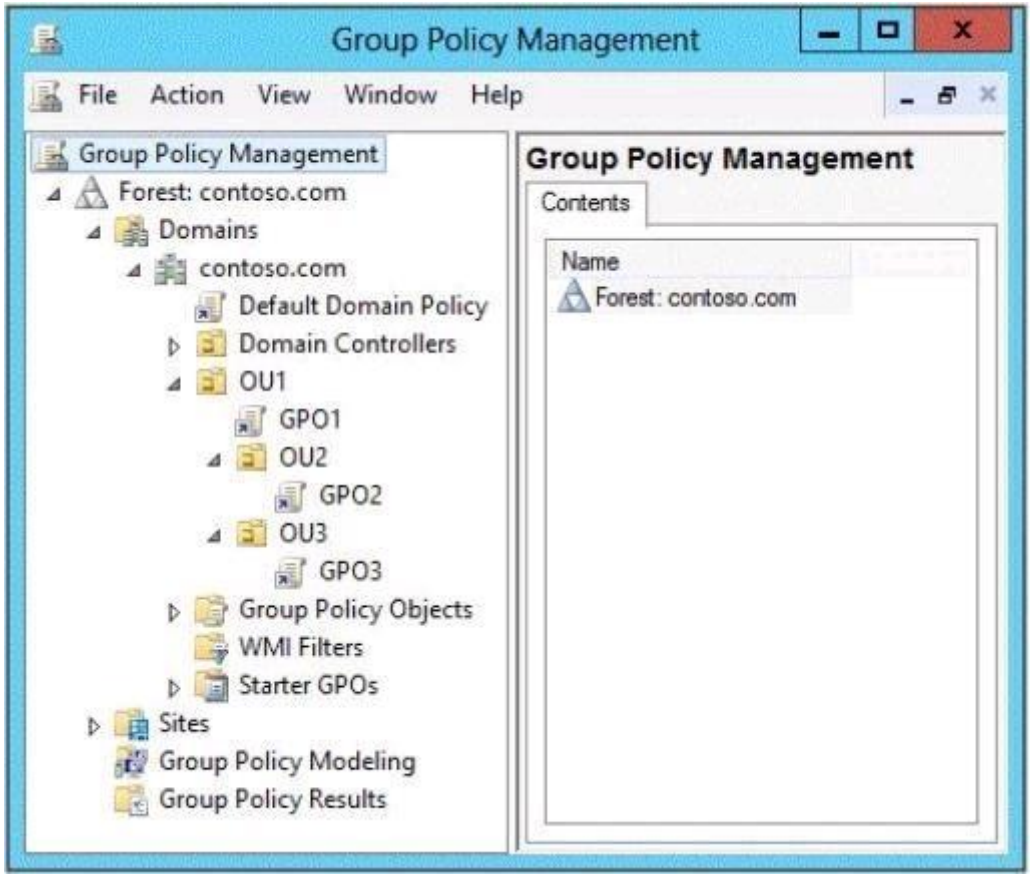
You need to configure the GPOs to meet the following requirements:

- Ensure that GPO2 only applies to the user accounts in OU2 that are members of a global group named Group2.
- Ensure that GPO3 only applies to the computer accounts in OU3 that have more than 100 GB of free disk space.

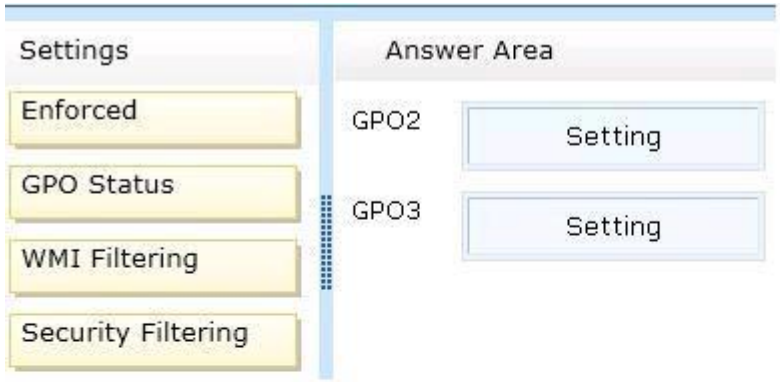
What should you do?

To answer, drag the appropriate setting to the correct GPO. Each setting 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.

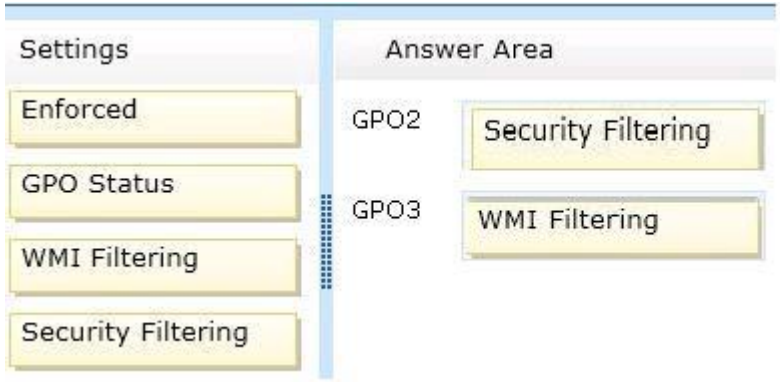
Exhibit:



Select and Place:



Correct Answer:



Section: Configure and Manage Group Policy
Explanation

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

Windows Management Instrumentation (WMI) filters allow you to dynamically determine the scope of Group Policy objects (GPOs) **based on attributes of the target computer.**
When a GPO that is linked to a WMI filter is applied on the target computer, the filter is evaluated on the target computer.
http://technet.microsoft.com/en-us/library/cc779036%28v=ws.10%29.aspx

QUESTION 25
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012. The domain contains 500 client

computers that run Windows 8 Enterprise.

You implement a Group Policy central store.

You have an application named Appl. Appl requires that a custom registry setting be deployed to all of the computers.

You need to deploy the custom registry setting. The solution must minimize administrator effort.

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

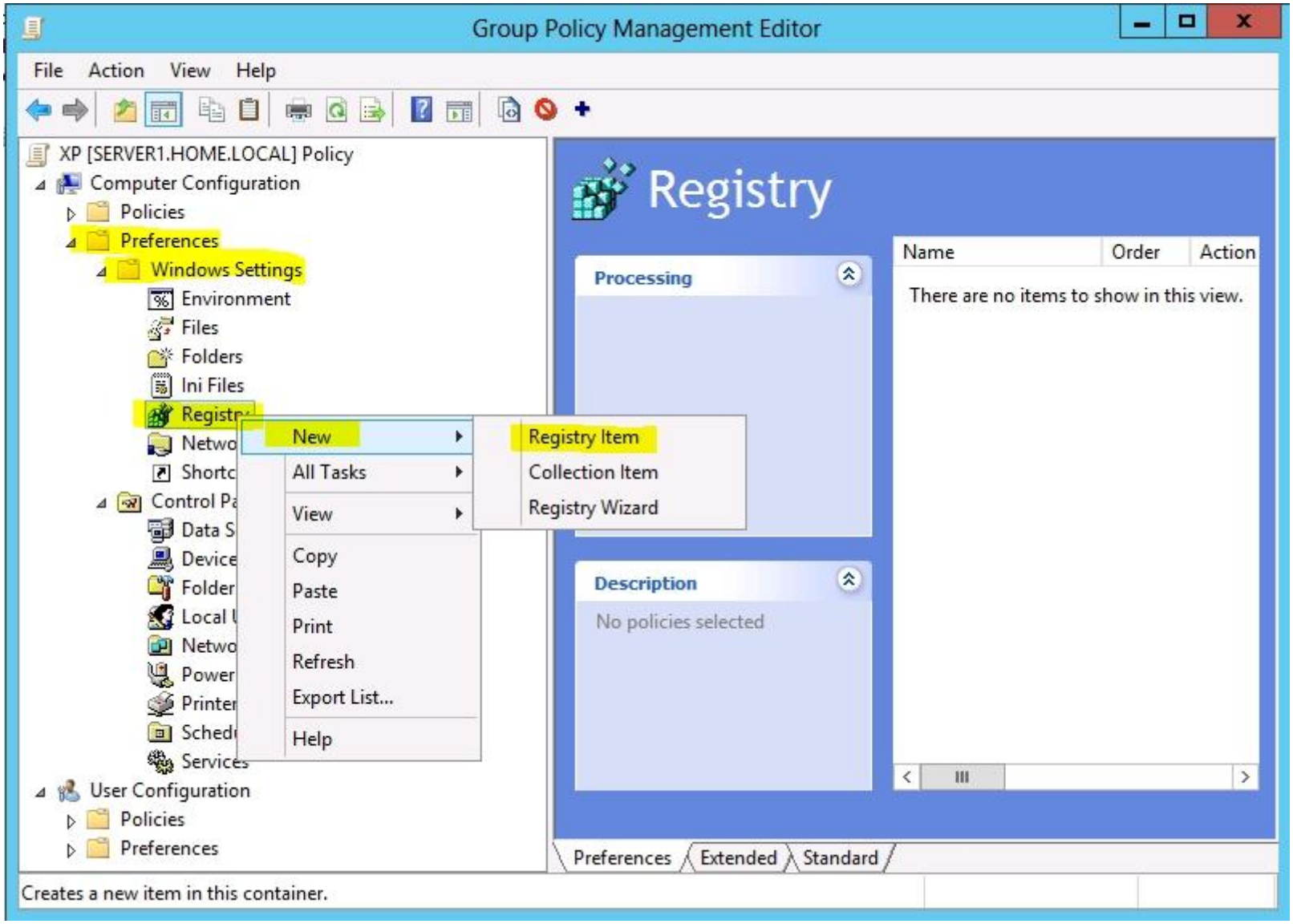
A. The Administrative Templates
B. An application control policy
C. The Group Policy preferences
D. The Software Installation settings

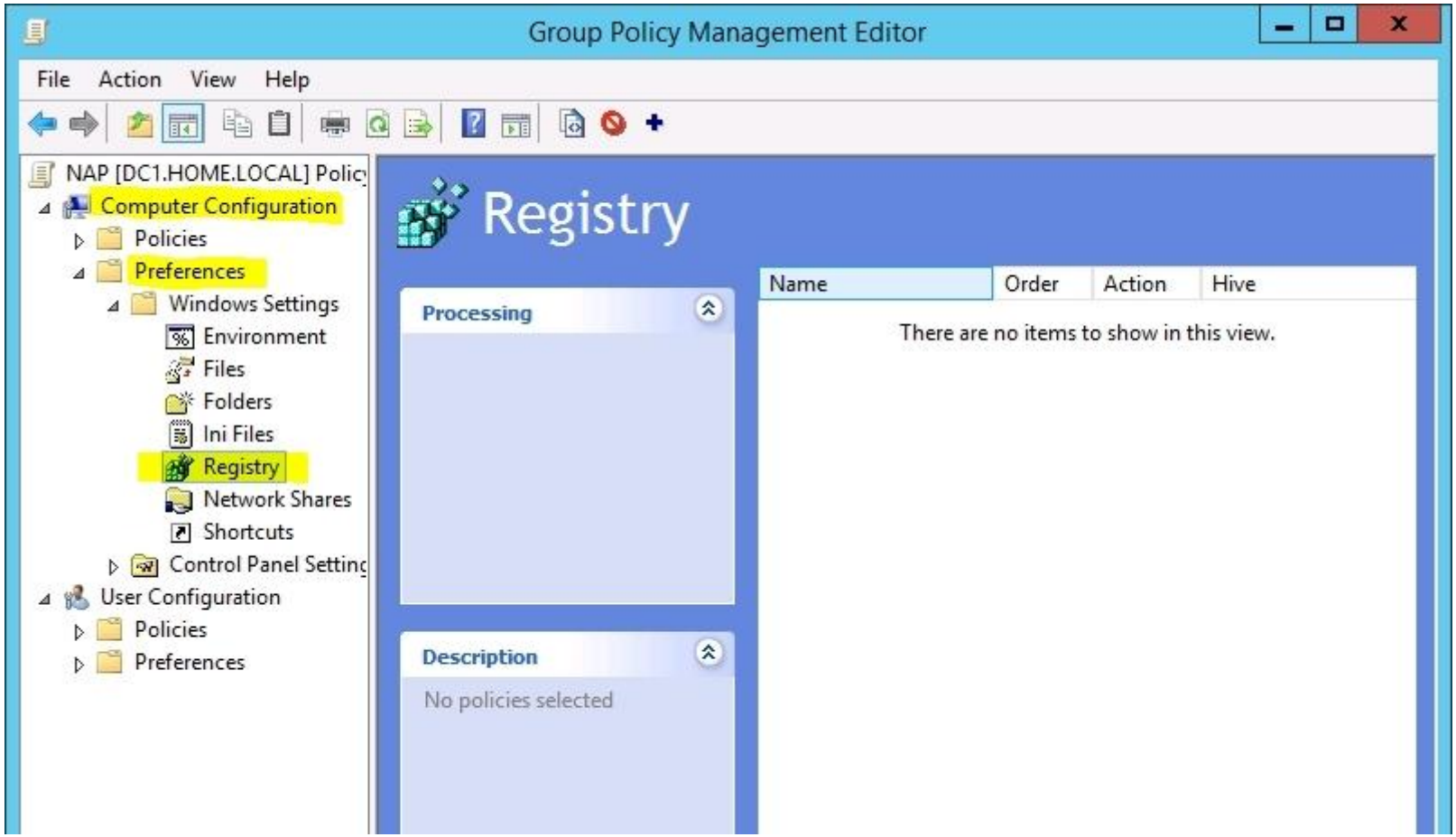
Correct Answer: C
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Group Policy preferences, new for the Windows Server 2008 operating system, include more than 20 new Group Policy extensions that expand the range of configurable settings within a Group Policy object (GPO). These new extensions are included in the Group Policy Management Editor window of the Group Policy Management Console (GPMC), under the new Preferences item. Examples of the new Group Policy preference extensions include folder options, mapped drives, printers, scheduled tasks, services, and Start menu settings.

Group Policy preferences provide better targeting, through item-level targeting and action modes. Additionally, rich user interfaces and standards-based XML configurations provide you with more power and flexibility over managed computers when you administer GPOs.

In addition to providing significantly more coverage, better targeting, and easier management, Group Policy preferences enable you to deploy settings to client computers without restricting the users from changing the settings. This capability provides you with the flexibility to decide which settings to enforce and which settings to not enforce. You can deploy settings that you do not want to enforce by using Group Policy preferences.


Group Policy Management Editor
File
Action
View
Help
XP [SERVER1.HOME.LOCAL] Policy
Computer Configuration
Policies
Preferences
Windows Settings
Environment
Files
Folders
Ini Files
Registry
Netwo
Shortc
Control Pa
Data S
Device
Folder
Local U
Netwo
Power
Printer
Sched
Services
User Configuration
Policies
Preferences
New
All Tasks
View
Copy
Paste
Print
Refresh
Export List...
Help
Registry Item
Collection Item
Registry Wizard
Registry
Processing
Description
No policies selected
Name
Order
Action
There are no items to show in this view.
Preferences
Extended
Standard
Creates a new item in this container.



QUESTION 26

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

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 dcl.contoso.com. You insert the USB flash drive in dcl.contoso.com.

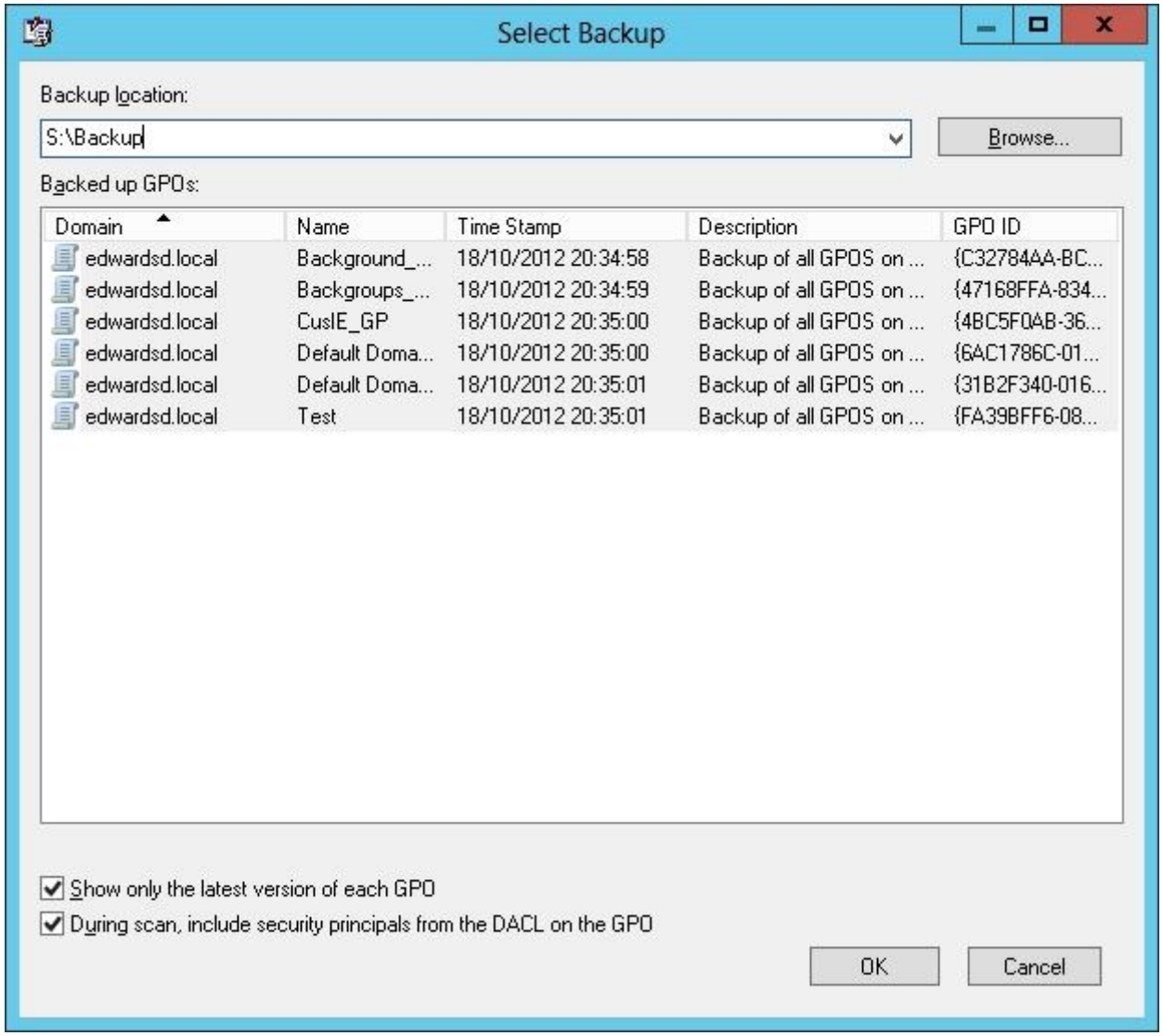
You need to identify the domain-specific reference in GPO1.

What should you do?

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

Correct Answer: D
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
The Migration Table Editor - The Migration Table Editor (MTE) is provided with Group Policy Management Console (GPMC) to facilitate the editing of migration tables.
Migration tables are used for copying or importing Group Policy objects (GPOs) from one domain to another, in cases where the GPOs include domain-specific information that must be updated during copy or import.



http://technet.microsoft.com/en-us/library/cc779961%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc771963.aspx
http://www.edwardsd.co.uk/work/2012/11/migrating-gpos-across-domains-with-gpmc/

QUESTION 27
Your network contains an Active Directory domain named contoso.com. All client computers run Windows Vista Service Pack 2 (SP2).

All client computers are in an organizational unit (OU) named OU1. All user accounts are in an OU named OU2. All users log on to their client computer by using standard user accounts.

A Group Policy object (GPO) named GPO1 is linked to OU1. A GPO named GPO2 is linked to OU2.

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

What should you do?

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

Correct Answer: A
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:

Note

Advanced audit policy settings can also be applied to client computers running Windows Vista. However, the audit policies for these client computers must be created and applied separately by using Auditpol.exe logon scripts.

Applies To: Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, **Windows Vista**
auditpol.exe: the audit policy command-line tool can be used to:

Set and query a system audit policy.
Set and query a per-user audit policy.
Set and query auditing options.
Set and query the security descriptor used to delegate access to an audit policy.
Report or back up an audit policy to a comma-separated value (CSV) text file.
Load an audit policy from a CSV text file.
Configure global resource SACLs.

http://technet.microsoft.com/en-us/library/dd692792%28v=ws.10%29.aspx

http://technet.microsoft.com/en-us/library/cc755264%28v=ws.10%29.aspx
http://technet.microsoft.com/pt-pt/library/dd408940%28v=ws.10%29.aspx
http://support.microsoft.com/kb/921469/en-us

QUESTION 28
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

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

You make a change to GPO1.

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

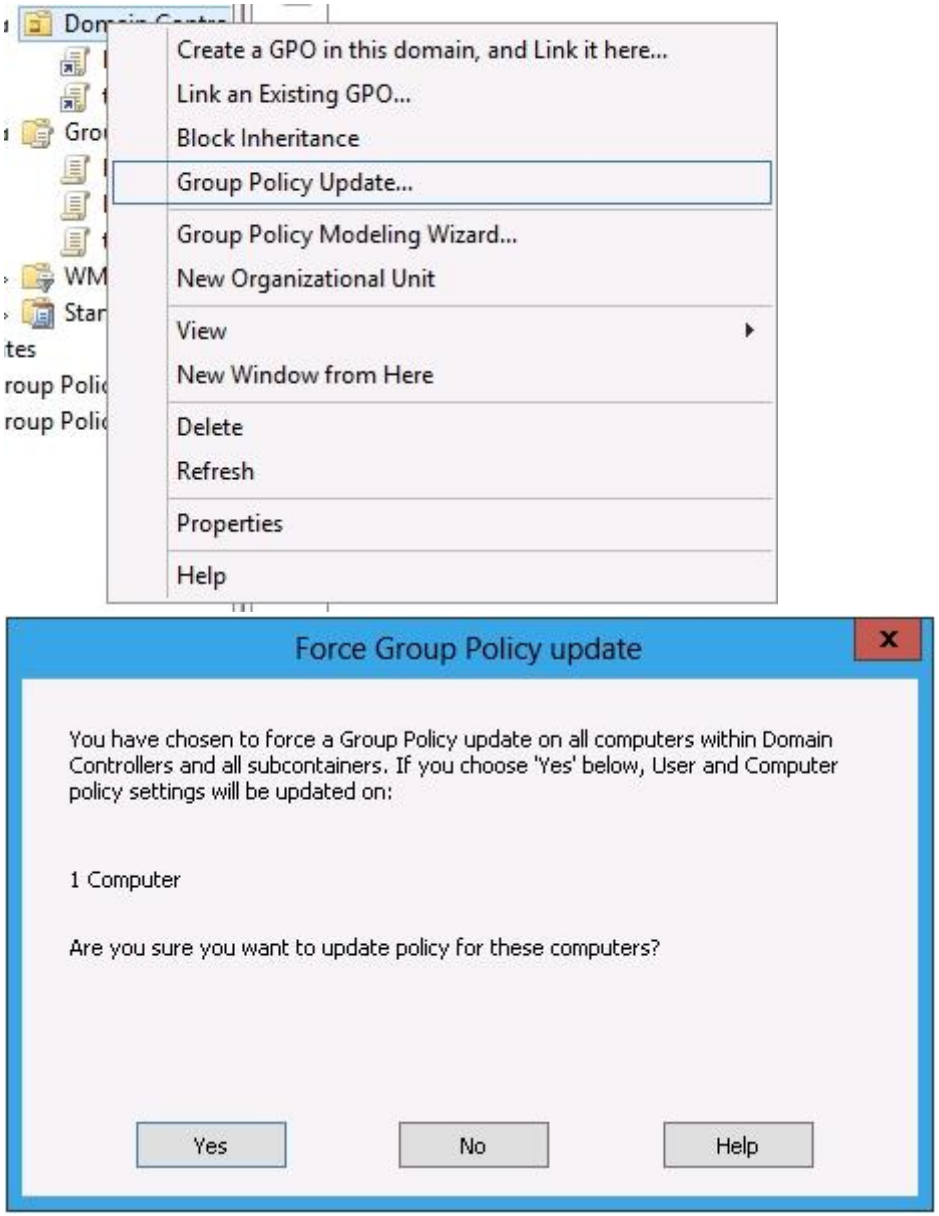
The solution must minimize administrative effort.

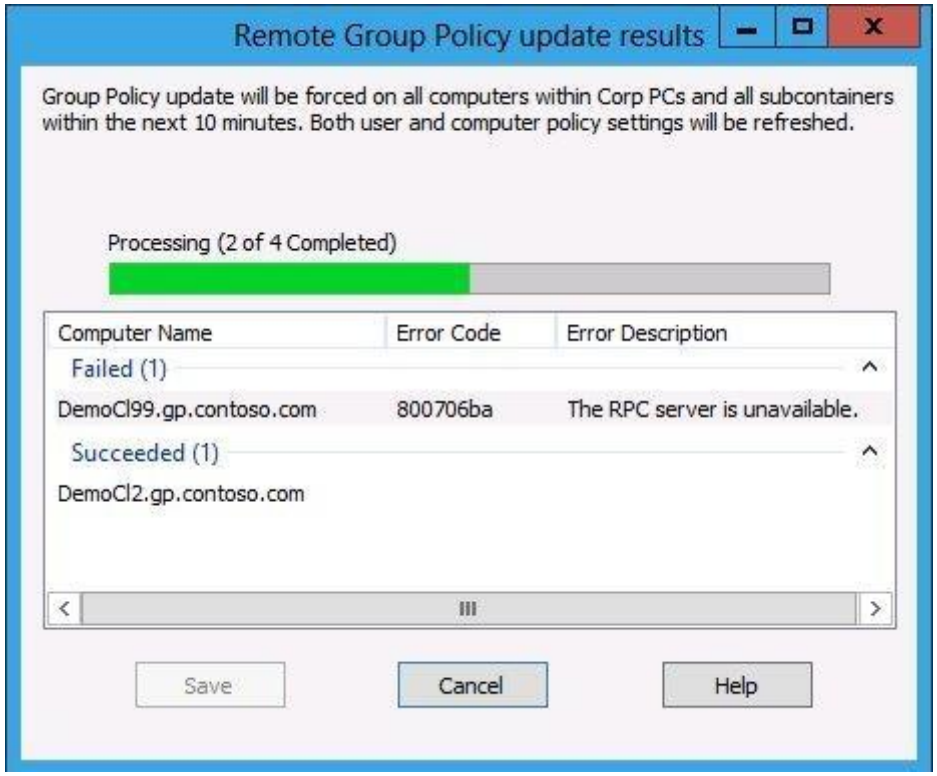
Which tool should you use?

A. Group Policy Object Editor
B. The Secedit command
C. Group Policy Management Console (GPMC)
D. Active Directory Users and Computers

Correct Answer: C
Section: Configure and Manage Group Policy
Explanation

Explanation/Reference:
Explanation: In the previous versions of Windows, this was accomplished by having the user run GPUpdate.exe on their computer.
Starting with Windows Server® 2012 and Windows® 8, you can now remotely refresh Group Policy settings for all computers in an OU from one central location through the **Group Policy Management Console (GPMC)**. Or you can use the **Invoke-GPUpdate cmdlet** to refresh Group Policy for a set of computers, not limited to the OU structure, for example, if the computers are located in the default computers container.


Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Update...
Group Policy Modeling Wizard...
New Organizational Unit
View
New Window from Here
Delete
Refresh
Properties
Help
Force Group Policy update
You have chosen to force a Group Policy update on all computers within Domain Controllers and all subcontainers. If you choose 'Yes' below, User and Computer policy settings will be updated on:
1 Computer
Are you sure you want to update policy for these computers?
Yes
No
Help



Incorrect:
Not B: Secedit configures and analyzes system security by comparing your current configuration to at least one template.

http://technet.microsoft.com/en-us//library/jj134201.aspx
http://blogs.technet.com/b/grouppolicy/archive/2012/11/27/group-policy-in-windows-server-2012-using-remote-gpupdate.aspx

QUESTION 29
Your network contains an Active Directory domain named contoso.com. The domain contains a Web server named www.contoso.com.
The Web server is available on the Internet. You implement DirectAccess by using the default configuration.
You need to ensure that users never attempt to connect to www.contoso.com by using DirectAccess.
The solution must not prevent the users from using DirectAccess to access other resources in contoso.com.

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

A. Name Resolution Policy
B. DNS Client

C. Network Connections
D. DirectAccess Client Experience Settings

Correct Answer: A
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
When an application on a Direct Access client attempts to resolve a name, it first compares the name with the rules in the NRPT (Name Resolution Policy Table)
If there are no matches, the Direct Access client uses Internet DNS servers to resolve the name

For DirectAccess, the NRPT must be configured with the namespaces of your intranet with a leading dot (for example, .internal.contoso.com or .corp.contoso.com).
For a DirectAccess client, any name request that matches one of these namespaces will be sent to the specified intranet Domain Name System (DNS) servers.
Include all intranet DNS namespaces that you want DirectAccess client computers to access.
There are no command line methods for configuring NRPT rules. You must use Group Policy settings. To configure the NRPT through Group Policy, use the Group Policy add-in at **Computer Configuration\Policies\Windows Settings\Name Resolution Policy** in the Group Policy object for DirectAccess clients. You can create a new NRPT rule and edit or delete existing rules. For more information, see Configure the NRPT with Group Policy.

The NRPT contains rules configured by an administrator for either names or namespaces and the settings for the required special handling. When performing a DNS name resolution, the DNS Client service compares the requested name against each rule in the NRPT before sending a DNS name query. Queries and responses that match an NRPT rule get the specified special handling applied. Queries and responses that do not match an NRPT rule are processed normally; that is, the DNS Client service sends the name queries to interface-configured DNS servers.
To minimize the number of NRPT rules, you want to specify namespaces that encompass as much of the relevant namespace as possible. However, you also might need to specify that individual names or namespaces within those namespaces be exempted from special handling. For these cases, you must configure an NRPT exemption.
An NRPT exemption is a rule that specifies no special handling.

Group Policy Management Editor

File Action View Help

- Default Domain Policy [SERVER
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution
        - Scripts (Startup/S
        - Security Settings
        - Policy-based QoS
      - Administrative Temp
    - Preferences
      - Windows Settings
        - Environment
        - Files
        - Folders
        - Ini Files
        - Registry
        - Network Shares
        - Shortcuts
      - Control Panel Setting
  - User Configuration
    - Policies
    - Preferences

Name Resolution Policy

Overview

The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and DirectAccess on DNS client computers. You can use this page to create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (OU).

Learn more about DNSSEC on the Web

Description

Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).

Create Rules

To which part of the namespace does this rule apply?

Suffix

Certification authority: (Optional)

Browse...

DNSSEC | DNS Settings for DirectAccess | Generic DNS Server | Encoding

Enable DNSSEC in this rule

DNSSEC settings

Validation:

Require DNS clients to check that name and address data has been validated by the DNS server

IPsec:

Use IPsec in communication between the DNS client and DNS server

Encryption type: No encryption (integrity only)

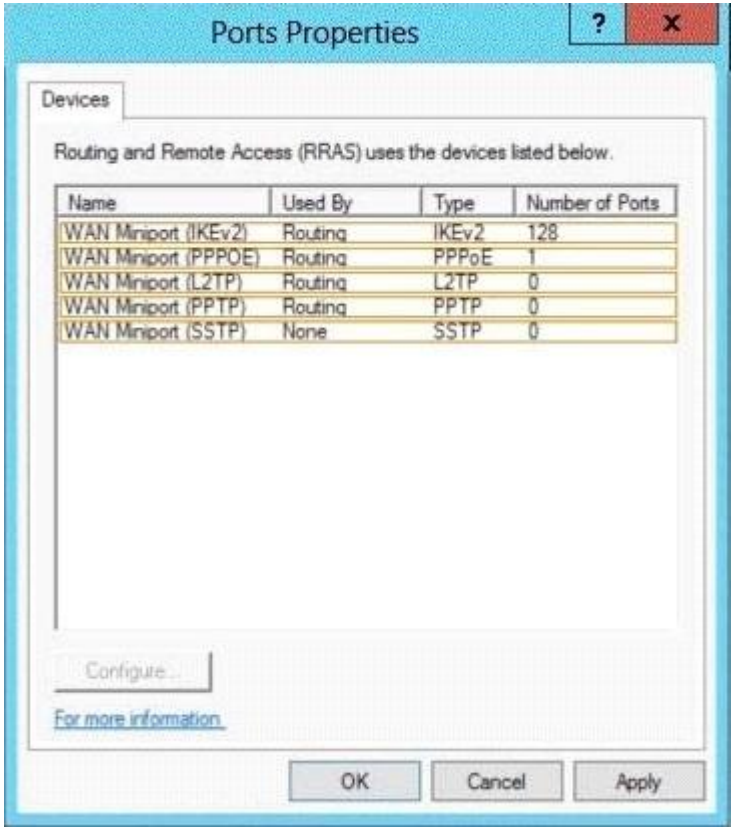
Update Create Clear

http://blogs.technet.com/b/meamcs/archive/2012/05/03/windows-server-2012-direct-access-part-1-what-s-new.aspx
http://technet.microsoft.com/en-us/magazine/ff394369.aspx

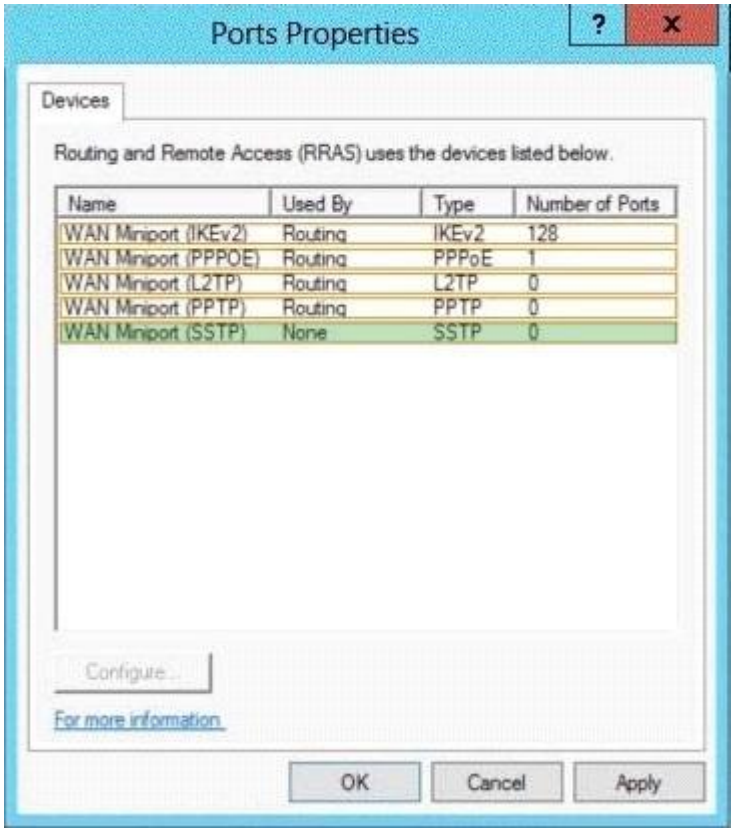
QUESTION 30
You have a server named Server1 that runs Windows Server 2012. Server1 has the Remote Access server role installed.
You need to configure the ports on Server1 to ensure that client computers can establish VPN connections to Server1 by using TCP port 443.

What should you modify? To answer, select the appropriate object in the answer area.

Hot Area:



Correct Answer:



Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
SSTP

Secure socket tunneling protocol, also referred to as SSTP, is by definition an application-layer protocol. It is designed to employ a synchronous communication in a back and forth motion between two programs. It allows many application endpoints over one network connection, between peer nodes, thereby enabling efficient usage of the communication resources that are available to that network.

SSTP protocol is based on SSL instead of PPTP or IPSec and uses TCP Port 443 for relaying SSTP traffic. Although it is closely related to SSL, a direct comparison can not be made between SSL and SSTP as SSTP is only a tunneling protocol unlike SSL. Many reasons exist for choosing SSL and not IPSec as the basis for SSTP. IPSec is directed at supporting site- to-site VPN connectivity and thus SSL was a better base for SSTP development, as it supports roaming. Other

reasons for not basing it on IPSec are:

It does not force strong authentication,
User clients are a must have,
Differences exist in the quality and coding of user clients from vendor to vendor,
Non-IP protocols are not supported by default,
Because IPSec was developed for site to site secure connections, it is likely to present problems for remote users attempting to connect from a location with a limited number of IP addresses.

To allow SSTP (Secure Socket Tunneling Protocol) traffic, configure the network firewall to open TCP port 443.
Verify that the Routing and Remote Access server has sufficient ports configured for remote access. By default, 128 ports are available for this device.

http://support.microsoft.com/kb/947032/en-us
http://support.microsoft.com/kb/947031/en-us
http://blogs.technet.com/b/rrasblog/archive/2006/06/14/which-ports-to-unblock-for-vpn-traffic-to-pass-through.aspx

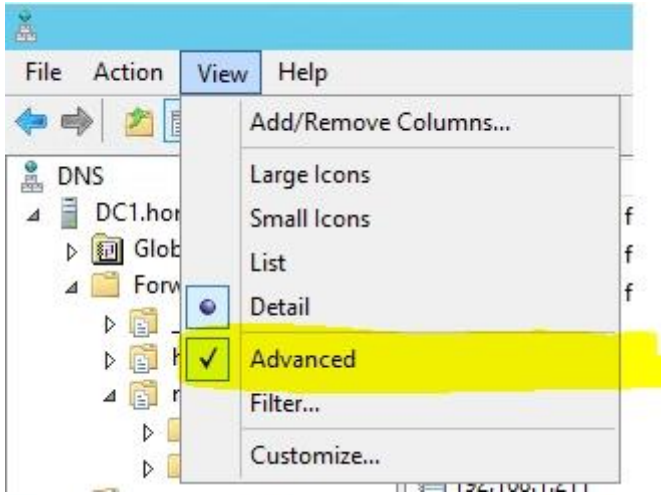
QUESTION 31
You have a DNS server named Server1. Server1 has a primary zone named contoso.com. Zone Aging/Scavenging is configured for the contoso.com zone.
One month ago, an Administrator removed a server named Server2 from the network. You discover that a static resource record for Server2 is present 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 Security settings of the static resource records
B. The Expires after value of contoso.com
C. The Record time stamp value of the static resource records
D. The time-to-live (TTL) value of the static resource records

Correct Answer: C
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
The DNS Server service supports aging and scavenging features. These features are provided as a mechanism for performing cleanup and removal of stale resource records, which can accumulate in zone data over time.
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

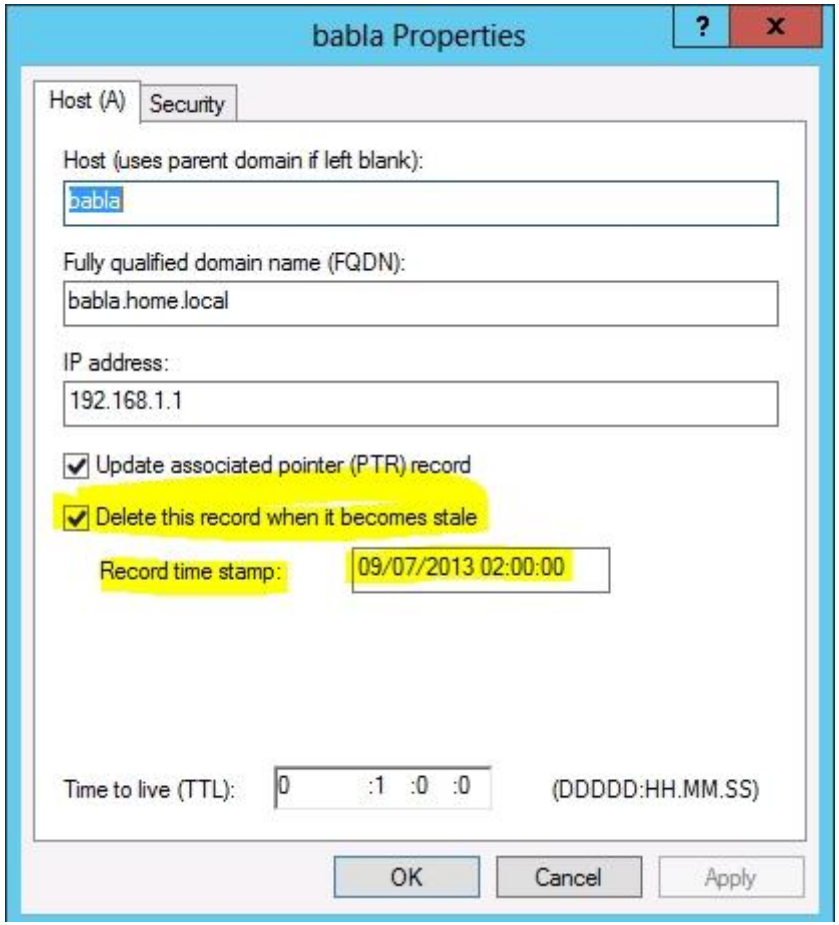


Depending on the how the resource record was originally added to the zone, do one of the following:

- 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 durin
  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.

Time stamping - For RRs that you add manually, a time stamp value of zero is used, indicating that they are not affected by the aging process and can remain without limitation in zone data unless you otherwise change their time stamp or delete them.



http://technet.microsoft.com/en-us/library/cc759204%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc771570.aspx

QUESTION 32

Your network contains two Active Directory domains named contoso.com and adatum.com. The network contains a server named Server1 that runs Windows Server 2012.

Server1 has the DNS Server server role installed. Server1 has a copy of the contoso.com DNS zone.

You need to configure Server1 to resolve names in the adatum.com domain.

The solution must meet the following requirements:

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

· Minimize Administrative effort.

VCEplus.com

Which type of zone should you create?

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

Correct Answer: D
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Stub zone

A stub zone is a copy of a zone that contains only those resource records that are necessary to identify the authoritative Domain Name System (DNS) servers for that zone. Typically, you use a stub zone to resolve names between separate DNS namespaces.

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

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

You can use stub zones to:

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

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

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

There are two lists of DNS servers involved in the loading and maintenance of a stub zone:

The list of master servers from which the DNS server loads and updates a stub zone. A master server may be a primary or secondary DNS server for the zone. In both cases, it will have a complete list of the DNS servers for the zone.

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

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

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

QUESTION 33
Your network contains two servers named Server1 and Server2. Both servers run Windows Server 2012 and have the DNS Server server role installed.
On Server1, you create a standard primary zone named contoso.com.
You need to ensure that Server2 can host a secondary zone for contoso.com.

What should you do from Server1?

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

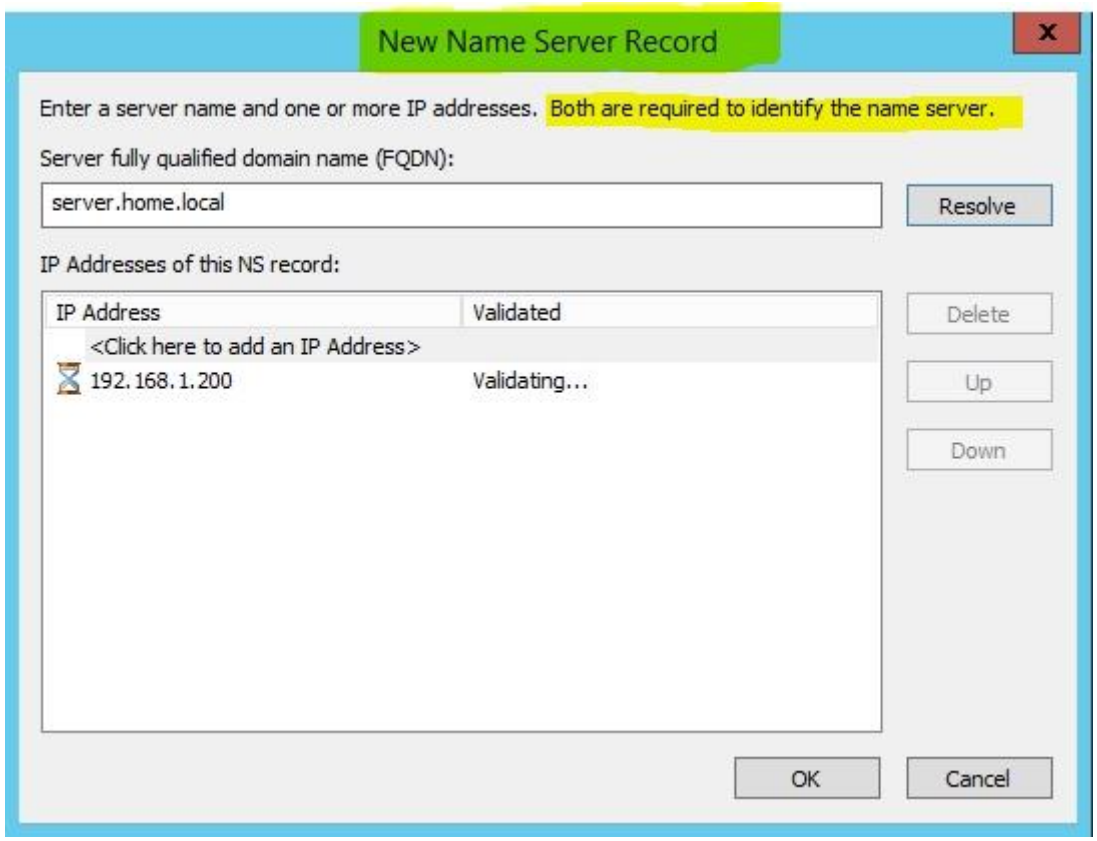
Correct Answer: A
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
DNS records are partitioned into zones, a zone contains resource records for the hosts that belong to the corresponding portion of the DNS namespace. The namespace for a zone can include one or multiple DNS domains. Zones are maintained by DNS servers, a zone can be stored as a file or within Active Directory. You may want to delegate a portion of the DNS namespace for a couple of reasons: in order to assign management to a department within the organization or to improve performance by spreading the load of a large DNS database across separate DNS servers.
Secondary zones cannot be AD-integrated under any circumstances.

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

Secondary Domain Name System (DNS) servers help provide load balancing and fault tolerance. **Secondary DNS servers maintain a read-only copy of zone**

data that is transferred periodically from the primary DNS server for the zone. You can configure DNS clients to query secondary DNS servers instead of (or in addition to) the primary DNS server for a zone, reducing demand on the primary server and ensuring that DNS queries for the zone will be answered even if the primary server is not available.



http://technet.microsoft.com/en-us/library/cc816885%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc816814%28v=ws.10%29.aspx
http://blog.hyperexpert.com/how-to-configure-a-secondary-dns-server-in-windows-server-2012/
http://technet.microsoft.com/en-us/library/cc770984.aspx

QUESTION 34
You have a server named Server1 that runs Windows Server 2012. Server1 has the Remote Access server role installed.
On Server1, you create a network policy named Policy1.
You need to configure Policy1 to apply only to VPN connections that use the L2TP protocol.

What should you configure in Policy1?

VCEplus.com

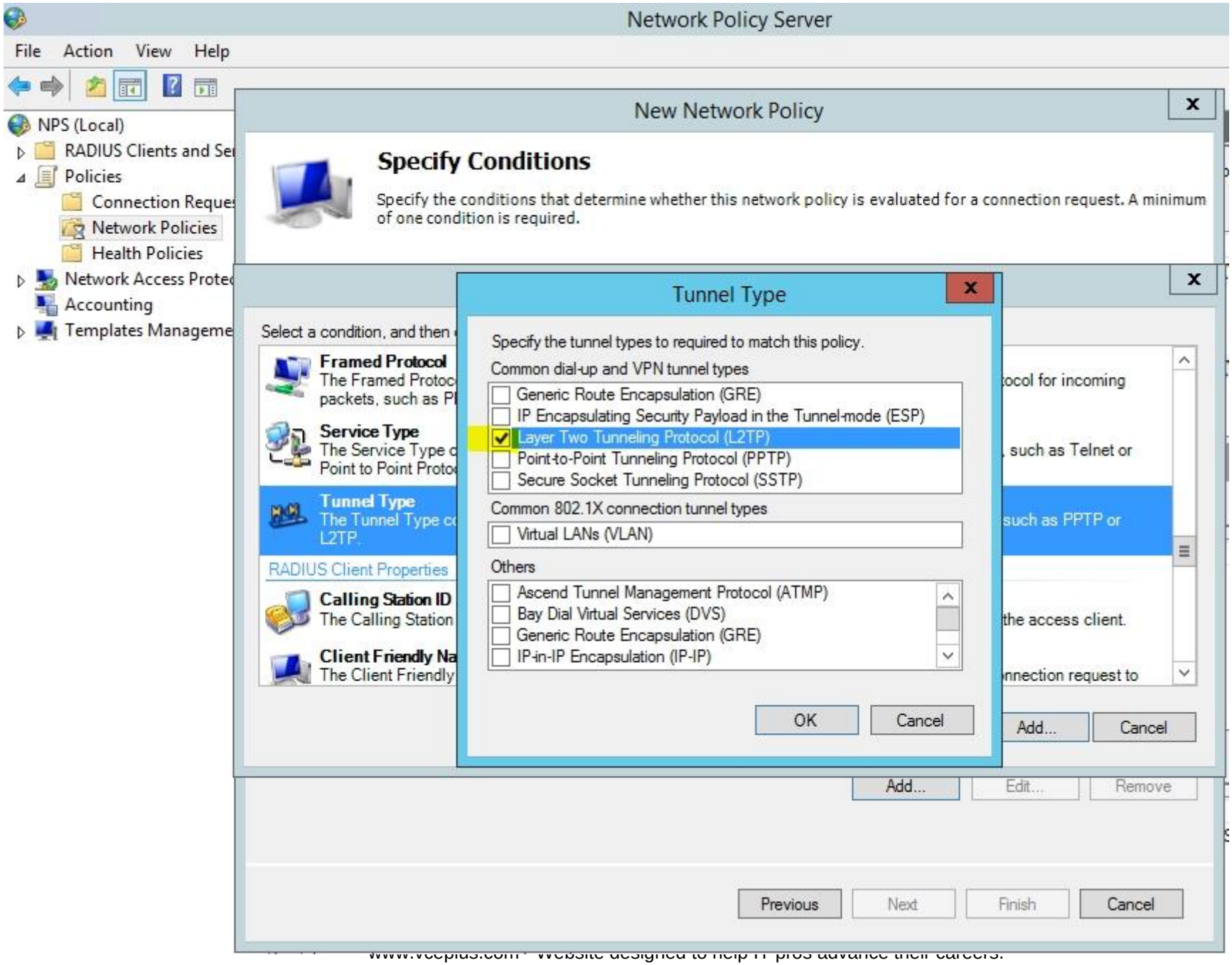
A. The Tunnel Type
B. The Service Type
C. The NAS Port Type
D. The Framed Protocol

Correct Answer: A
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Network Policy Server (NPS) uses network policies, formerly named remote access policies, and the dial-in properties of user accounts to determine whether a connection request should be authorized to connect to the network.
You can use this procedure to configure a new network policy in either the NPS snap-in or the Routing and Remote Access Service snap-in.

Tunnel Type
Restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP. The Tunnel Type attribute is typically used when you deploy virtual local area networks (VLANs).

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



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

http://technet.microsoft.com/en-us/library/cc755309%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc754422%28v=ws.10%29.aspx

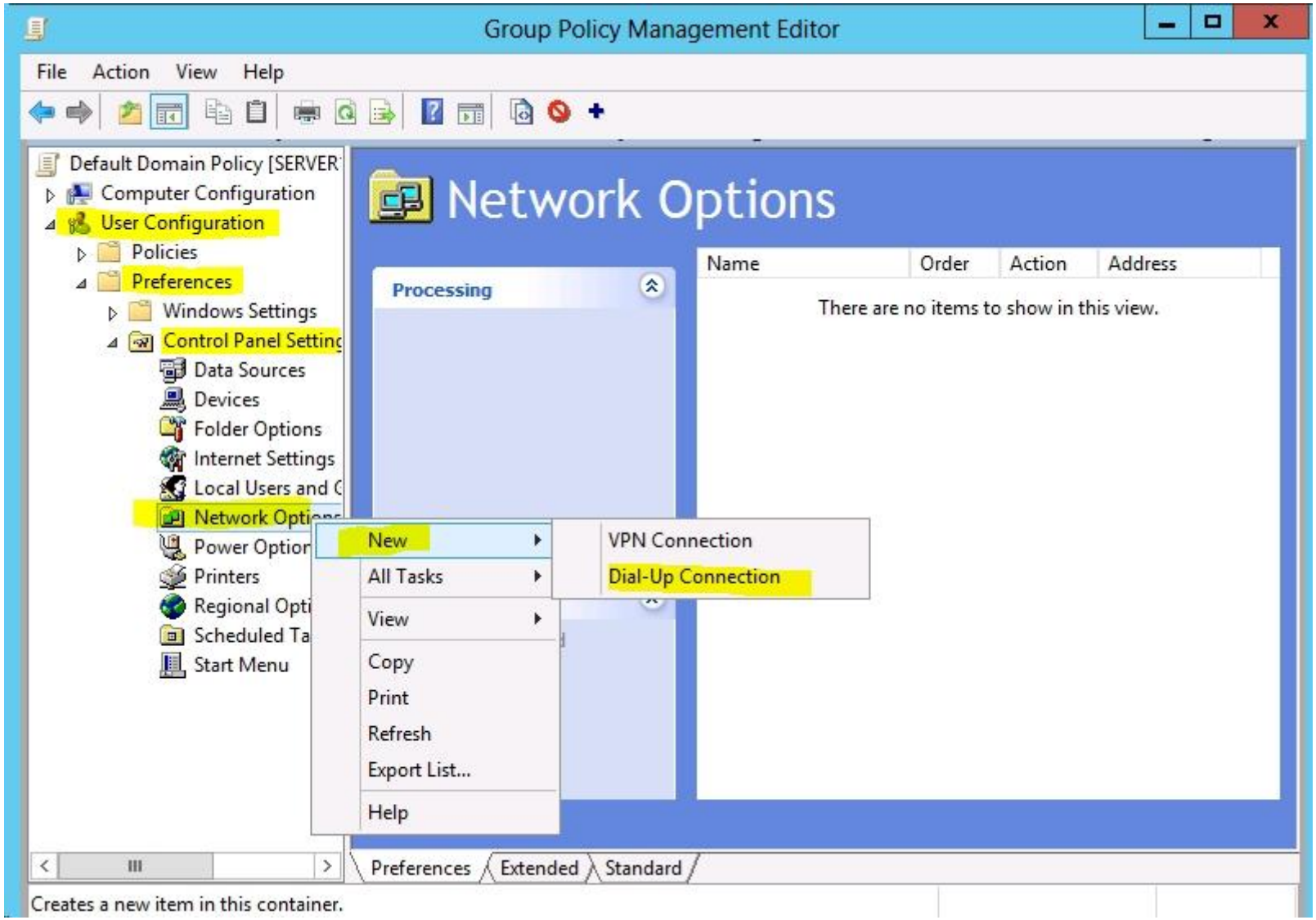
QUESTION 35
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012. All sales users have laptop computers that run Windows 8.
The sales computers are joined to the domain. All user accounts for the sales department are in an organizational unit (OU) named 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. Policies/Administrative Templates/Windows Components/Windows Mobility Center
C. Preferences/Control Panel Settings/Network Options
D. Policies/Administrative Templates/Network/Network Connections

Correct Answer: C
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:



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.

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

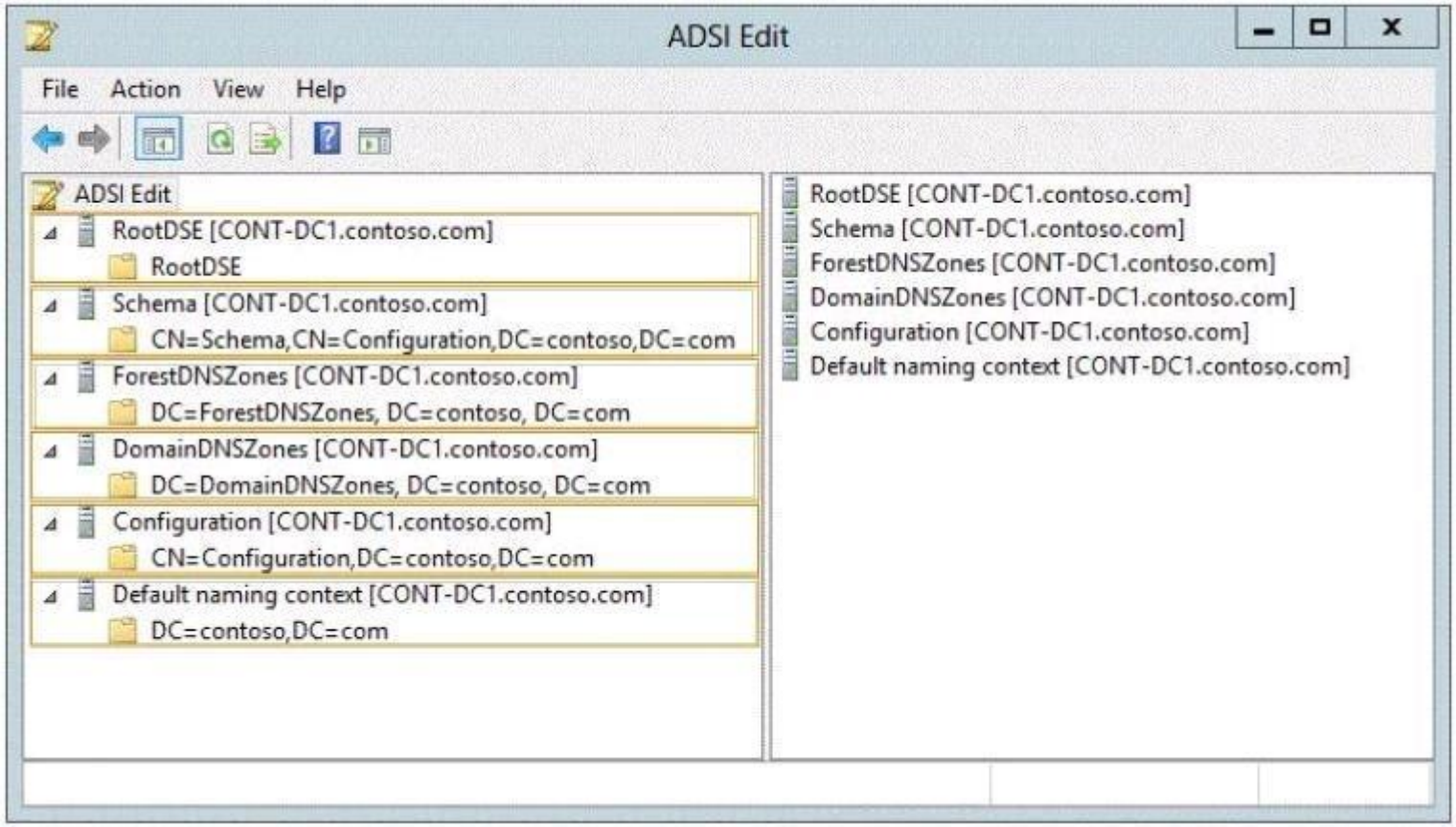
QUESTION 36
HOTSPOT

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012 and are configured as DNS servers. All DNS zones are Active Directory-integrated. Active Directory Recycle Bin is enabled.

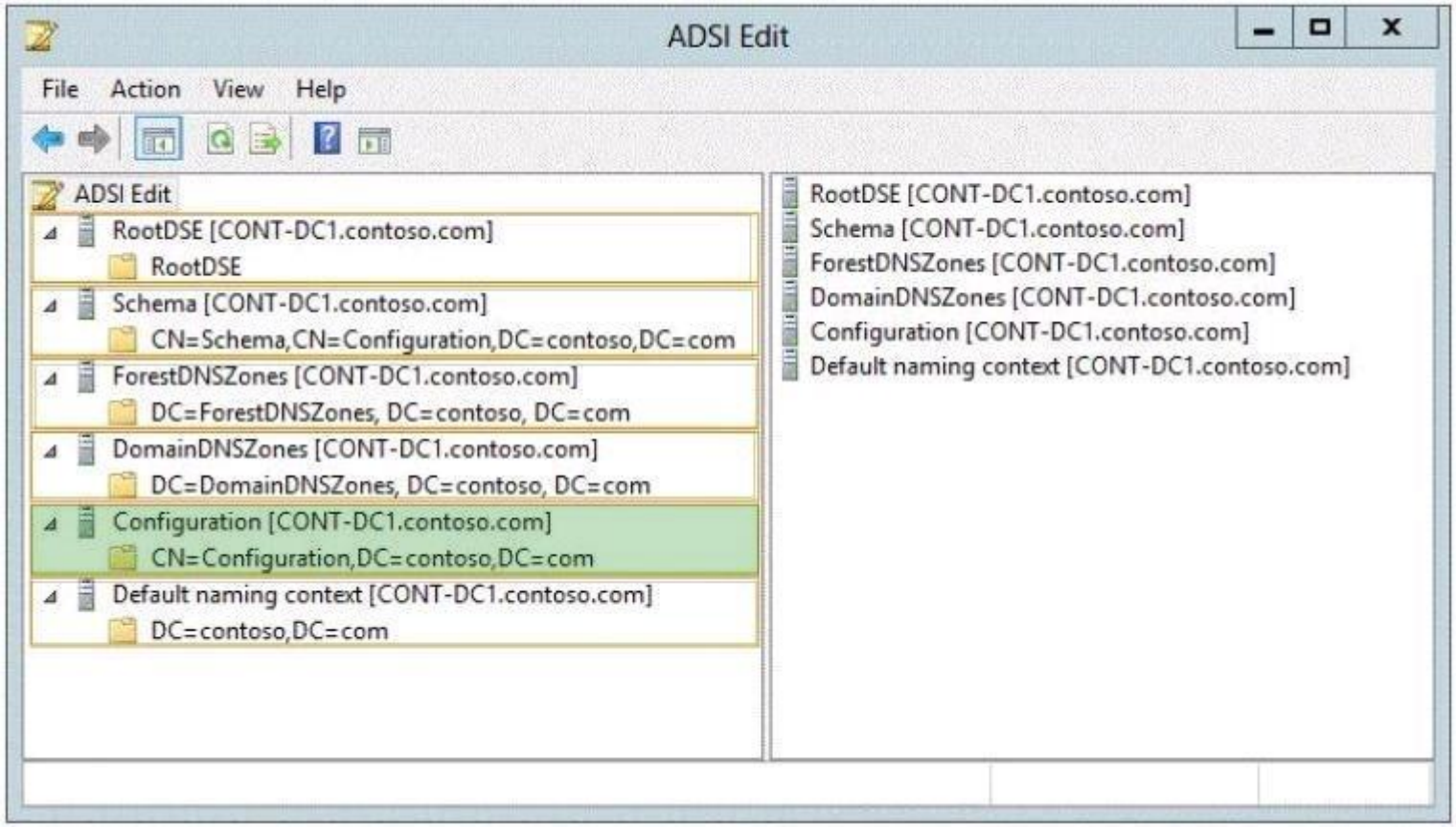
You need to modify the amount of time deleted objects are retained in the Active Directory Recycle Bin.
Which naming context should you use?

To answer, select the appropriate naming context in the answer area.

Hot Area:



Correct Answer:



Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Starting in Windows Server 2008 R2, Active Directory now implements a true recycle bin. No longer will you need an authoritative restore to recover deleted users, groups, OU's, or other objects. Instead, it is now possible to use PowerShell commands to bring back objects with all their attributes, backlinks, group memberships, and metadata.

The amount of time that an object can be recovered is controlled by the Deleted Object Lifetime (DOL). This time range can be set on the msDS-deletedObjectLifetime attribute. By default, it will be the same number of days as the Tombstone Lifetime (TSL). The TSL set for a new forest since Windows Server 2003 SP1 has been 180 days*, and since by default DOL = TSL, the default number of days that an object can be restored is therefore 180 days. If tombstoneLifetime is NOT SET or NULL, the tombstone lifetime is that of the Windows default: 60 days. This is all configurable by the administrator.

```
Administrator: Windows PowerShell
PS C:\> Set-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=contoso,dc=com" -Part
ition "CN=Configuration,DC=contoso,dc=com" -Replace:@{"msDS-DeletedObjectLifetime" = 365}
PS C:\>
```

msDS-deletedObjectLifetime
New to Windows Server 2008 R2
Is set on the “CN=Directory Service,CN=Windows NT, CN=Services, **CN=Configuration**, DC=COMPANY,DC=COM” container
Describes how long a deleted object will be restorable

To modify the deleted object lifetime by using Ldp.exe

To open Ldp.exe, click Start, click Run, and then type ldp.exe.

To connect and bind to the server hosting the forest root domain of your Active Directory environment, under Connections, click Connect, and then click Bind.

In the console tree, right-click the CN=Directory Service,CN=Windows NT,CN=Services,**CN=Configuration container**, and then click Modify.

In the Modify dialog box, in Edit Entry Attribute, type msDS-DeletedObjectLifeTime.

In the Modify dialog box, in Values, type the number of days that you want to set for the tombstone lifetime value. (The minimum is 3 days.)

In the Modify dialog box, under Operation click Replace, click Enter, and then click Run.

http://technet.microsoft.com/en-us/library/dd392260%28v=ws.10%29.aspx
http://blogs.technet.com/b/askds/archive/2009/08/27/the-ad-recycle-bin-understanding-implementing-best-practices-and-troubleshooting.aspx

QUESTION 37
Your network contains an Active Directory domain named contoso.com.
You have a standard primary zone names 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.

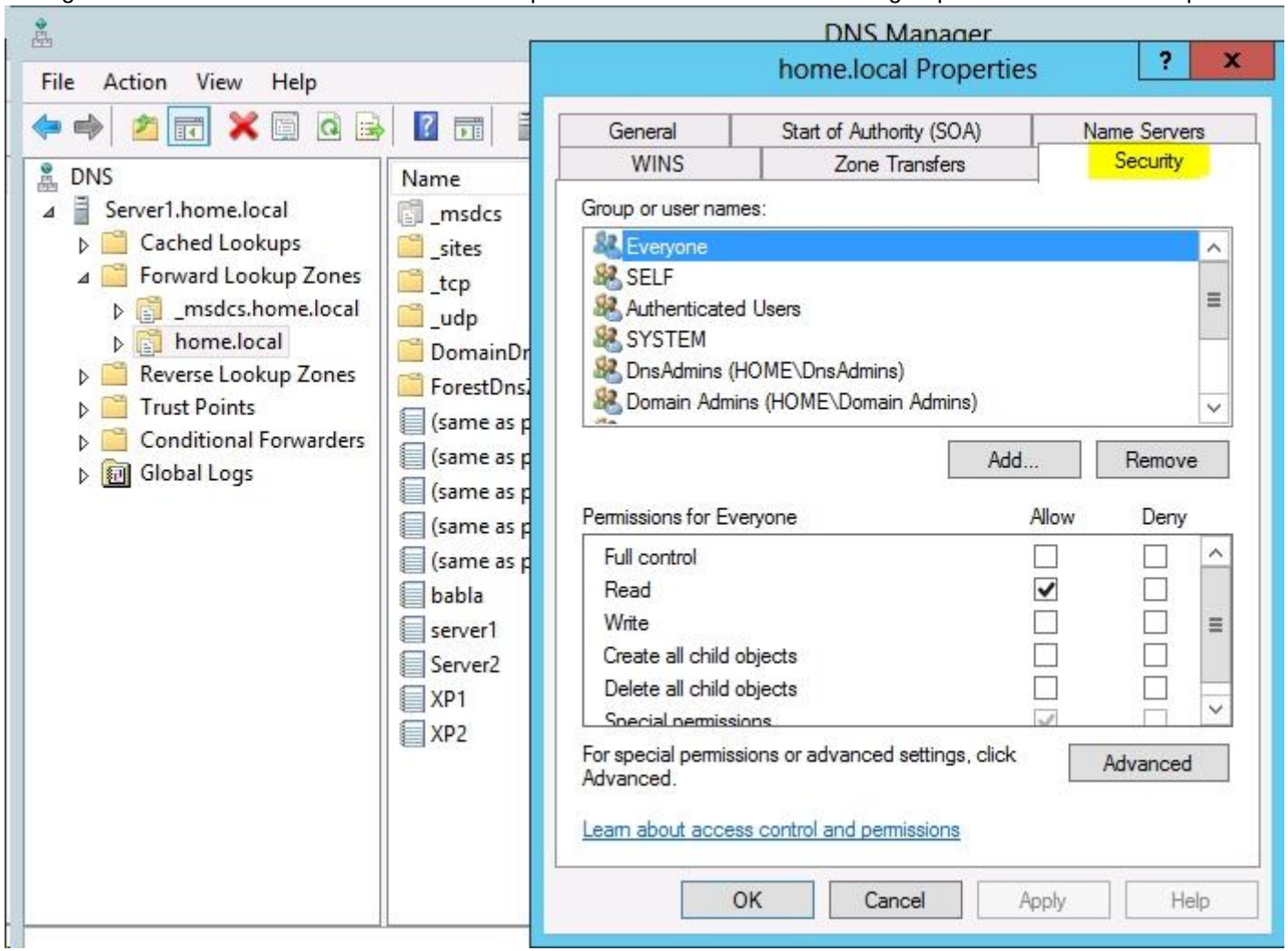
What should you do first?

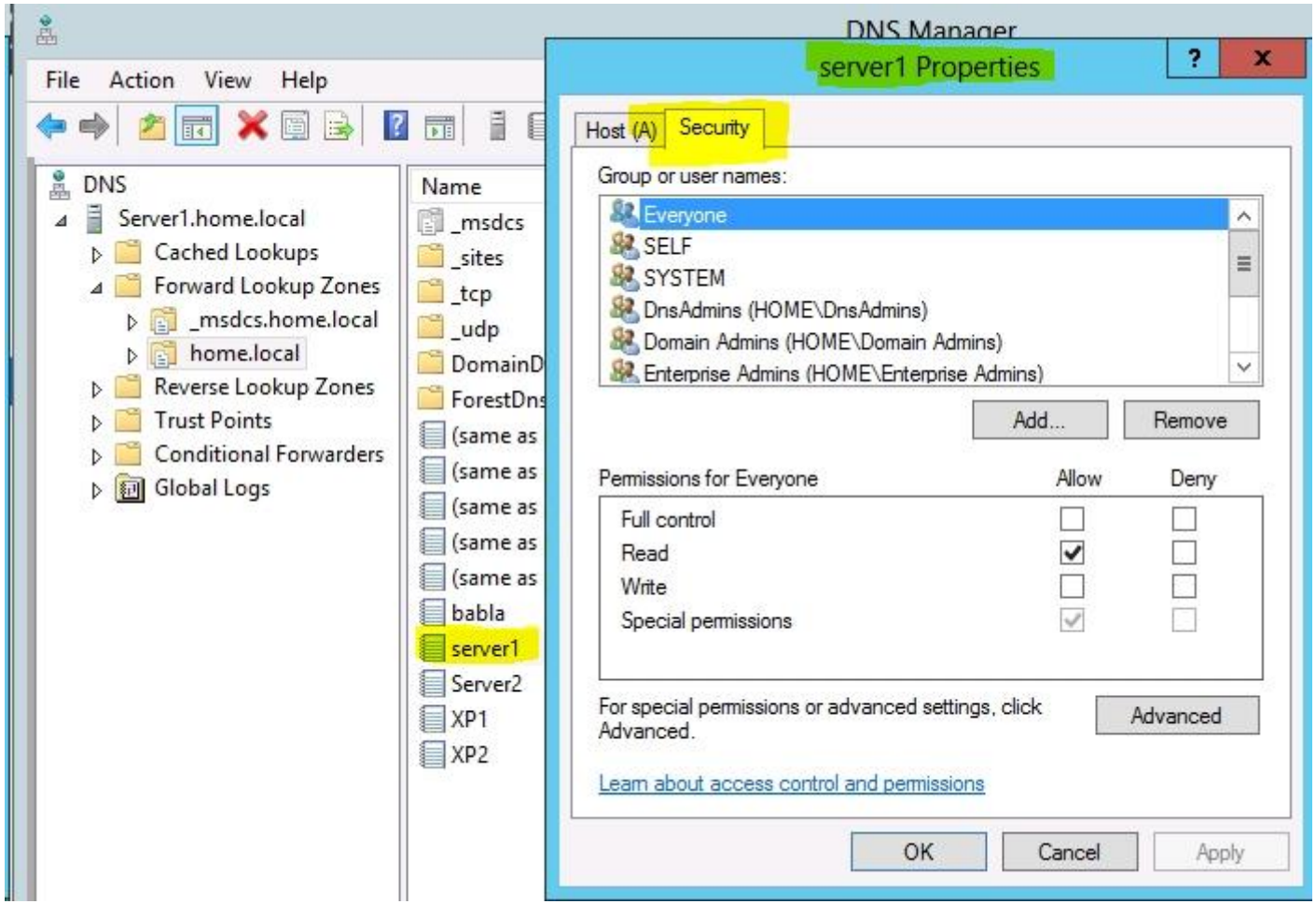
A. Run the Zone Signing Wizard for the zone.
B. From the properties of the zone, change the zone type.
C. Run the new Delegation Wizard for the zone.
D. From the properties of the zone, modify the Start Of Authority (SOA) record.

Correct Answer: B
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:

DNS update security is available only for zones that are integrated into Active Directory. After you integrate a zone, you can use the access control list (ACL) editing features that are available in the DNS snap-in to add or to remove users or groups from the ACL for a specific zone or for a resource record.



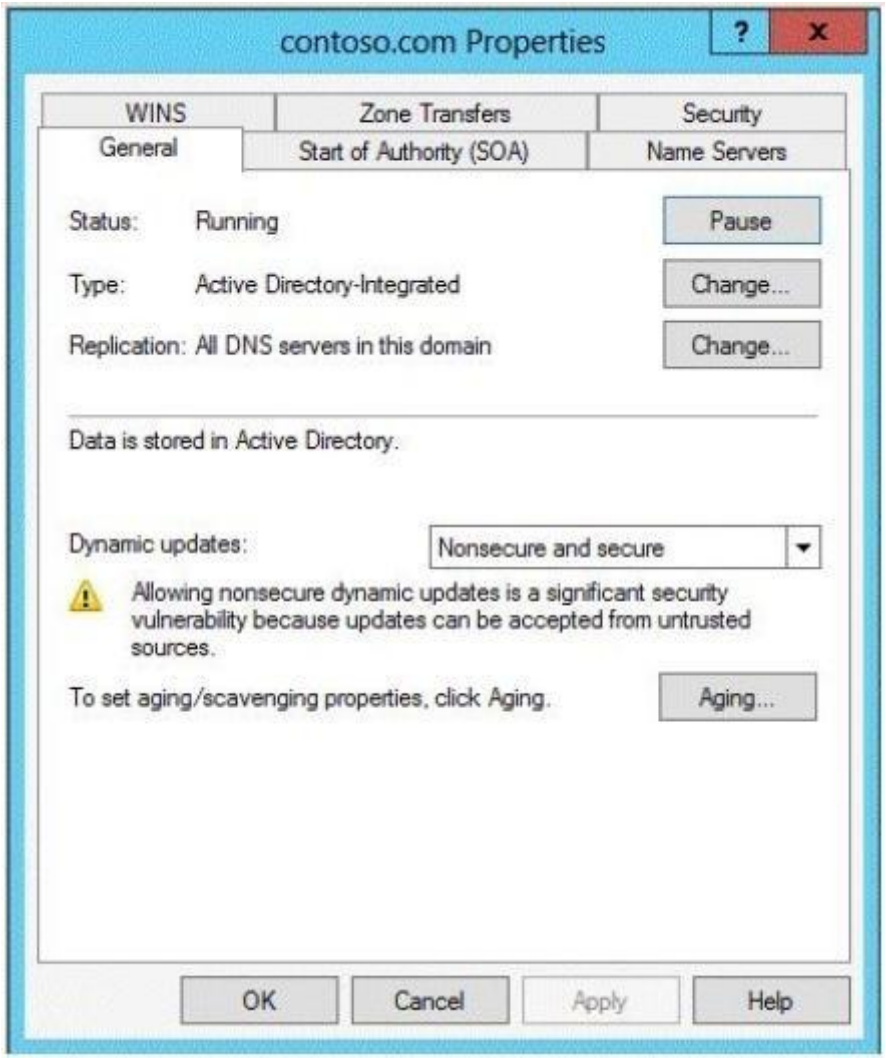


http://technet.microsoft.com/en-us/library/cc753014.aspx

QUESTION 38

Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1. DC1 is a DNS server for contoso.com.

The properties of the contoso.com zone are configured as shown in the exhibit. (Click the Exhibit button.)



The domain contains a server named Server1 that is part of a workgroup named Workgroup.

Server1 is configured to use DC1 as a DNS server.

You need to ensure that Server1 dynamically registers a host (A) record in the contoso.com zone.

What should you configure?

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

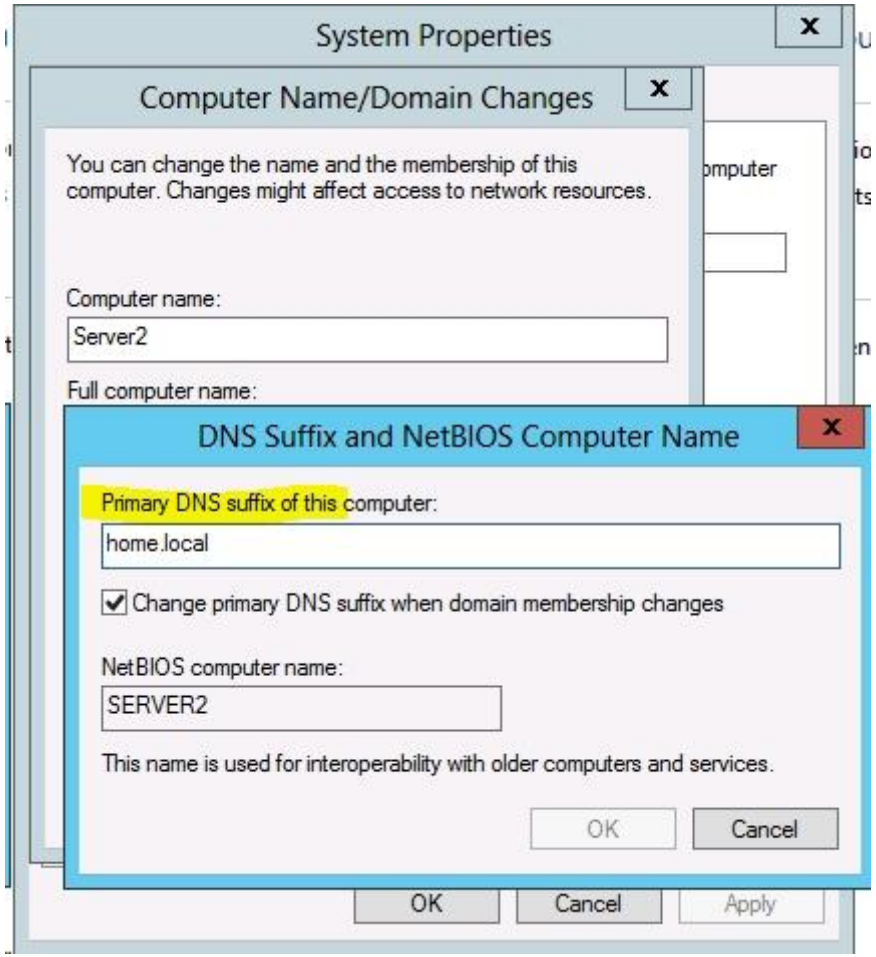
Correct Answer: C
Section: Configure Network Services and Access Services
Explanation

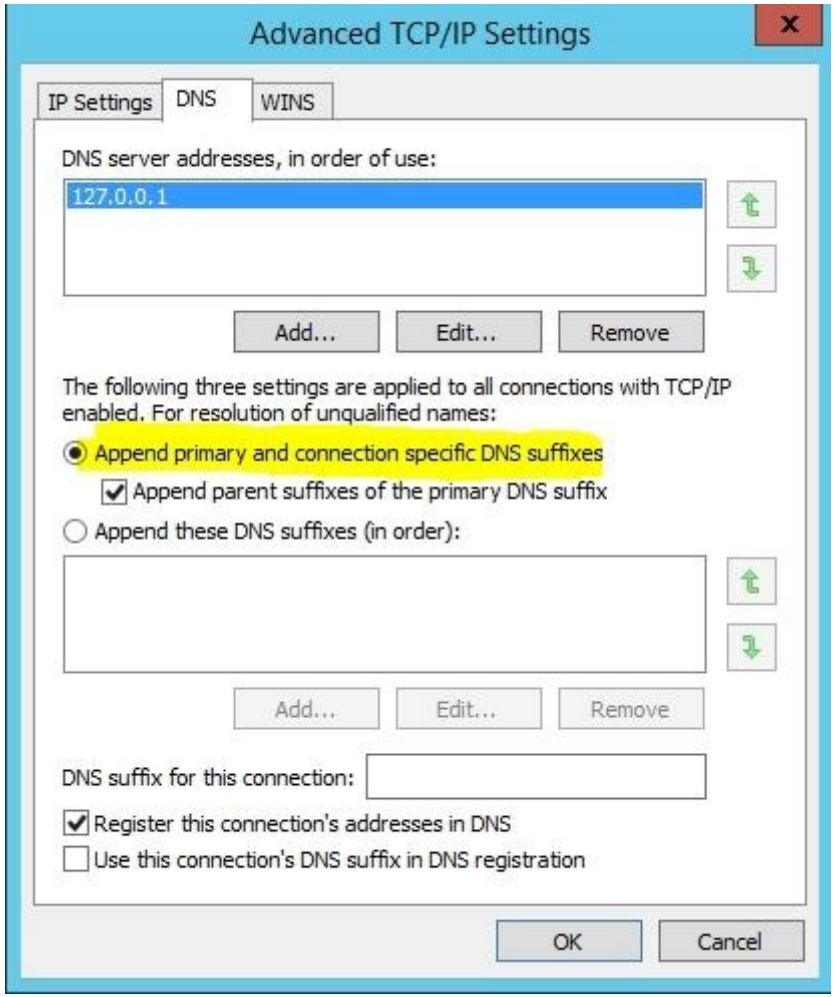
Explanation/Reference:
What Is **DNS Suffix**?

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

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

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


System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
Server2
Full computer name:
DNS Suffix and NetBIOS Computer Name
Primary DNS suffix of this computer:
home.local
Change primary DNS suffix when domain membership changes
NetBIOS computer name:
SERVER2
This name is used for interoperability with older computers and services.
OK
Cancel
OK
Cancel
Apply



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

QUESTION 39
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012. 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?

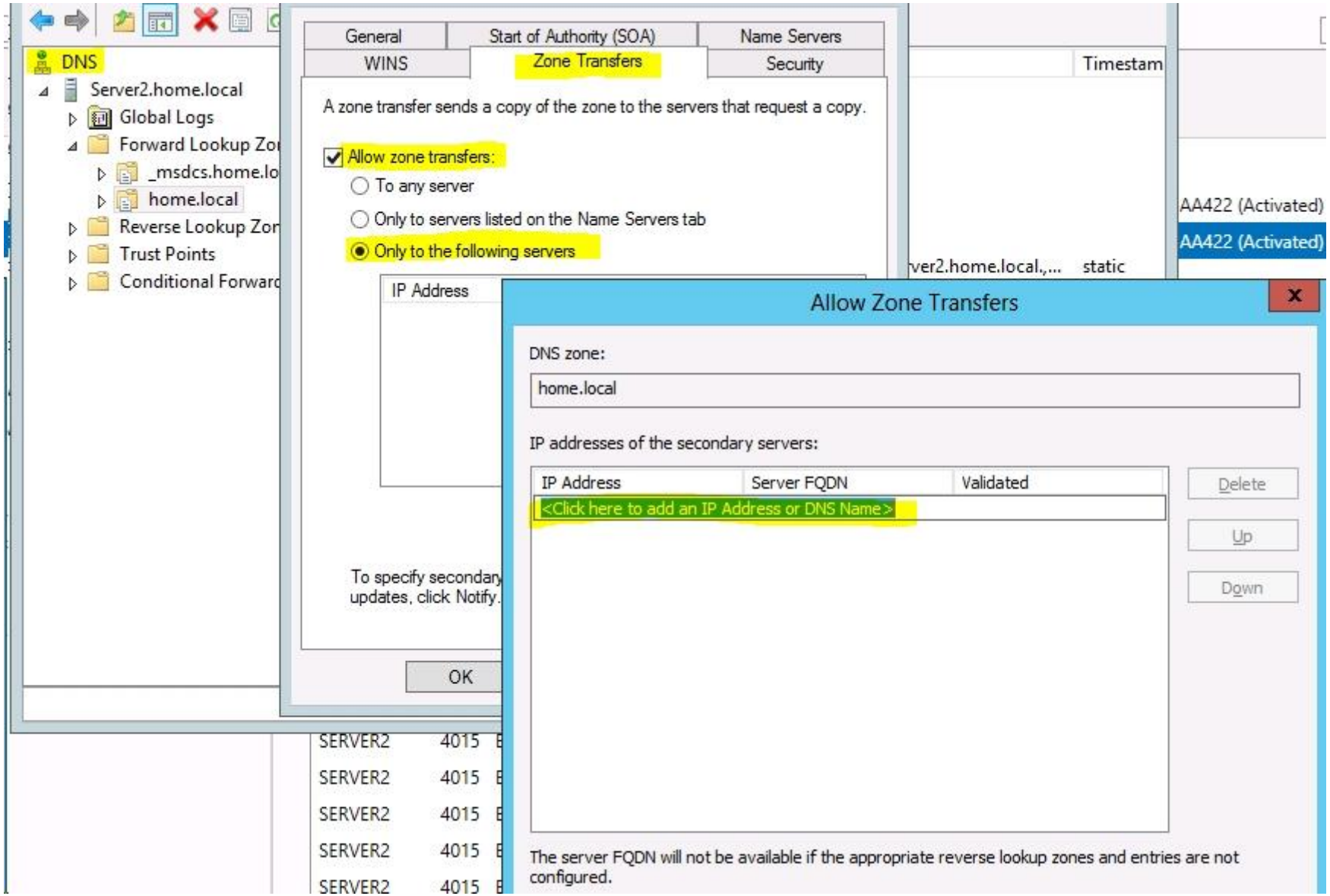
A. From Windows PowerShell, run the **Set-DnsServerSetting** cmdlet and specify DC1 as a target.
B. From DNS Manager, modify the Zone Transfers settings of the contoso.com zone.
C. From DNS Manager, modify the replication scope of the contoso.com zone.
D. From tDNS manager, modify the Security settings of the contoso.com zone.

Correct Answer: B
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Definition of a **Zone Transfer**: A Zone Transfer is the term used to refer to the process by which the contents of a DNS Zone file are copied from a primary DNS server to a secondary DNS server.
Master servers can be any other DNS server that loads the zone, such as either the primary server for the zone or another secondary server. When the master server receives the request for the zone, it can reply with either a partial or full transfer of the zone to the secondary server.
By default, the DNS server will only allow a zone transfer to authoritative DNS servers listed in the name server (NS) resource records for the zone.

A Zone transfer will occur during any of the following scenarios:
- When starting the DNS Service on the secondary DNS server.
- When the refresh time expires.
- When changes are saved to the Primary Zone file and there is a Notify List.

Zone Transfers are always initiated by the secondary DNS server. The primary DNS server simply answers the request for a Zone Transfer.



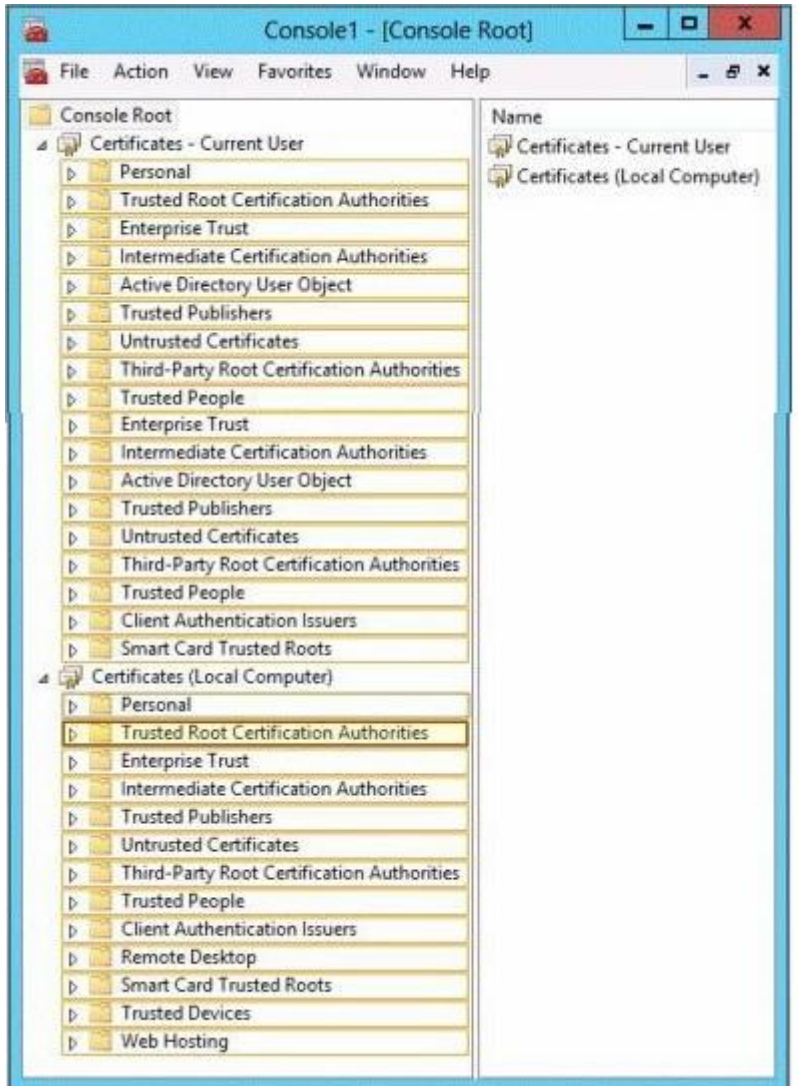
http://support.microsoft.com/kb/164017/en-us

http://technet.microsoft.com/en-us/library/cc781340%28v=ws.10%29.aspx

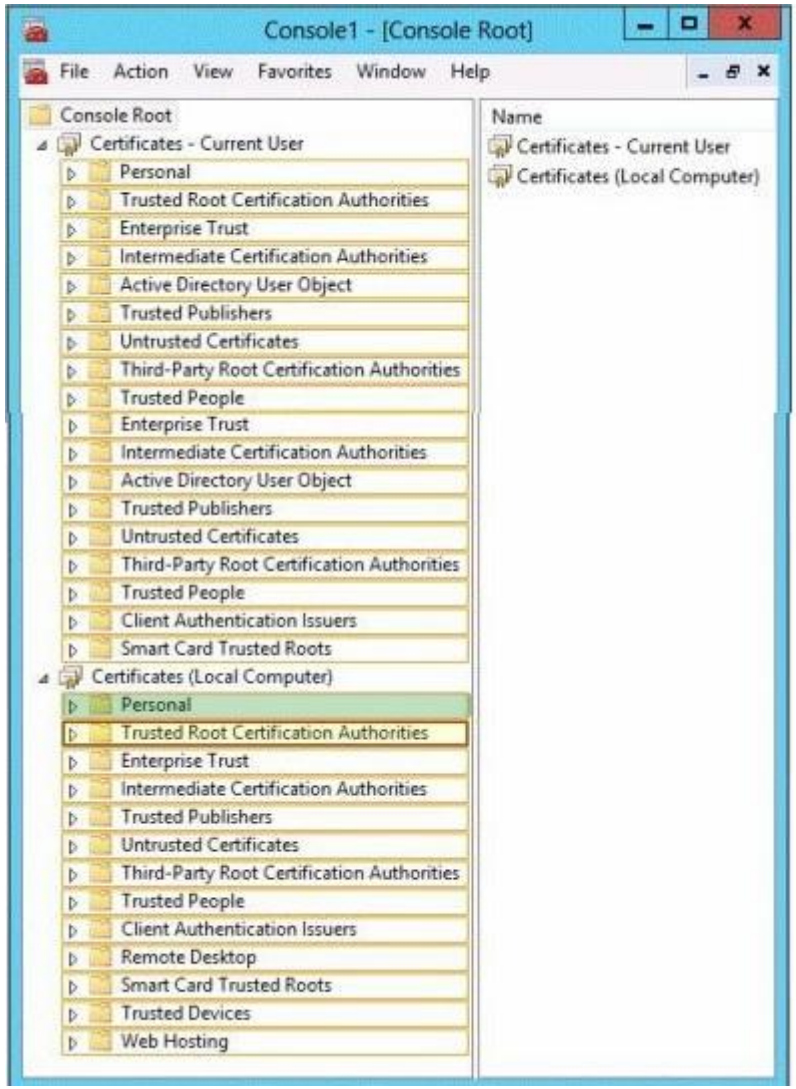
QUESTION 40
You have a server named Server1 that has the Web Server (IIS) server role installed.
You obtain a Web Server certificate.
You need to configure a website on Server1 to use Secure Socket Layer (SSL).

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

Hot Area:



Correct Answer:



Section: Configure Network Services and Access Services
Explanation

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

If it is a Self Signed certificate, it only can be used on the local server machine.
If it is a public certificate, you'll need to download the CA root certificate of the certificate and install the CA root certificate into the Trusted Root Certificate Authorities store.
Root certificates provide a level of trust that certificates that are lower in the hierarchy can inherit. Each certificate is inspected for a parent certificate until the search reaches the root certificate.
For more information about certificate, please refer to: http://technet.microsoft.com/en-us/library/cc700805.aspx

http://support.microsoft.com/kb/232137/en-us
http://www.sqlservermart.com/HowTo/Windows_Import_Certificate.aspx
http://msdn.microsoft.com/en-us/library/windows/hardware/ff553506%28v=vs.85%29.aspx
http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis
http://support.microsoft.com/kb/299875/en-us
http://technet.microsoft.com/en-us/library/dd163531.aspx
http://blogs.msdn.com/b/mosharaf/archive/2006/10/30/using-test-certificate-with-reporting-services-2005-to-establish-ssl-connection.aspx

QUESTION 41
Your network contains a DNS server named Server1 that runs Windows Server 2012. Server1 has a zone named contoso.com. The network contains a server named Server2 that runs Windows Server 2008 R2. Server1 and Server2 are members of an Active Directory domain named contoso.com.
You change the IP address of Server2.

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

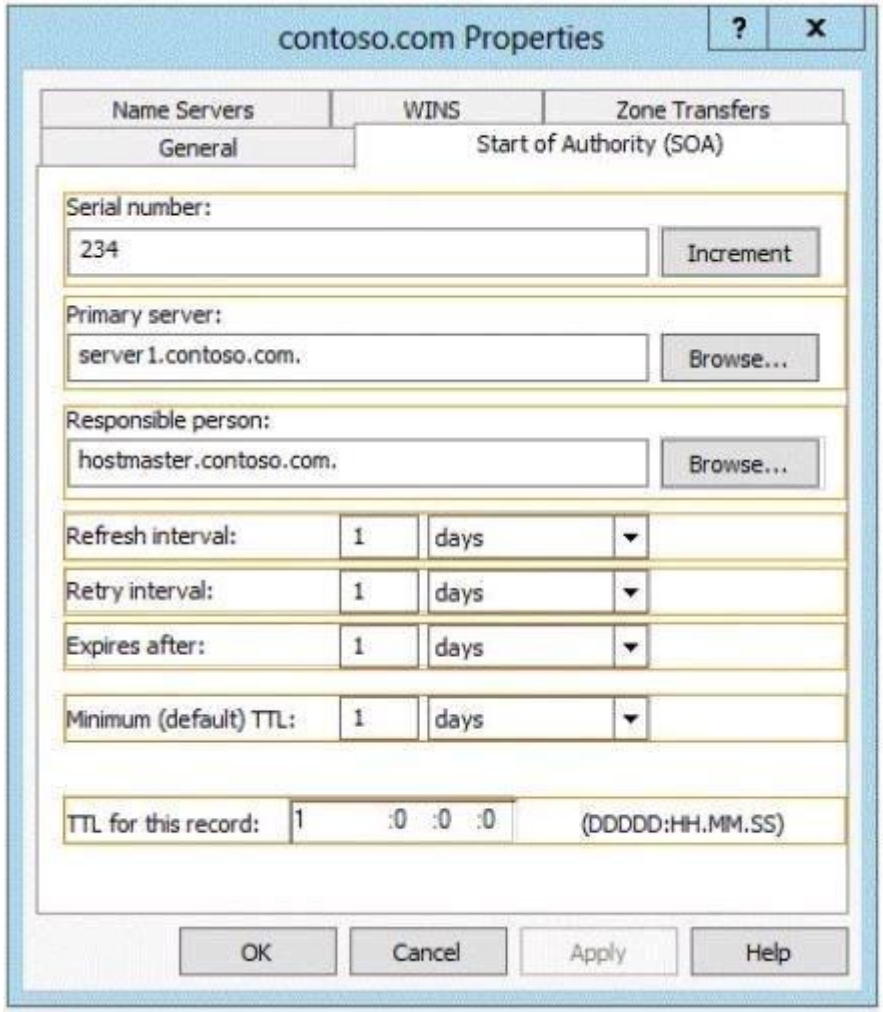
On the affected users' client computers, you flush the DNS client resolver cache, and the users successfully connect to Server2.

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

Which value should you modify in the Start of Authority (SOA) record?

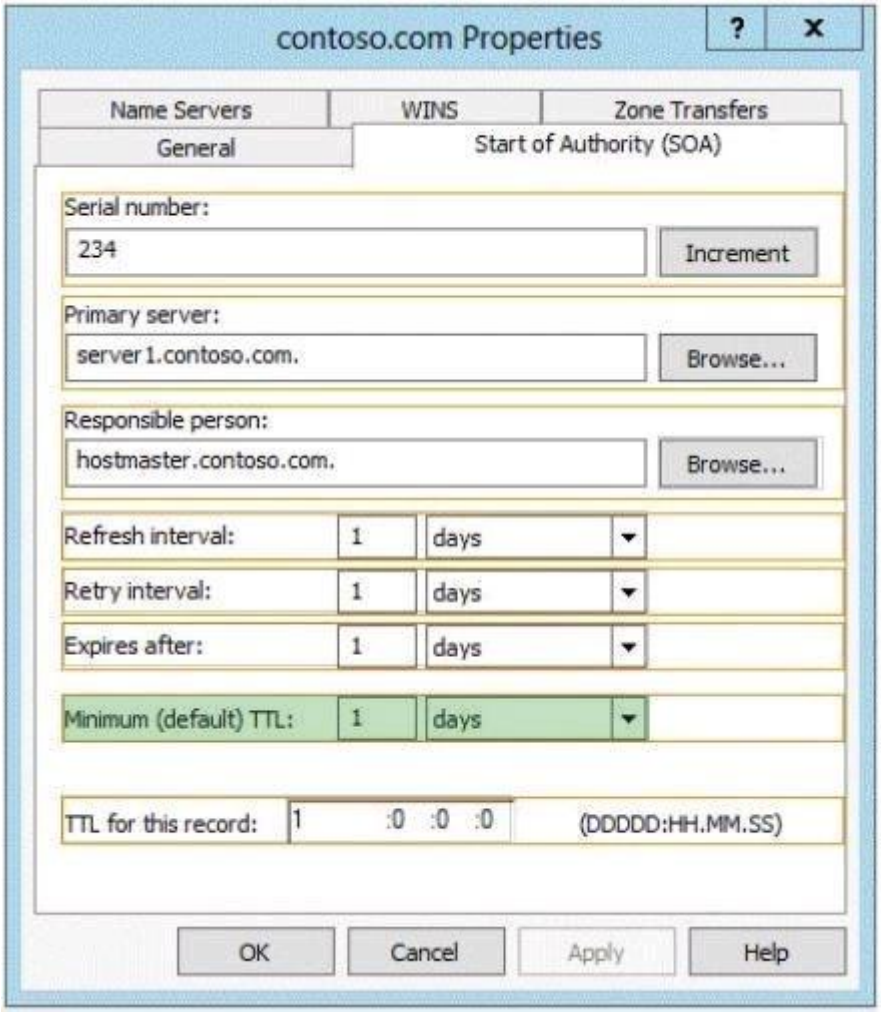
To answer, select the appropriate setting in the answer area.

Hot Area:



Correct Answer:

VCEplus.com



Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
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.

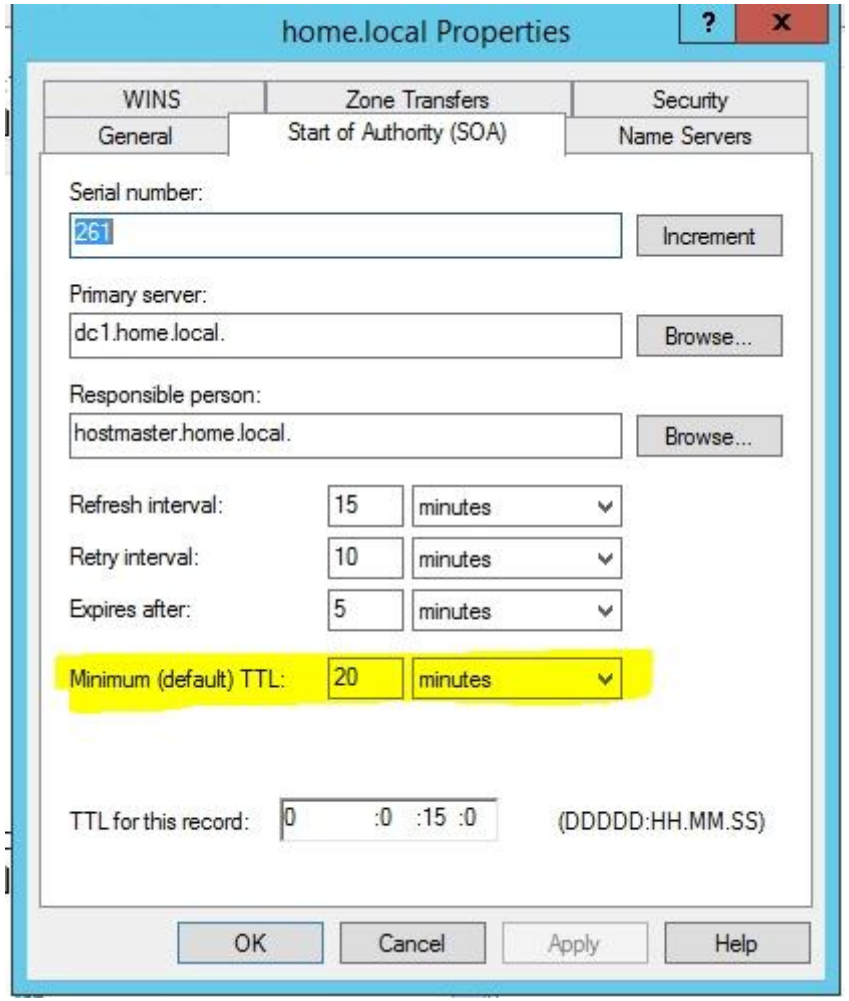
The Default TTL, is just that a default for newly created records. Once the records are created their TTL is independent of the Default TTL on the SOA.

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.

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



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

```
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
```

http://support.microsoft.com/kb/297510/en-us
https://en.wikipedia.org/wiki/Time_to_live
http://www.faqs.org/rfcs/rfc2308.html#ixzz0qVpTEitk

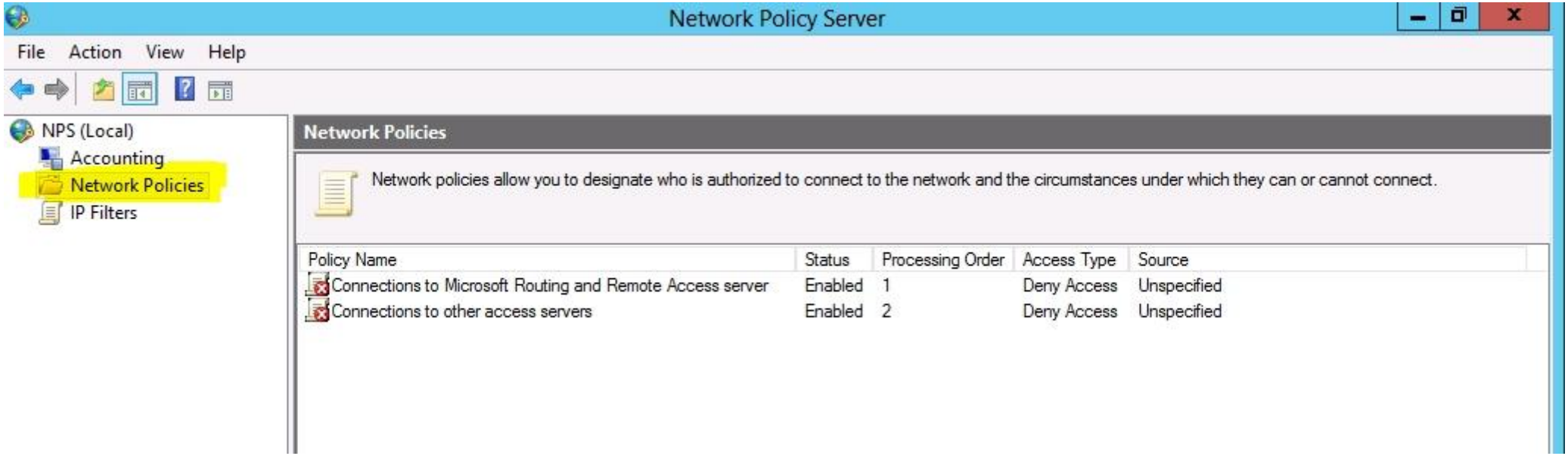
QUESTION 42
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012. You enable and configure Routing and Remote Access (RRAS) on Server1. You create a user account named User1.
You need to ensure that User1 can establish VPN connections to Server1.

What should you do?

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

Correct Answer: A
Section: Configure Network Services and Access Services
Explanation

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



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

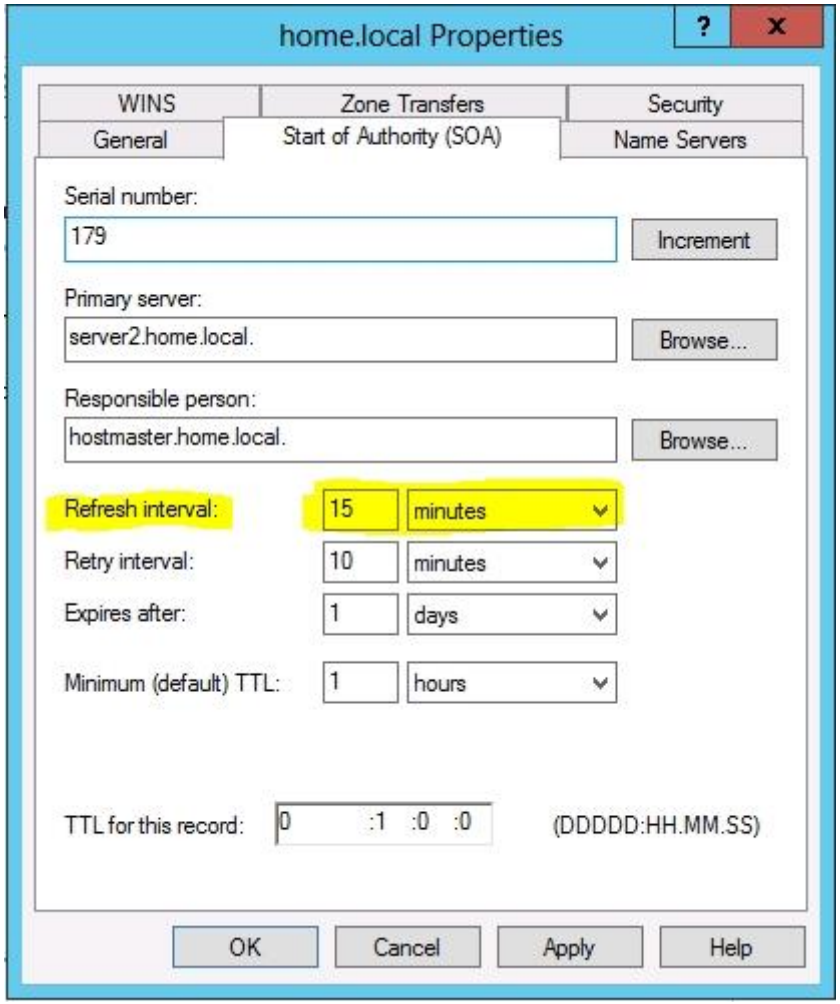
QUESTION 43
Server1 as a DNS server hosts a Primary zone,Server2 is the secondary zone contoso.com domain, you need to determine how long Server2 Server1 to renew regional, how to configure

A. Refresh interval
B. Restart DNS
C. Forwarders
D. Stub zone

Correct Answer: A
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Refresh interval. Used to determine how often other DNS servers that load and host the zone must attempt to renew the zone.

Open DNS.
In the console tree, right-click the applicable zone and click **Properties**.
On the **General** tab, verify that the zone type is either **Primary** or **Active Directory-integrated**.
Click the **Start of Authority (SOA)** tab.
In **Refresh interval**, click a time period in minutes, hours, or days, and type a number in the text box.
Click **OK** to save the adjusted interval.



http://technet.microsoft.com/en-us/library/cc755646(v=ws.10).aspx

QUESTION 44

Your network contains an Active Directory domain named fabrikam.com. You implement DirectAccess and an IKEv2 VPN. You need to view the properties of the VPN connection.

Which connection properties should you view? To answer, select the appropriate connection properties in the answer area.

Hot Area:

Correct Answer:

Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
DirectAccess, also known as Unified Remote Access, is a VPN-like technology that provides intranet connectivity to client computers when they are connected to

the Internet. Unlike many traditional VPN connections, which must be initiated and terminated by explicit user action, DirectAccess connections are designed to connect automatically as soon as the computer connects to the Internet. With Windows Server 2012, DirectAccess is fully integrated into the operating system, providing a user interface to configure it without UAG.

IKEv2 is a tunneling protocol that uses the IPsec Tunnel Mode protocol over UDP port 500. An IKEv2 VPN provides resilience to the VPN client when the client moves from one wireless hotspot to another or when it switches from a wireless to a wired connection. The use of IKEv2 and IPsec allows support for strong authentication and encryption methods.

DirectAccess – Always Connected!
Microsoft DirectAccess is a remote access technology that is best described as an automatic VPN. When a user takes their DirectAccess-enabled laptop home, to the coffee shop, or wherever, as soon as they have Internet access they also automatically have corporate network access. There is nothing that the user needs to launch or log on to, to establish this access. Their computer takes a combination of computer credentials (NTLM authentication) and their user credentials that they used to log on to the computer in the first place (Kerberos authentication) and uses those items to establish IPSec tunnels to a DirectAccess server sitting in the company datacenter. Because of the automatic establishment of these tunnels, users can literally be working on their laptop in the office, close the lid and take it home, open the lid when they get home, and continue working as if nothing happened. As long as they are connected to the Internet at home (or wherever they happen to be), these tunnels will build in the background within seconds and the user simply continues to work. They have access to all resources in the network just like they did when they were inside the office.

http://technet.microsoft.com/en-us/library/jj613767.aspx
http://technet.microsoft.com/en-us/security/jj991832.aspx
http://en.wikipedia.org/wiki/DirectAccess
http://technet.microsoft.com/en-us/library/dd469817%28v=ws.10%29.aspx

QUESTION 45
You have a server named Server1 that runs Windows Server 2012. Server1 has the Remote Access server role installed.
On Server1, you create a network policy named PPTP_Policy.
You need to configure PPTP_Policy to apply only to VPN connections that use the PPTP protocol.

What should you configure in PPTP_Policy?

A. The Service Type
B. The Tunnel Type
C. The Framed Protocol
D. The NAS Port Type

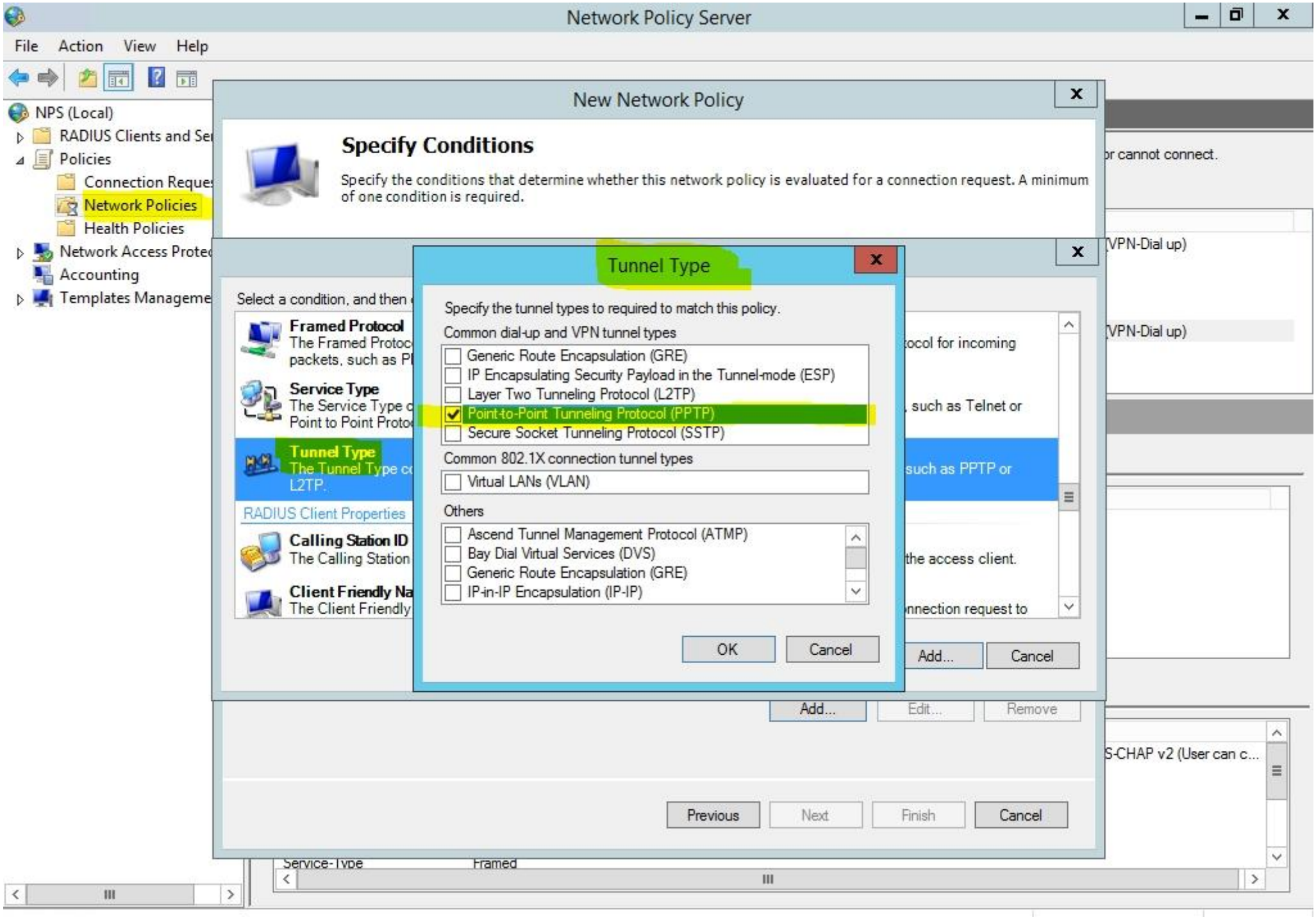
Correct Answer: B
Section: Configure Network Services and Access Services

VCEplus.com

Explanation

Explanation/Reference:
Network Policy Server (NPS) uses network policies, formerly named remote access policies, and the dial-in properties of user accounts to determine whether a connection request should be authorized to connect to the network.
You can use this procedure to configure a new network policy in either the NPS snap-in or the Routing and Remote Access Service snap-in.

Tunnel Type
Restricts the policy to only clients that create a specific type of tunnel, such as **PPTP** or **L2TP**. The Tunnel Type attribute is typically used when you deploy virtual local area networks (VLANs).


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Se
Policies
Connection Reques
Network Policies
Health Policies
Network Access Protec
Accounting
Templates Manageme
New Network Policy
Specify Conditions
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.
Select a condition, and then
Framed Protocol
Service Type
Tunnel Type
RADIUS Client Properties
Calling Station ID
Client Friendly Na
Tunnel Type
Specify the tunnel types to required to match this policy.
Common dial-up and VPN tunnel types
Generic Route Encapsulation (GRE)
IP Encapsulating Security Payload in the Tunnel-mode (ESP)
Layer Two Tunneling Protocol (L2TP)
Point-to-Point Tunneling Protocol (PPTP)
Secure Socket Tunneling Protocol (SSTP)
Common 802.1X connection tunnel types
Virtual LANs (VLAN)
Others
Ascend Tunnel Management Protocol (ATMP)
Bay Dial Virtual Services (DVS)
Generic Route Encapsulation (GRE)
IP-in-IP Encapsulation (IP-IP)
OK
Cancel
Add...
Cancel
Add...
Edit...
Remove
Previous
Next
Finish
Cancel
Service-Type
Framed
(VPN-Dial up)
(VPN-Dial up)
S-CHAP v2 (User can c...

http://technet.microsoft.com/en-us/library/cc755309%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc754422%28v=ws.10%29.aspx

QUESTION 46
Your network contains a RADIUS server named Server1.
You install a new server named Server2 that runs Windows Server 2012 and has Network Policy Server (NPS) installed.
You need to ensure that all accounting requests for Server2 are forwarded to Server1.
On Server2, you configure a Connection Request Policy.

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

Hot Area:

Correct Answer:

VCEplus.com

Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
When you configure NPS as a RADIUS proxy, you create a new connection request policy that NPS uses to determine which connection requests to forward to other RADIUS servers. In addition, the connection request policy is configured by specifying a remote RADIUS server group that contains one or more RADIUS servers, which tells NPS where to send the connection requests that match the connection request policy.

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

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

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

A remote RADIUS server group is a named group that contains one or more RADIUS servers. If you configure more than one server, you can specify load balancing settings to either determine the order in which the servers are used by the proxy or to distribute the flow of RADIUS messages across all servers in the group to prevent overloading one or more servers with too many connection requests.

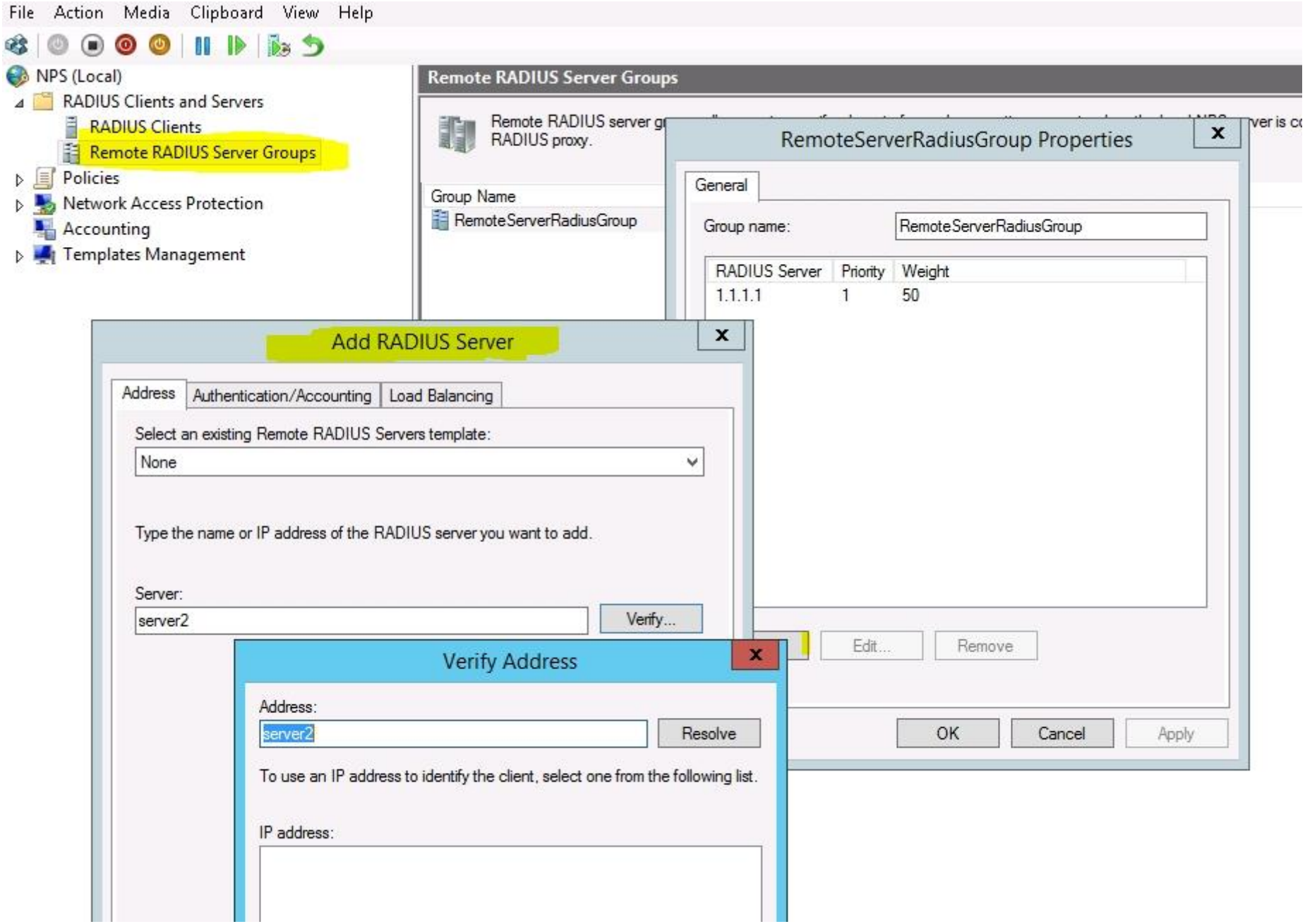
Each server in the group has the following settings:

- Name or address
- Each group member must have a unique name within the group. The name can be an IP address or a name that can be resolved to its IP address.
- Authentication and accounting
- You can forward authentication requests, accounting requests, or both to each remote RADIUS server group member.
- Load balancing

A priority setting is used to indicate which member of the group is the primary server (the priority is set to 1). For group members that have the same priority, a weight setting is used to calculate how often RADIUS messages are sent to each server. You can use additional settings to configure the way in which the NPS server detects when a group member first becomes unavailable and when it becomes available after it has been determined to be unavailable.

After a remote RADIUS server group is configured, it can be specified in the authentication and accounting settings of a connection request policy. Because of this, you can configure a remote RADIUS server group first. Next, you can configure the connection request policy to use the newly configured remote RADIUS server group. Alternatively, you can use the New Connection Request Policy Wizard to create a new remote RADIUS server group while you are creating the connection request policy.

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



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

Remote RADIUS server groups are unrelated to and separate from Windows groups and Network Access Protection (NAP) remediation server groups.
http://technet.microsoft.com/en-us/library/cc754518.aspx
http://technet.microsoft.com/en-us/library/cc753894.aspx

QUESTION 47
Your network contains two Active Directory forests named contoso.com and adatum.com.
The contoso.com forest contains a server named server1.contoso.com.
The adatum.com forest contains a server named server2.adatum.com.
Both servers have the Network Policy Server role service installed. The network contains a server named Server3.
Server3 is located in the perimeter network and has the Network Policy Server role service installed.
You plan to configure Server3 as an authentication provider for several VPN servers.
You need to ensure that RADIUS requests received by Server3 for a specific VPN server are always forwarded to server1.contoso.com.

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

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

Correct Answer: BE
Section: Configure Network Services and Access Services
Explanation

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

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

File Action Media Clipboard View Help

Network Policy Server

File Action View Help

NPS (Local)
- RADIUS Clients and Se
  - RADIUS Clients
  - Remote RADIUS Se
- Policies
  - Connection Reques
  - Network Policies
  - Health Policies
- Network Access Protec
  - System Health Vali
  - Remediation Server
- Accounting
- Templates Manageme
  - Shared Secrets
  - RADIUS Clients
  - Remote RADIUS Se
  - IP Filters
  - Health Policies
  - Remediation Server

remote RADIUS servers. For

New Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

- Forwarding Connection Request
  - Authentication
  - Accounting

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

- ○ Authenticate requests on this server
- ◉ Forward requests to the following remote RADIUS server group for authentication:

RemoteServerRadiusGroup [New...]

RemoteServerRadiusGroup

- ○ Accept users without validating credentials

Previous | Next | Finish | Cancel

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

QUESTION 48
Your network contains an Active Directory domain named fabrikam.com. You implement DirectAccess.
You need to view the properties of the DirectAccess connection.

Which connection properties should you view? To answer, select the appropriate connection properties in the answer area.

Hot Area:

Correct Answer:

Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:

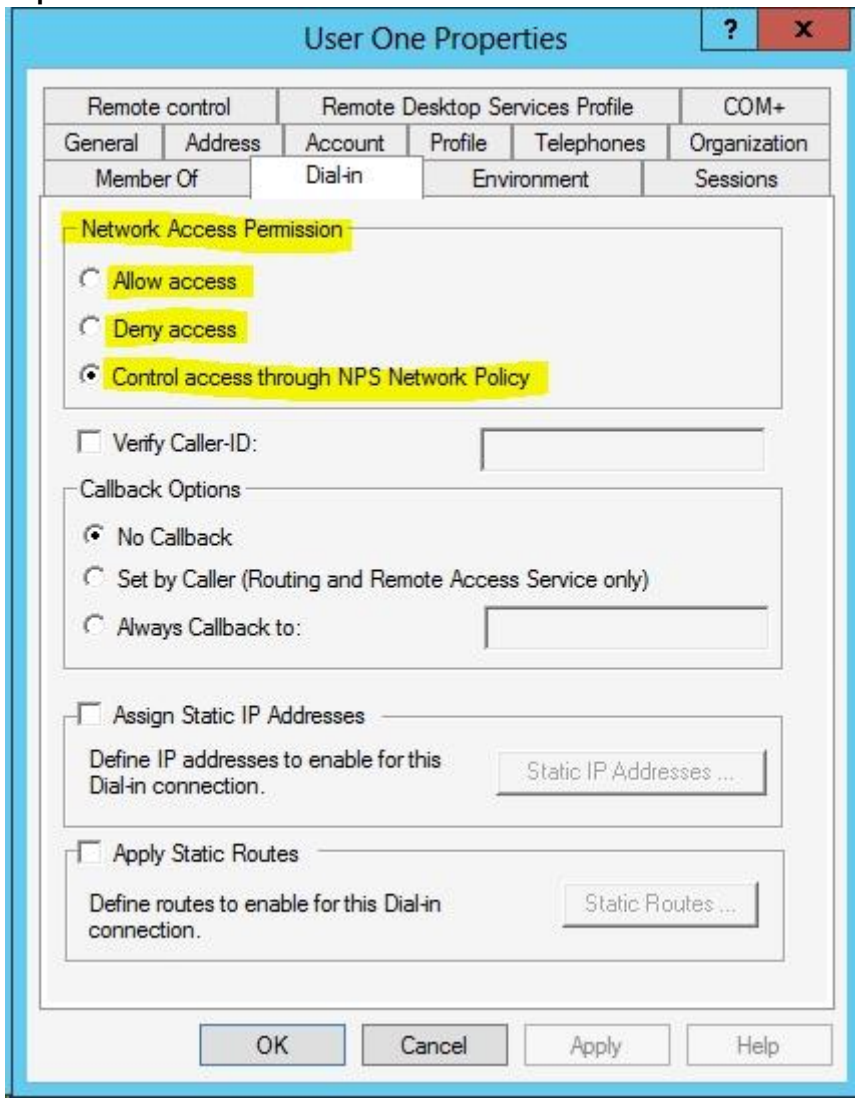
QUESTION 49
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012.
You enable and configure Routing and Remote Access (RRAS) on Server1.
You create a user account named User1. You need to ensure that User1 can establish VPN connections to Server1.

What should you do?

A. Add a RADIUS client.
B. Create a connection request policy.
C. Modify the members of the Remote Management Users group.
D. Modify the Dial-in setting of User1.

Correct Answer: D
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:



Access permission is also granted or denied based on the dial-in properties of each user account.
http://technet.microsoft.com/en-us/library/cc772123.aspx

QUESTION 50
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com.
All of the DNS servers in both of the domains run Windows Server 2012. The network contains two servers named Server1 and Server2.
Server1 hosts an Active Directory-integrated zone for contoso.com. Server2 hosts an Active Directory-integrated zone for fabrikam.com.
Server1 and Server2 connect to each other by using a WAN link.
Client computers that connect to Server1 for name resolution cannot resolve names in fabrikam.com.
You need to configure Server1 to support the resolution of names in fabrikam.com.
The solution must ensure that users in contoso.com can resolve names in fabrikam.com if the WAN link fails.

What should you do on Server1?

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

Correct Answer: C
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
With **secondary, you have ability to resolve records from the other domain even if its DNS servers are temporarily unavailable**
While secondary zones contain copies of all the resource records in the corresponding zone on the master name server, stub zones contain only three kinds of resource records:
- A copy of the SOA record for the zone.
- Copies of NS records for all name servers authoritative for the zone.
- Copies of A records for all name servers authoritative for the zone.

That's it; no CNAME records, MX records, SRV records, or A records for other hosts in the zone for a Stub Zone.
StubZone: What Happens if all Communication to Source Servers Is Lost?
In this regard, a stub zone behaves just like a standard secondary zone. A DNS secondary zone must get refreshed within a given expiration interval specified in the SOA record. The default zone expiration interval for Windows DNS is one day. If a DNS server can't refresh a secondary zone or stub zone within this interval, the server stops answering queries for the zone. Clients configured to use that DNS server as their primary server don't have any other way of finding another DNS server that might have a current copy of the zone. **Once their locally-cached resource records begin to expire, any process that relies on DNS name lookups in the source zone will start to fail.**

http://www.windowsnetworking.com/articles-tutorials/windows-2003/DNS_Stub_Zones.html
http://technet.microsoft.com/en-us/library/cc771898.aspx
http://redmondmag.com/Articles/2004/01/01/The-Long-and-Short-of-Stub-Zones.aspx?Page=2

QUESTION 51
Your network contains two servers named Server1 and Server2. Both servers run Windows Server 2012 and have the DNS Server server role installed.

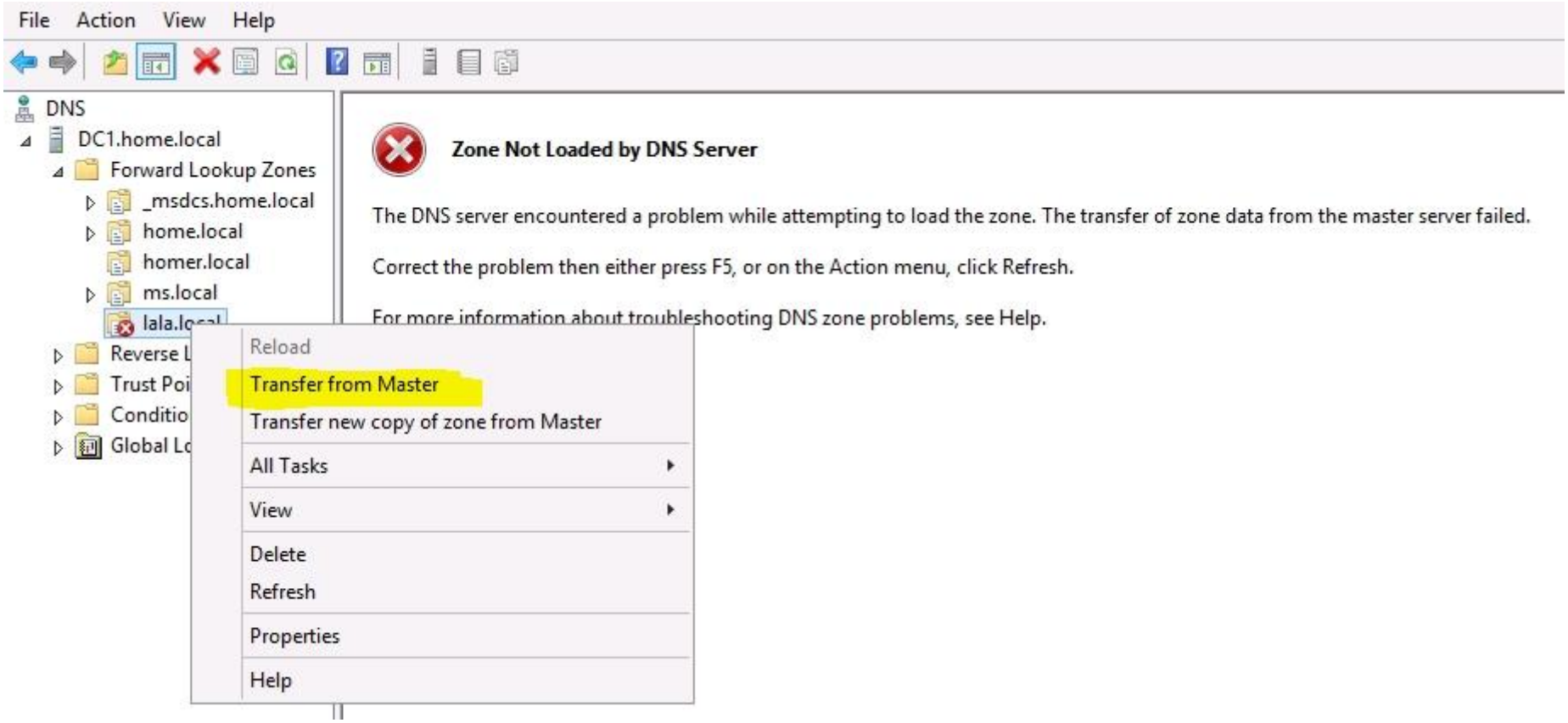
Server1 hosts a primary zone for contoso.com. Server2 hosts a secondary zone for contoso.com.
The zone is not configure to notify secondary servers of changes automatically. You update several records on Server1.
You need to force the replication of the contoso.com zone records from Server1 to Server2.

What should you do from Server2?

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

Correct Answer: D
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Initiate a zone transfer at a secondary server.
Open DNS; In the console tree, right-click the applicable zone and click **Transfer from master.**



http://technet.microsoft.com/en-us/library/cc779391%28v=ws.10%29.aspx

QUESTION 52
Your network contains an Active Directory domain named contoso.com. All client computers run Windows 8.
Your company has users who work from home. Some of the home users have desktop computers. Other home users have laptop computers.
All of the computers are joined to the domain. All of the computer accounts are members of a group named Group1.
Currently, the home users access the corporate network by using a PPTP VPN.
You implement DirectAccess by using the default configuration and you specify Group1 as the DirectAccess client group.
The home users who have desktop computers report that they cannot use DirectAccess to access the corporate network.
The home users who have laptop computers report that they can use DirectAccess to access the corporate network.
You need to ensure that the home users who have desktop computers can access the network by using DirectAccess.

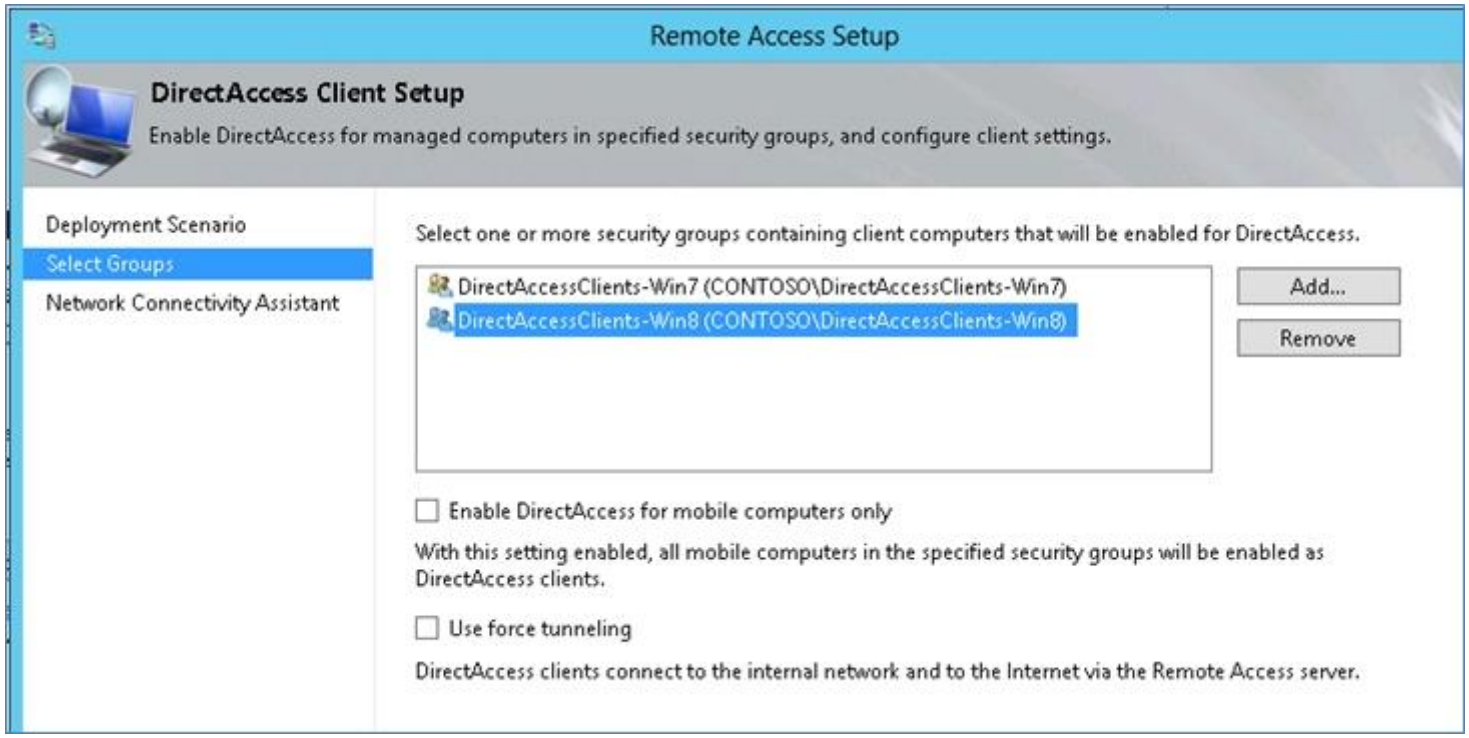
What should you modify?

A. The security settings of the computer accounts for the desktop computers
B. The membership of the RAS and IAS Servers group
C. The WMI filter for Direct Access Client Settings GPO
D. The conditions of the Connections to Microsoft Routing and Remote Access server policy

Correct Answer: C
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
DirectAccess does not face the same limitations of a VPN. DirectAccess allows a laptop or desktop that is configured properly to automatically connect by using a bidirectional connection between the client and the server.

Will DirectAccess be available to mobile computers only, or to any computer?
When you configure DirectAccess clients in the Enable DirectAccess wizard, you can choose to allow only mobile computers in the specified security groups to connect using DirectAccess. **If you restrict access to mobile computers, Remote Access automatically configures a WMI filter** to ensure that the DirectAccess client GPO is applied only to mobile computers in the specified security groups. The Remote Access administrator requires permissions to create or modify group policy WMI filters to enable this setting.



http://technet.microsoft.com/en-us/library/jj574145.aspx

QUESTION 53
You have a DNS server named Server1 that has a Server Core Installation on Windows Server 2012.
You need to view the time-to-live (TTL) value of a name server (NS) record that is cached by the DNS Server service on Server1.

What should you run?

A. Show-DNSServerCache
B. dnscacheugc.exe
C. ipconfiq.exe /displaydns
D. nslookup.exe

Correct Answer: A
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Show-DnsServerCache - Shows the records in a DNS Server Cache.
The Show-DNSServerCache shows all cached Domain Name System (DNS) server resource records in the following format: Name, ResourceRecordData, Time-to-Live (TTL).

Windows PowerShell

```
PS C:\> Show-DnsServerCache -ComputerName "Win12S-05.DNSServer-01.Contoso.com"
```

```
HostName                    RecordType Timestamp            TimeToLive      RecordData

--------                    ---------- ---------            ----------      ----------

@                           NS         0                    00:00:00        a.root-servers.net.

@                           NS         0                    00:00:00        b.root-servers.net.

@                           NS         0                    00:00:00        c.root-servers.net.

@                           NS         0                    00:00:00        d.root-servers.net.

@                           NS         0                    00:00:00        e.root-servers.net.

@                           NS         0                    00:00:00        f.root-servers.net.

@                           NS         0                    00:00:00        g.root-

Win12S-05.DNSServer-01.... A           0                    00:46:48        172.23.90.136

localhost                   A          0                    17089.09:29:04  127.0.0.1

a.root-servers.net          A          0                    00:00:00        198.41.0.4

b.root-servers.net          A          0                    00:00:00
```

http://technet.microsoft.com/en-us/library/jj649915.aspx

http://www.windowsnetworking.com/articles_tutorials/Managing-DNS-servers-using-PowerShell.html

QUESTION 54
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 the 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

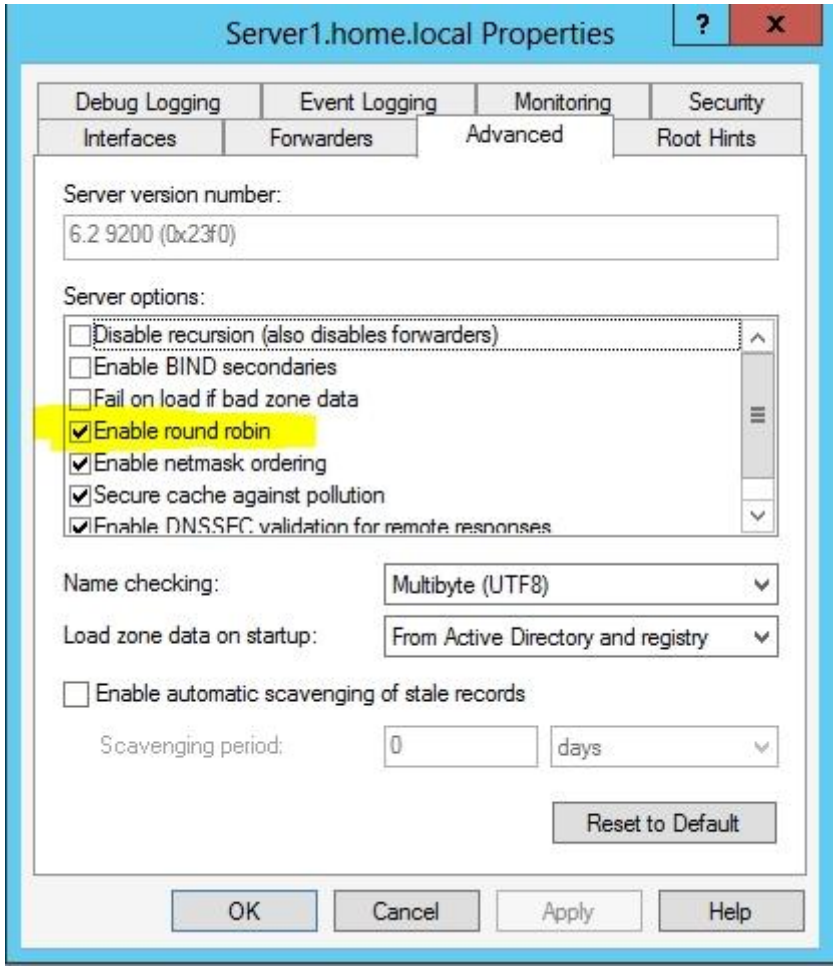
You need to use DNS records to load balance name resolution queries for **intranet.contoso.com** between the two Web servers.

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

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
Round robin is a local balancing mechanism used by DNS servers to share and distribute network resource loads. You can use it to rotate all resource record (RR) types contained in a query answer if multiple RRs are found.
By default, DNS uses round robin to rotate the order of RR data returned in query answers where multiple RRs of the same type exist for a queried DNS domain name. This feature provides a simple method for load balancing client use of Web servers and other frequently queried multihomed computers.
If round robin is disabled for a DNS server, the order of the response for these queries is based on a static ordering of RRs in the answer list as they are stored in the zone (either its zone file or Active Directory).



Question is know to have multiple answers depending on the number of server at the question like:

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

at this scenario it would be 3 the correct answer.

A records for each IP is needed.

http://technet.microsoft.com/en-us/library/cc772506.aspx
http://technet.microsoft.com/en-us/library/cc772774%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc787484%28v=ws.10%29.aspx

QUESTION 55
You have a Direct Access Server named Server1 running Server 2012 .

You need to add prevent users from accessing websites from an Internet connection

What should you configure?

A. Split Tunneling
B. Security Groups
C. Force Tunneling
D. Network Settings

Correct Answer: C
Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
C. To make Internet resources available to DirectAccess clients that use force tunneling, you can use a proxy server, which can receive IPv6-based requests for Internet resources and translate them to requests for IPv4-based Internet resources.

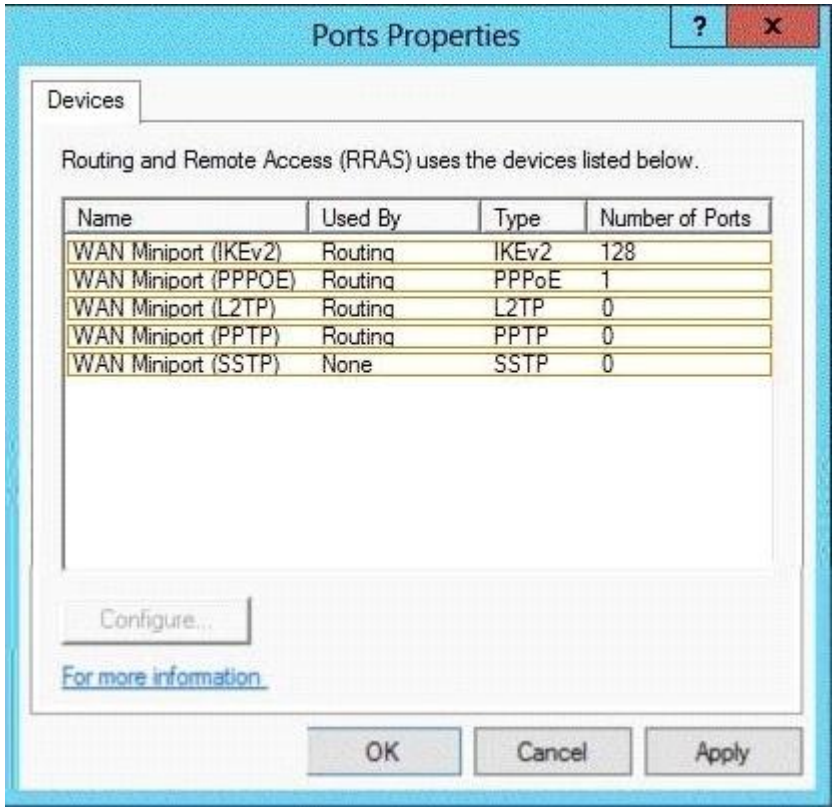
You can **configure DirectAccess clients to send all of their traffic through the tunnels to the DirectAccess server with force tunneling**. When force tunneling is configured, DirectAccess clients that detect that they are on the Internet modify their IPv4 default route so that default route IPv4 traffic is not sent. With the exception of local subnet traffic, all traffic sent by the DirectAccess client is IPv6 traffic that goes through tunnels to the DirectAccess server.

http://technet.microsoft.com/en-us/library/jj134204.aspx#BKMK_forcetunnel
http://blogs.technet.com/b/tomshinder/archive/2010/03/30/more-on-directaccess-split-tunneling-and-force-tunneling.aspx
http://blogs.technet.com/b/csstwplatform/archive/2009/12/15/directaccess-how-to-configure-force-tunneling-for-da-so-that-client-are-forced-to-use-ip-https.aspx
http://technet.microsoft.com/en-us//library/ee649127%28v=ws.10%29.aspx

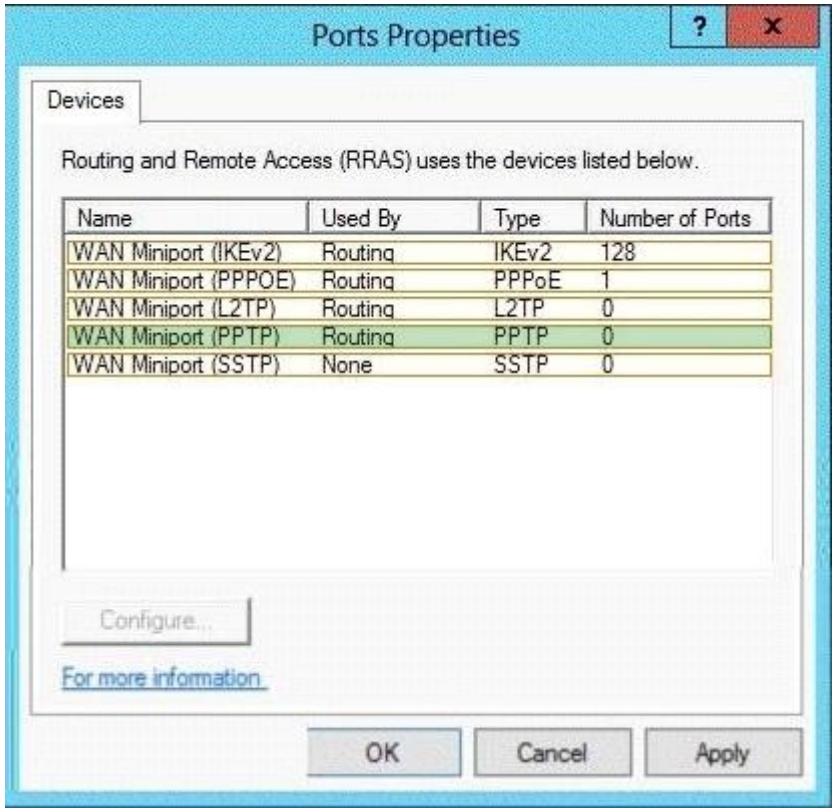
QUESTION 56
You have a server named Server1 that runs Windows Server 2012. Server1 has the Remote Access server role installed.
You need to configure the ports on Server1 to ensure that client computers can establish VPN connections to Server1.
The solution must NOT require the use of certificates or pre-shared keys.

What should you modify? To answer, select the appropriate object in the answer area.

Hot Area:



Correct Answer:



Section: Configure Network Services and Access Services
Explanation

Explanation/Reference:
The PPTP specification does **not describe encryption** or **authentication** features and relies on the Point-to-Point Protocol being tunneled to implement security functionality.

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

QUESTION 57
Your network contains multiple Active Directory sites.
You have a Distributed File System (DFS) namespace that has a folder target in each site.
You discover that some client computers connect to DFS targets in other sites.
You need to ensure that the client computers only connect to a DFS target in their respective site.

What should you modify?

A. the properties of the Active Directory site links.
B. the properties of the Active Directory sites.
C. the delegation settings of the namespace
D. the referral settings of the namespace

Correct Answer: D
Section: Configure file and print services
Explanation

Explanation/Reference:
A **referral is an ordered list of servers that a client computer receives from a domain controller or namespace** server when the user accesses a namespace root or DFS folder with targets. After the computer receives the referral, the computer attempts to access the first server in the list. If the server is not available, the client computer attempts to access the next server. If a server becomes unavailable, you can configure clients to fail back to the preferred server after it becomes available.

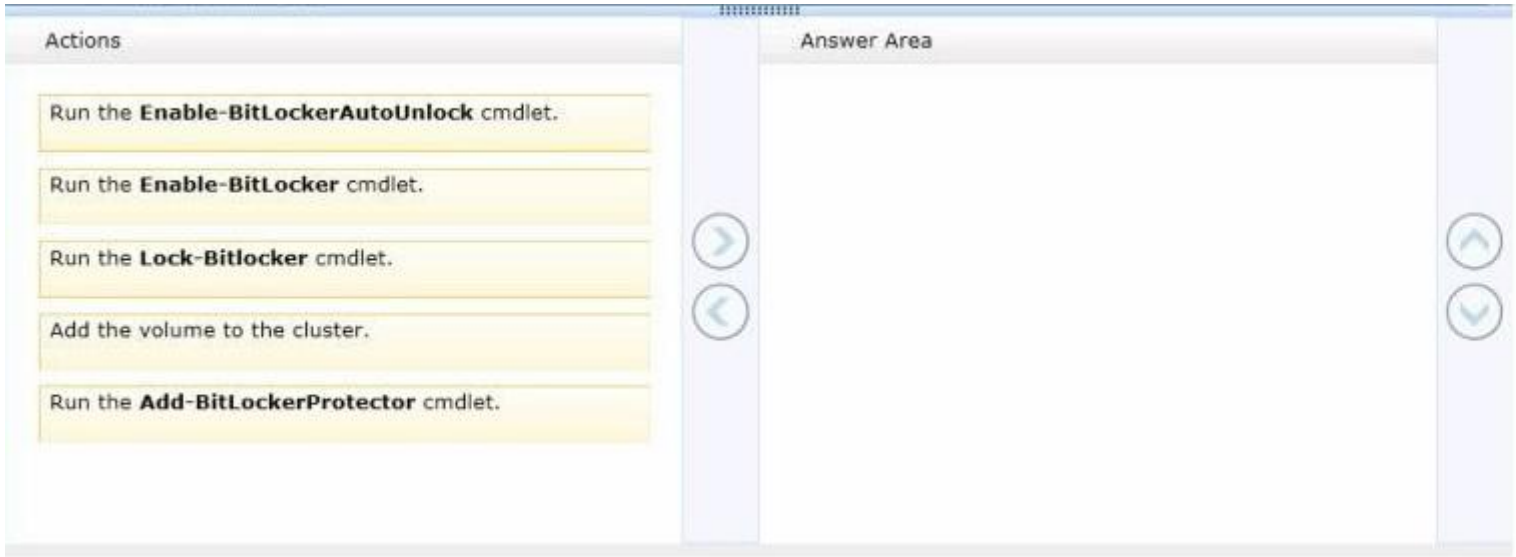
http://technet.microsoft.com/en-us/library/cc771266.aspx
http://blogs.technet.com/b/askds/archive/2011/10/27/dfs-override-referral-ordering-messing-with-the-natural-order.aspx
http://www.windowsnetworking.com/articles_tutorials/Configuring-DFS-Namespaces.html

QUESTION 58
Your network contains an Active Directory domain named contoso.com.
You have a failover cluster named Cluster1. All of the nodes in Cluster1 have BitLocker Drive Encryption (BitLocker) installed.
You plan to add a new volume to the shared storage of Cluster1.

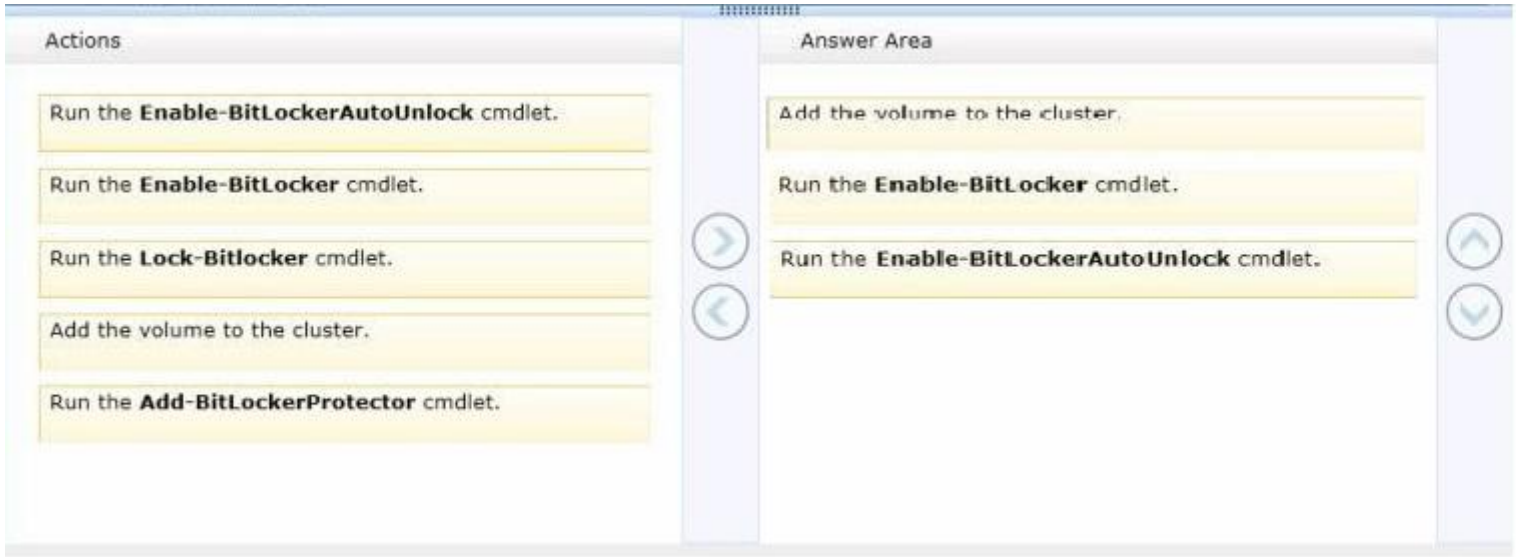
You need to add the new volume to the shared storage. The solution must meet the following requirements:
- Encrypt the volume.
- Avoid using maintenance mode on the cluster.

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

Select and Place:



Correct Answer:



Section: Configure file and print services
Explanation

Explanation/Reference:
Enable-BitLocker - Enables encryption for a BitLocker volume.

Enable-BitLockerAutoUnlock - Enables automatic unlocking for a BitLocker volume.

http://technet.microsoft.com/en-us/library/jj649829.aspx

QUESTION 59
Your network contains an Active Directory domain named contoso.com. The domain functional level in Windows Server 2008. All domain controllers run Windows Server 2008 R2.
The domain contains a file server named Server1 that runs Windows Server 2012.
Server1 has a BitLocker Drive Encryption (BitLocker)-encrypted drive. Server1 uses a trusted Platform Module (TPM) chip.
You enable the Turn on TPM backup to Active Directory Domain Services policy setting by using a Group Policy object (GPO).
You need to ensure that you can back up the BitLocker recovery information to Active Directory.

What should you do?

A. Upgrade a domain controller to Windows 2012.
B. Enable the Store BitLocker recovery information in the Active Directory Services (Windows Server2008 and Windows Vista) policy settings.
C. Raise the forest functional level to Windows 2008 R2.
D. Add a BitLocker data recovery agent

Correct Answer: B
Section: Configure file and print services
Explanation

Explanation/Reference:
You can configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives and the Trusted Platform Module (TPM) to Active Directory Domain Services (AD DS). Recovery information includes the recovery password for each BitLocker-protected drive, the TPM owner password, and the information required to identify which computers and drives the recovery information applies to. Optionally, you can also save a package containing the actual keys used to encrypt the data as well as the recovery password required to access those keys.

http://technet.microsoft.com/en-us/library/dd875529(v=ws.10).aspx

QUESTION 60
Your company has a main office and a branch office. The main office is located in Seattle. The branch office is located in Montreal.
Each office is configured as an Active Directory site. The network contains an Active Directory domain named adatum.com.
The Seattle office contains a file server named Server1. The Montreal office contains a file server named Server2.
The servers run Windows Server 2012 and have the File and Storage Services server role, the DFS Namespaces role service, and the DFS Replication role service installed.
Server1 and Server2 each have a share named Share1 that is replicated by using DFS Replication.
You need to ensure that users connect to the replicated folder in their respective office when they connect to \\contoso.com\Share1.

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

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

Correct Answer: ABD
Section: Configure file and print services
Explanation

Explanation/Reference:
To create a namespace
Click Start, point to **Administrative Tools**, and then click **DFS Management**.

In the console tree, right-click the **Namespaces** node, and then click **New Namespace**.

Follow the instructions in the **New Namespace Wizard**.

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

Important
Do not attempt to create a domain-based namespace using the Windows Server 2008 mode unless the forest functional level is Windows Server 2003 or higher. Doing so can result in a namespace for which you cannot delete DFS folders, yielding the following error message: “The folder cannot be deleted. Cannot complete this function.”
http://technet.microsoft.com/en-us/library/cc731531.aspx

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

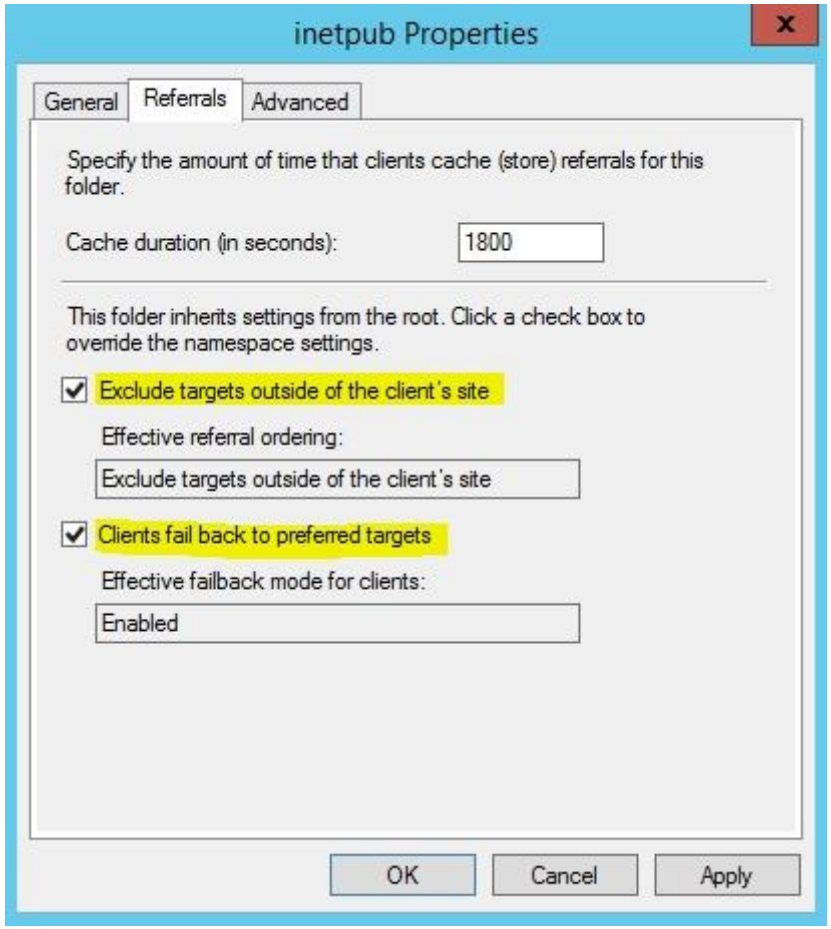
1. Click Start, point to Administrative Tools, and then click DFS Management.

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

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

4. In the Share and Publish Replicated Folder Wizard, click **Share and publish the replicated folder in a namespace**, and then follow the steps in the wizard.

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

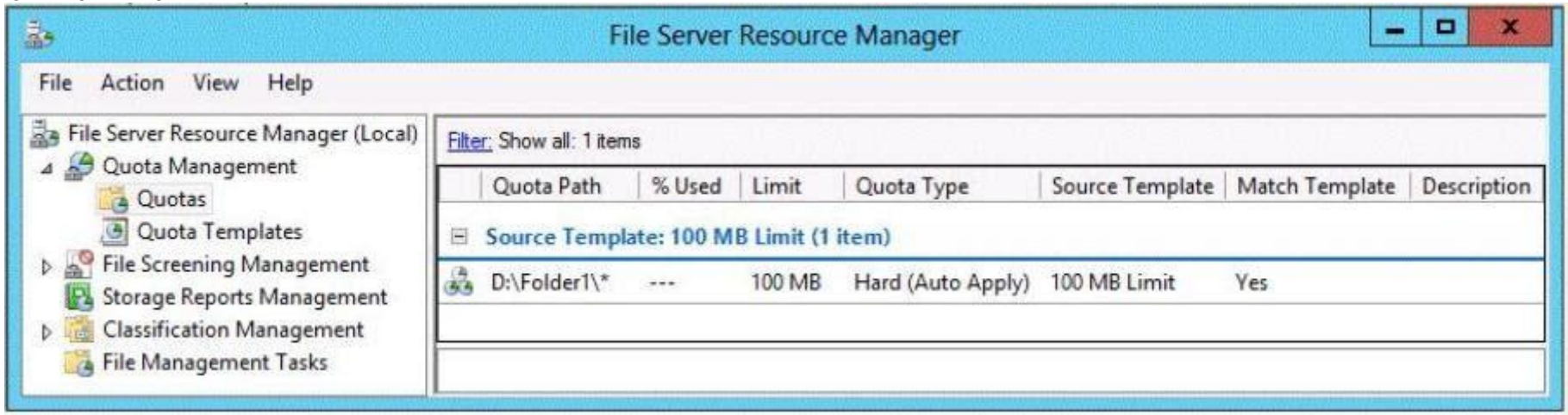


http://technet.microsoft.com/en-us/library/cc772778%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc732414.aspx
http://technet.microsoft.com/en-us/library/cc772379.aspx
http://technet.microsoft.com/en-us/library/cc732863%28v=ws.10%29.aspx

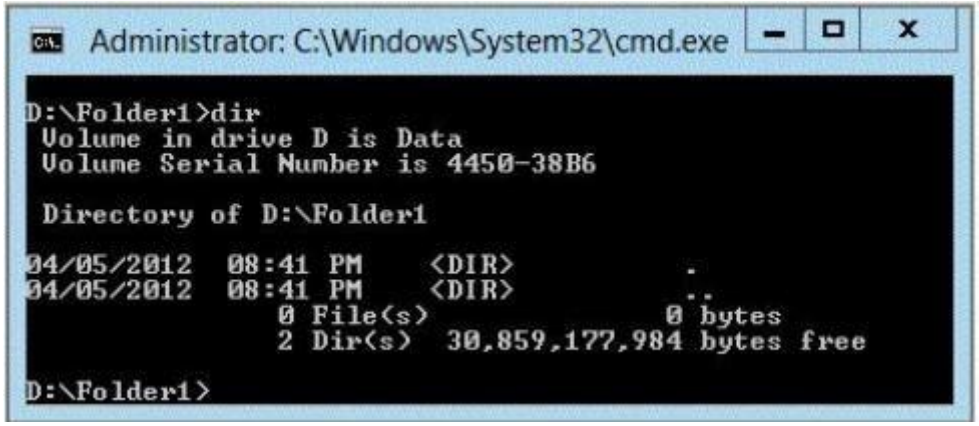
QUESTION 61
You have a server named Server1 that runs Windows Server 2012. An administrator creates a quota as shown in the Quota exhibit. (Click the Exhibit button.)
You run the dir command as shown in the Dir exhibit. (Click the Exhibit button.)

You need to ensure that D:\Folder1 can only consume 100 MB of disk space. What should you do?

Quota (exhibit):



Dir (exhibit):

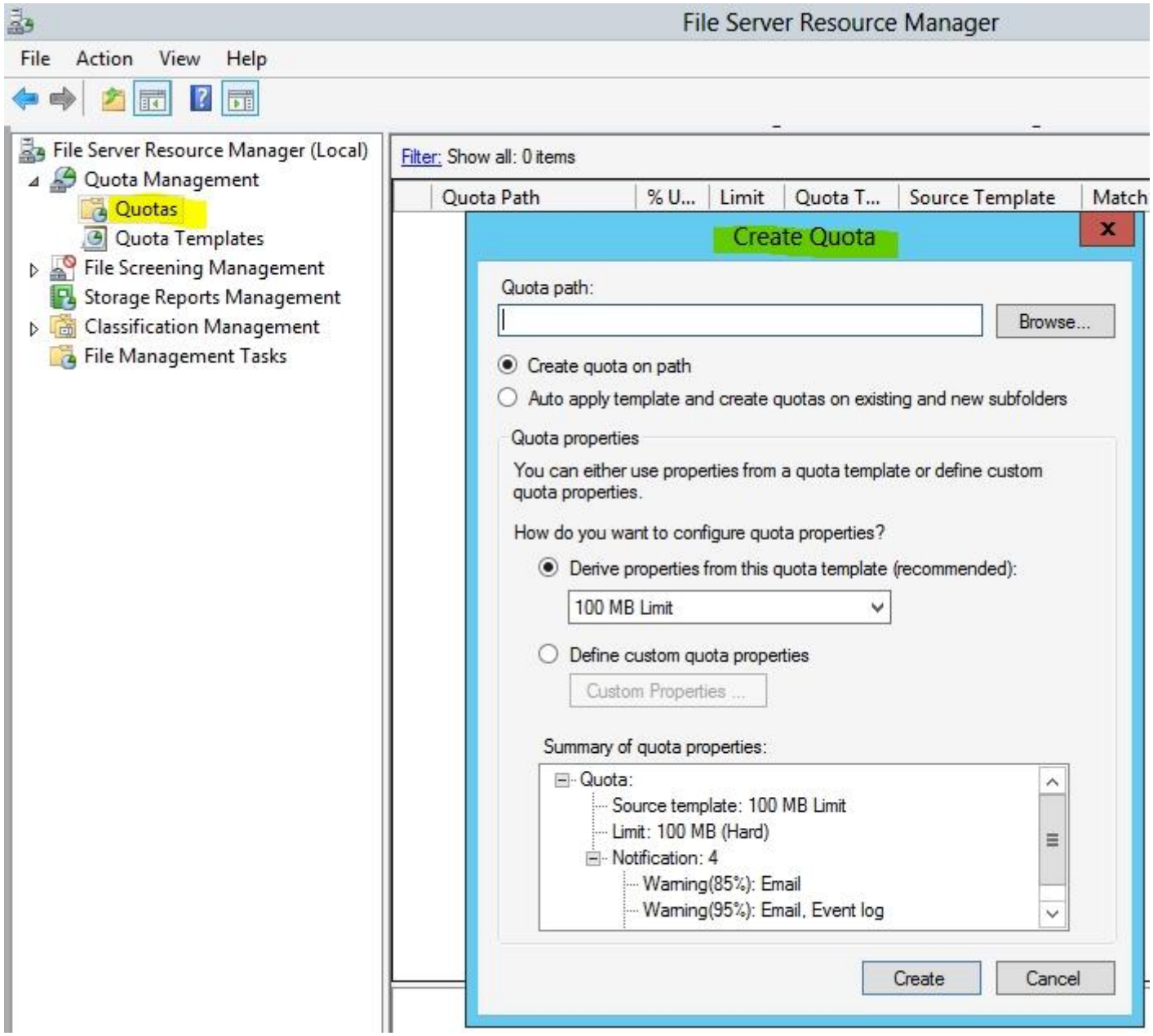


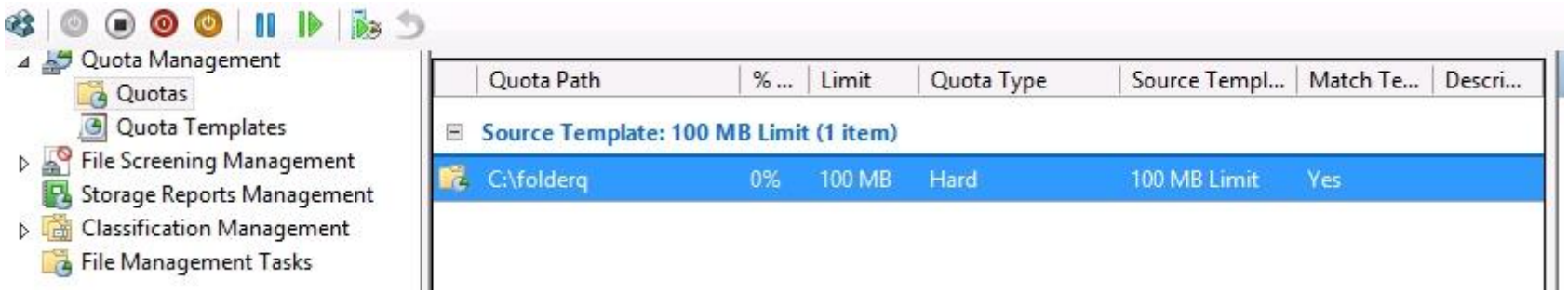
A. From File Server Resource Manager, edit the existing quota.
B. From the properties of drive D, enable quota management.
C. From the Services console, set the Startup Type of the Optimize drives service to Automatic.
D. From File Server Resource Manager, create a new quota.

Correct Answer: D
Section: Configure file and print services
Explanation

Explanation/Reference:
Create a new **Quota on path**, without using the auto apply template and create quota on existing and new subfolders.

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


File Server Resource Manager
File Action View Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
File Screening Management
Storage Reports Management
Classification Management
File Management Tasks
Filter: Show all: 0 items
Quota Path
% U...
Limit
Quota T...
Source Template
Match
Create Quota
Quota path:
Browse...
Create quota on path
Auto apply template and create quotas on existing and new subfolders
Quota properties
You can either use properties from a quota template or define custom quota properties.
How do you want to configure quota properties?
Derive properties from this quota template (recommended):
100 MB Limit
Define custom quota properties
Custom Properties ...
Summary of quota properties:
Quota:
Source template: 100 MB Limit
Limit: 100 MB (Hard)
Notification: 4
Warning(85%): Email
Warning(95%): Email, Event log
Create
Cancel



QUESTION 62
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012.
The domain contains an organizational unit (OU) named FileServers_OU. FileServers_OU contains the computer accounts for all of the file servers in the domain.
You need to audit the users who successfully access shares on the file servers.

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

Hot Area:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Correct Answer:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Section: Configure file and print services

Explanation

Explanation/Reference:
Notes:
To audit object accesses, enable auditing of the object access event category by following the steps above. Then, enable auditing on the specific object. For information about how to enable auditing on an object, see "Apply or modify auditing policy settings for a local file or folder" or "Apply or modify auditing policy settings for an object using Group Policy" in Related Topics.
After your audit policy is configured, events will be recorded in the security log. Open the security log to view these events. For information about the security log, see "Use the security log" in Related Topics.
The default auditing policy setting for domain controllers is No Auditing. This means that even if auditing is enabled in the domain, the domain controllers do not inherit auditing policy locally. If you want domain auditing policy to apply to domain controllers, you must modify this policy setting.
http://technet.microsoft.com/en-us/library/cc787268%28v=ws.10%29.aspx

QUESTION 63
Your network contains an Active Directory domain named contoso.com. The domain does not contain a certification authority (CA).
All servers run Windows Server 2012.
All client computers run Windows 8.
You need to add a data recovery agent for the Encrypting File System (EFS) to the domain.

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

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

Correct Answer: AC
Section: Configure file and print services
Explanation

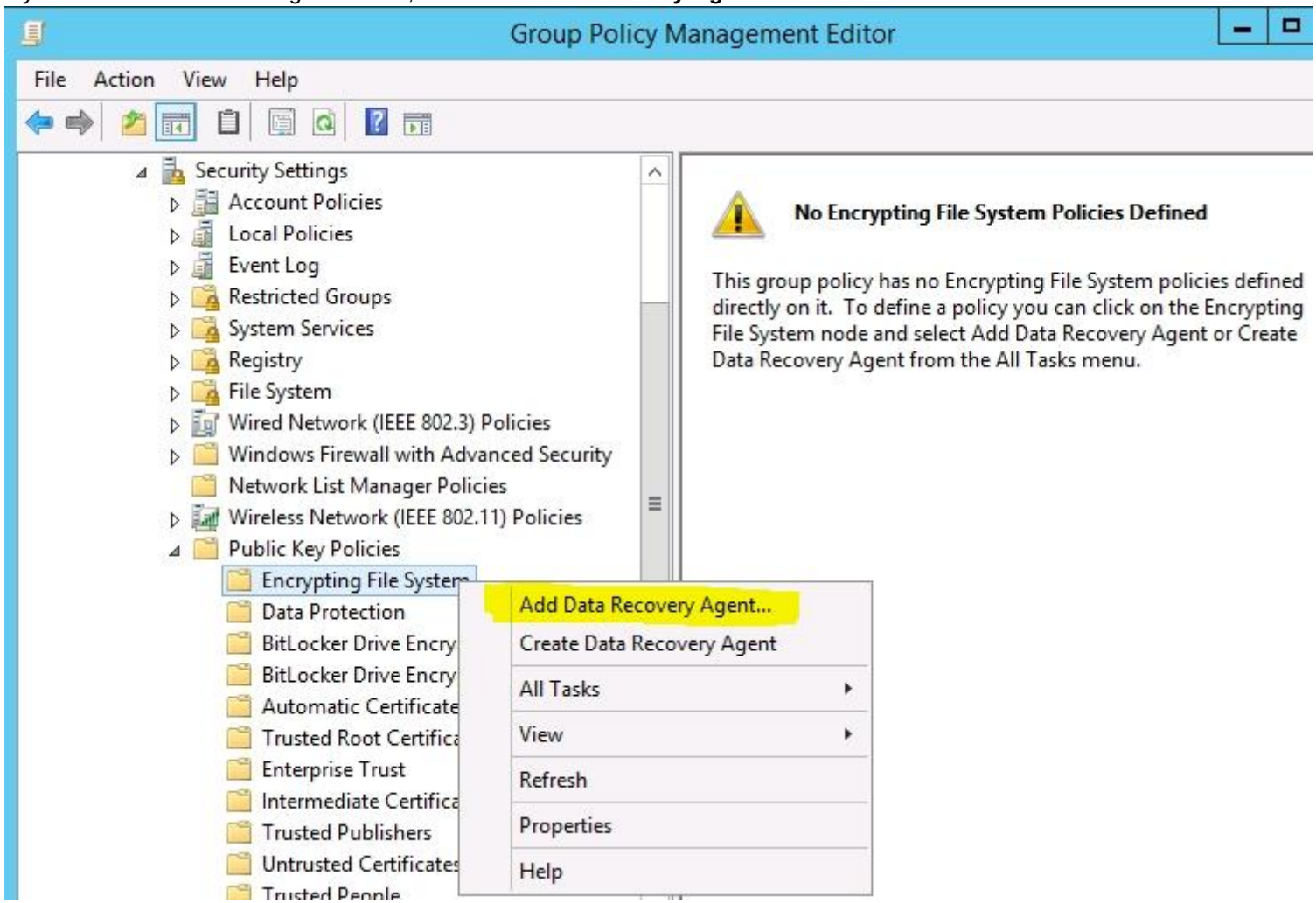
Explanation/Reference:
Get-Certificate - Submits a certificate request to an enrollment server and installs the response or retrieves a certificate for a previously submitted request.

A first note about preparation: before your users first encrypt a file, you should ask yourself where the users' encryption keys will come from. If you don't take any action at all, the encryption keys will be generated randomly by each user when they first encrypt a file, so that each user has a self-signed certificate and an associated private key. This is not ideal for many organizations, because these keys and certificates are decentralized and are difficult to administer and back up. A far better solution is to create a Windows enterprise certification authority (CA) in your domain, and to configure certificate templates for EFS certificates, along with an auto-enrollment policy. Auto-enrolled certificates allow for centralized management of users' certificates, along with the possibility of private key archival,

which reduces the reliance on data recovery agents as your sole point of recovery.

If you need to create a certificate to use as the Encrypting File System (EFS) recovery certificate, right-click Encrypting File System and click Create Data Recovery Agent.

If you want to use an existing certificate, click **Add Data Recovery Agent**.



Before changing the recovery policy in any way, you should first back up the recovery keys to a floppy disk ;)

http://technet.microsoft.com/en-us/library/cc776181%28v=ws.10%29.aspx
http://support.microsoft.com/kb/315672/en-us
http://support.microsoft.com/kb/298009/en-us
http://technet.microsoft.com/en-us/library/cc512680.aspx
http://technet.microsoft.com/en-us/library/cc778448(v=ws.10).aspx

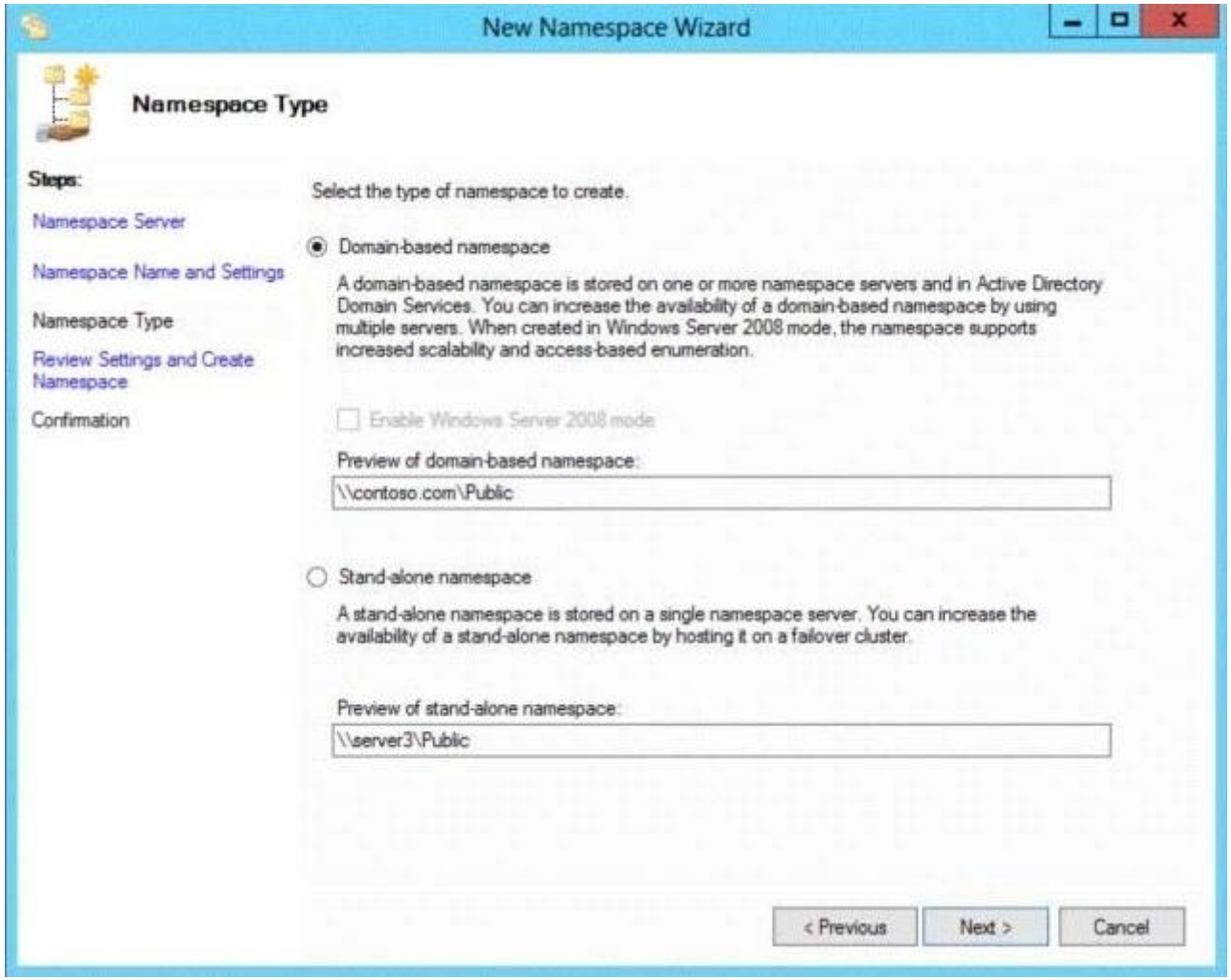
QUESTION 64
Your network contains an Active Directory domain named contoso.com. The domain contains three domain controllers. The domain controllers are configured as shown in the following table.

Domain controller name	Operating system	Operations master role
Server1	Windows Server 2008 R2	PDC emulator Infrastructure master
Server2	Windows Server 2008 R2	RID master
Server3	Windows Server 2012	Schema master

You are creating a Distributed File System (DFS) namespace as shown in the exhibit. (Click the Exhibit button.)
You need to identify which configuration prevents you from creating a DFS namespace in Windows Server 2008 mode.

Which configuration should you identify?

Exhibit:



A. The location of the PDC emulator role
B. The functional level of the domain
C. The operating system on Server1 and Server3
D. The location of the RID master role

Correct Answer: B

Section: Configure file and print services
Explanation

Explanation/Reference:
If you use a domain-based namespace, you may have to choose one of the following namespace modes:
1. Windows 2000 Server mode
2. Windows Server 2008 mode

In addition, in order to use the Windows Server 2008 mode for the DFS namespace, there are some prerequisites for the domain to use Windows Server 2008 mode namespace.
Prerequisites:
1. The domain uses the Windows Server 2008 domain functional level.
2. All namespace servers are running Windows Server 2008.

DFS in Windows Server 2008 has been improved. The DFSR, a service running in Windows Server 2008, can now be used to replicate SYSVOL contents. Previously, we had to use FRS for SYSVOL.
In Windows Server 2008, the DFS has the following new features added:
- DFS in Windows Server 2008 boasts a number of improvements. Access-based enumeration and cluster support is just the beginning
- Access-Based Enumeration: This feature allows users to see only files and folders on a file server that they have permission to access. This is not enabled by default, and it is supported only when any of the following conditions meet:

A namespace server is a domain controller or member server that hosts a namespace. The number of namespaces you can host on a server is determined by the operating system running on the namespace server.
Migrate the following domain-based namespace from Windows 2000 Server mode to Windows Server 2008 mode.

http://technet.microsoft.com/en-us/library/ff633469(v=WS.10).aspx
http://technet.microsoft.com/en-us/library/cc753448.aspx

QUESTION 65
Your network contains an Active Directory domain named adatum.com. The domain contains five servers.
The servers are configured as shown in the following table.

Server name	Configuration
DC1	Domain controller and DNS server
DC2	Domain controller and DHCP server
Server1	Windows Deployment Services (WDS)
Server2	Certification authority (CA)
Server3	File server

All desktop computers in adatum.com run Windows 8 and are configured to use BitLocker Drive Encryption (BitLocker) on all local disk drives.
You need to deploy the Network Unlock feature.
The solution must minimize the number of features and server roles installed on the network.

To which server should you deploy the feature?

A. Server3
B. Server1
C. DC2
D. Server2
E. DC1

Correct Answer: B
Section: Configure file and print services
Explanation

Explanation/Reference:
Windows 8 and Windows Server 2012 has added a new BitLocker protector option for operating system volumes called Network Unlock. Network Unlock enables easier management for BitLocker enabled desktops and servers in a domain environment by providing automatic unlock of operating system volumes at system reboot when connected to a wired corporate network. This feature requires the client hardware to have a DHCP driver implemented in its UEFI firmware.

Without Network Unlock, operating system volumes protected by TPM+PIN protectors require a PIN to be entered when a machine reboots or resumes from hibernation (for example, by Wake on LAN). This can make it difficult to enterprises to roll out software patches to unattended desktops and remotely administered

servers.

Network Unlock allows BitLocker-enabled systems with TPM+PIN and that meet the hardware requirements to boot into Windows without user intervention. Network Unlock works in a similar fashion to the TPM+StartupKey at boot. Rather than needing to read the StartupKey from USB media, however, the key for Network Unlock is composed from a key stored in the TPM and an encrypted network key that is sent to the server, decrypted and returned to the client in a secure session.

The **BitLocker-NetworkUnlock feature must be installed on a Windows Deployment Server** (which does not have to be configured--the WDSServer service just needs to be running).

Network Unlock Core requirements

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

- Computers running Windows 8 or Windows Server 2012 with UEFI DHCP drivers can be Network Unlock clients.
- BitLocker Network Unlock optional feature installed on Windows Server 2012.
- A separate Windows Server 2012 server running the Windows Deployment Services (WDS) role.
- A DHCP server, separate from the WDS server.
- Properly configured public/private key pairing.
- Network Unlock Group Policy settings configured.

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

QUESTION 66
You have a server named Server1 that runs Windows Server 2012. Server1 has the File Server Resource Manager role service installed.
Server1 has a folder named Folder1 that is used by the sales department.
You need to ensure that an email notification is sent to the sales manager when a File Screening Audit report is generated.

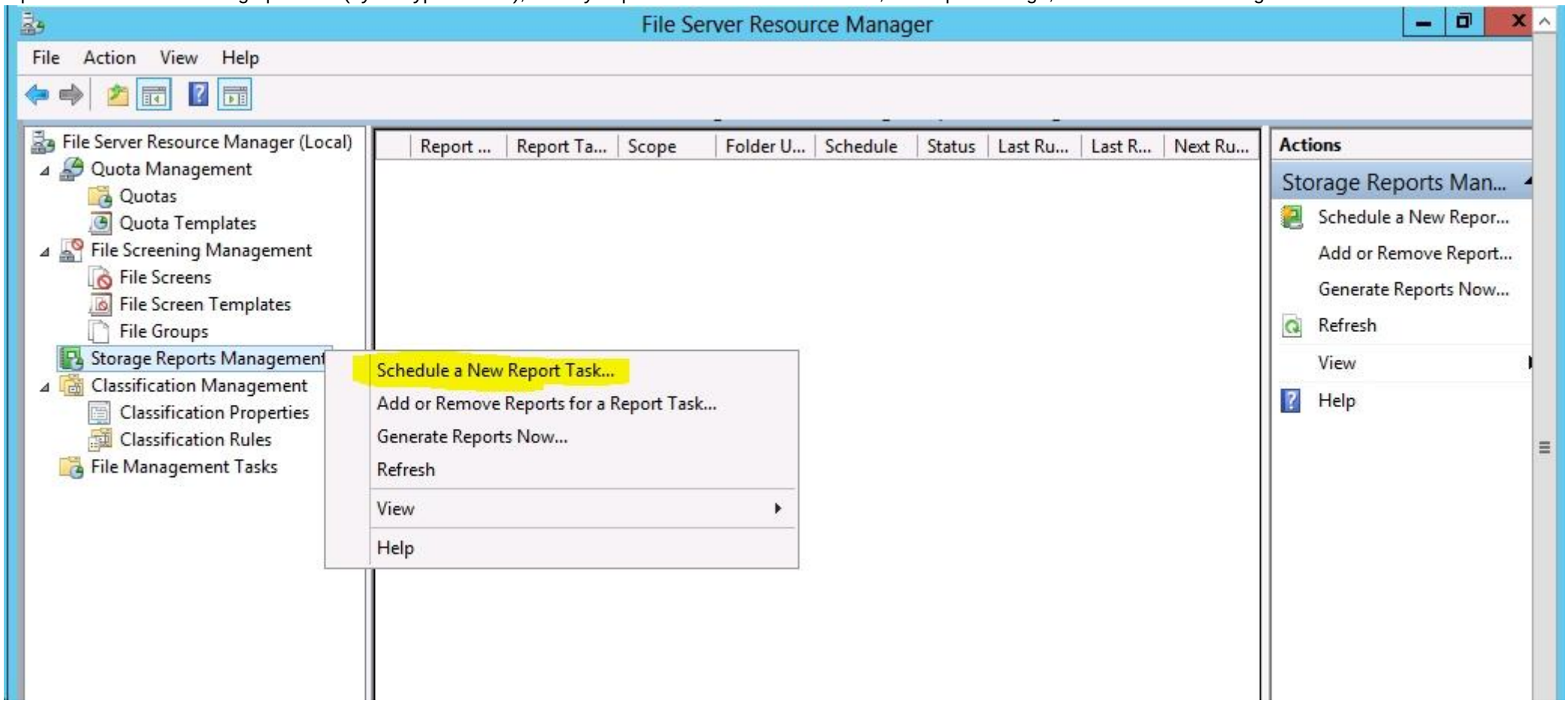
What should you configure on Server1?

A. A file screen exception
B. A file group

C. A storage report task
D. A file screen

Correct Answer: C
Section: Configure file and print services
Explanation

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



Before you run a File Screen Audit report, in the File Server Resource Manager Options dialog box, on the File Screen Audit tab, verify that the Record file screening activity in the auditing database check box is selected.
http://technet.microsoft.com/en-us/library/cc755988.aspx

QUESTION 67
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers run Windows Server 2012.
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.

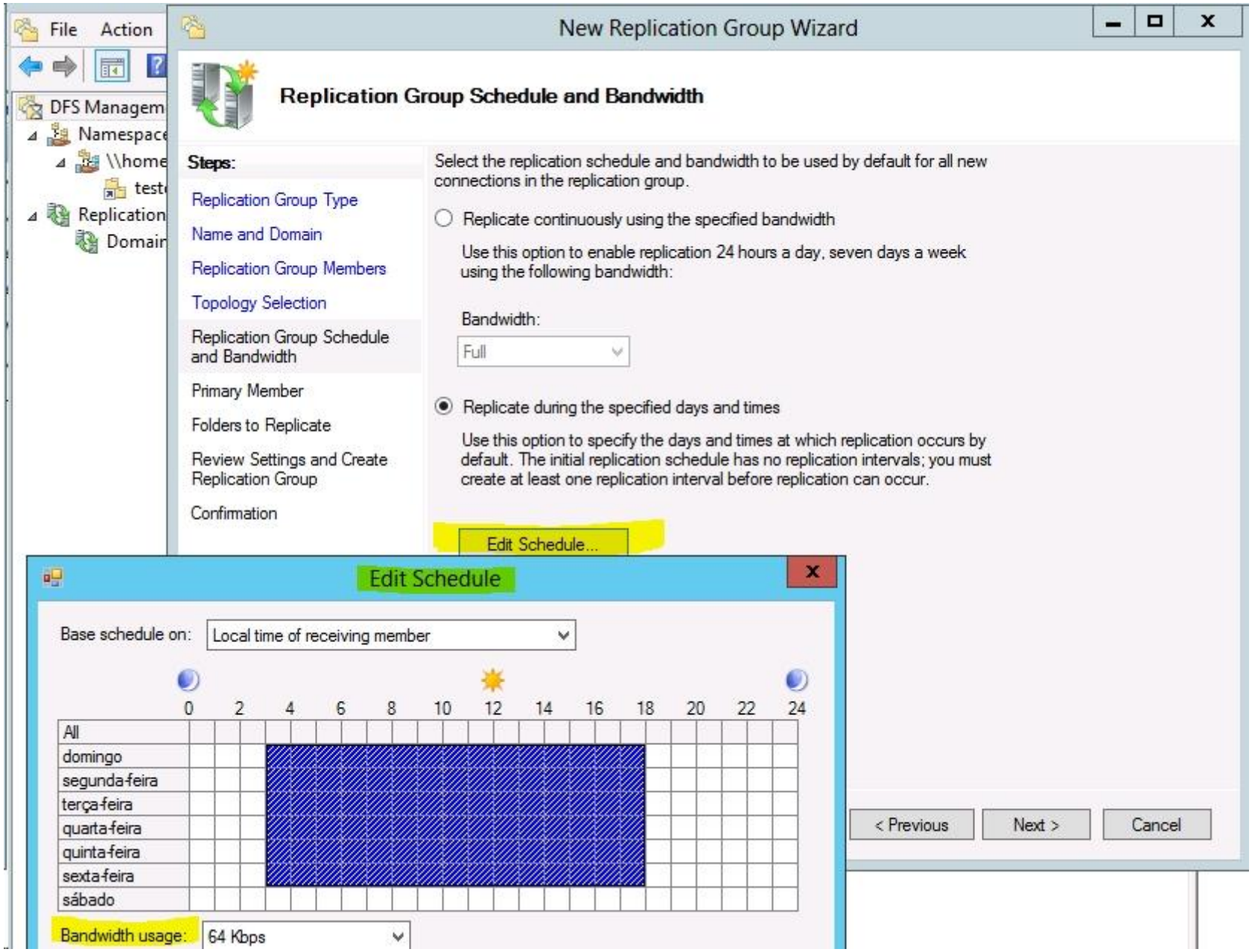
What should you modify?

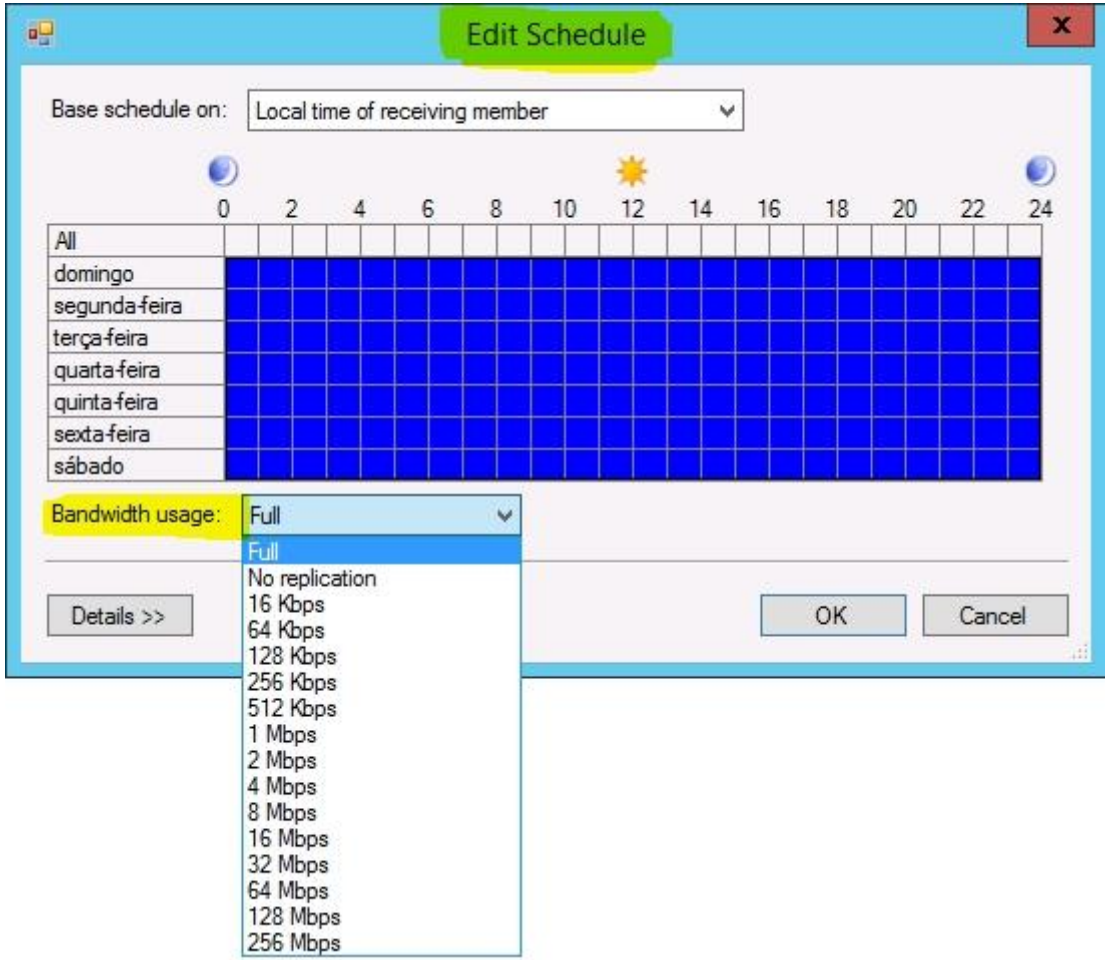
A. The cache duration of the namespace
B. The staging quota of the replicated folder
C. The referral ordering of the namespace
D. The schedule of the replication group

Correct Answer: D
Section: Configure file and print services
Explanation

Explanation/Reference:
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.
http://technet.microsoft.com/library/cc773238%28WS.10%29.aspx#BKMK_024

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.


File Action
DFS Managem
Namespace
\\home
test
Replication
Domain
New Replication Group Wizard
Replication Group Schedule and Bandwidth
Steps:
Replication Group Type
Name and Domain
Replication Group Members
Topology Selection
Replication Group Schedule and Bandwidth
Primary Member
Folders to Replicate
Review Settings and Create Replication Group
Confirmation
Select the replication schedule and bandwidth to be used by default for all new connections in the replication group.
Replicate continuously using the specified bandwidth
Use this option to enable replication 24 hours a day, seven days a week using the following bandwidth:
Bandwidth:
Full
Replicate during the specified days and times
Use this option to specify the days and times at which replication occurs by default. The initial replication schedule has no replication intervals; you must create at least one replication interval before replication can occur.
Edit Schedule...
< Previous
Next >
Cancel
Edit Schedule
Base schedule on:
Local time of receiving member
0 2 4 6 8 10 12 14 16 18 20 22 24
All
domingo
segunda-feira
terça-feira
quarta-feira
quinta-feira
sexta-feira
sábado
Bandwidth usage:
64 Kbps



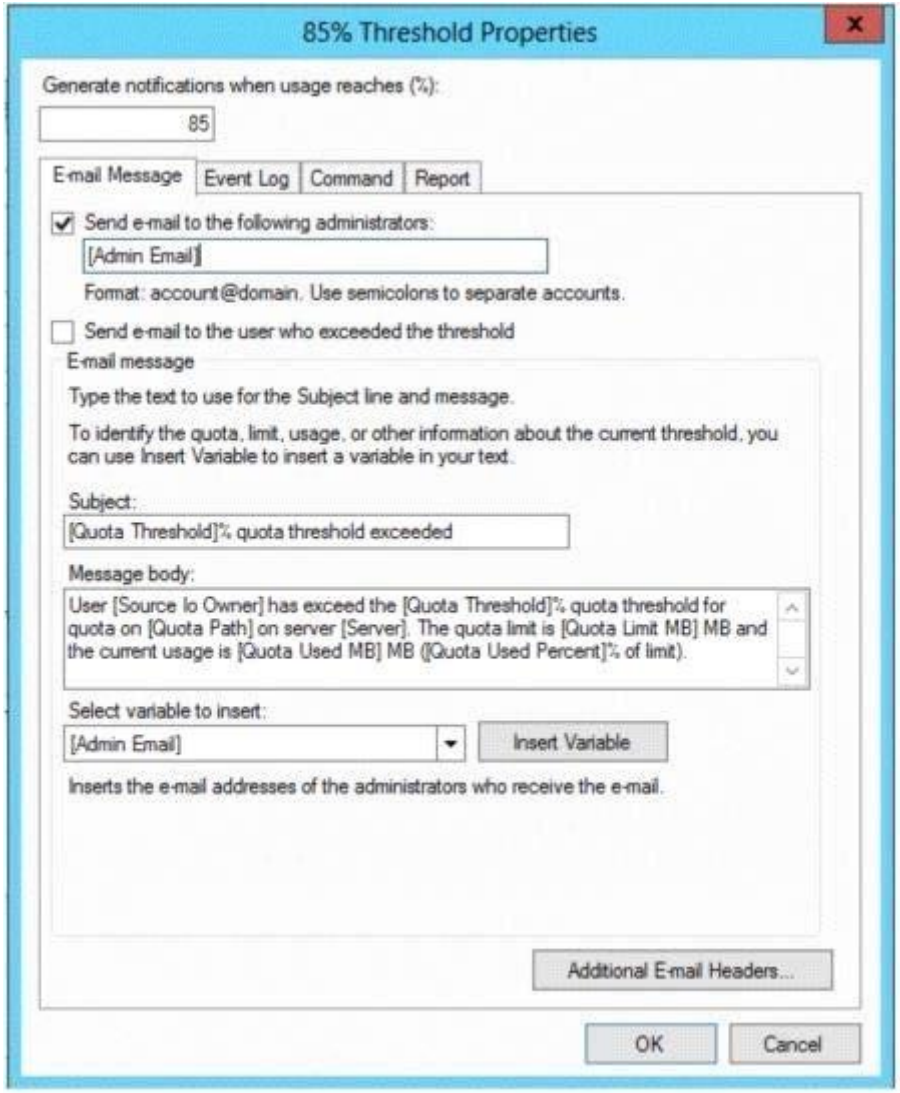
http://technet.microsoft.com/en-us/library/cc732278.aspx

QUESTION 68

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012. Server1 has the File Server Resource Manager role service installed. You configure a quota threshold as shown in the exhibit. (Click the Exhibit button.) You need to ensure that a user named User1 receives an email notification when the threshold is exceeded.

What should you do?

Exhibit:

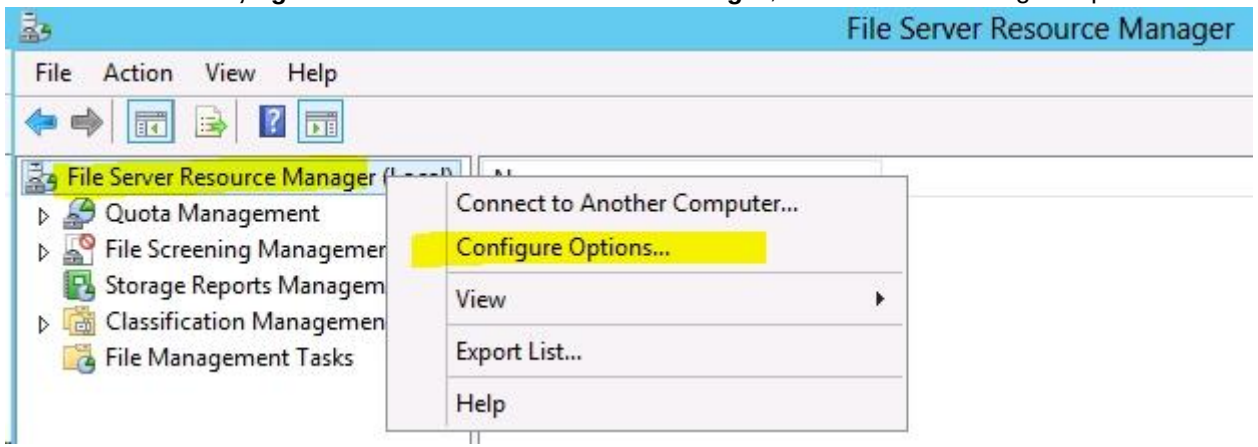


A. Configure the File Server Resource Manager Options.
B. Modify the members of the Performance Log Users group.

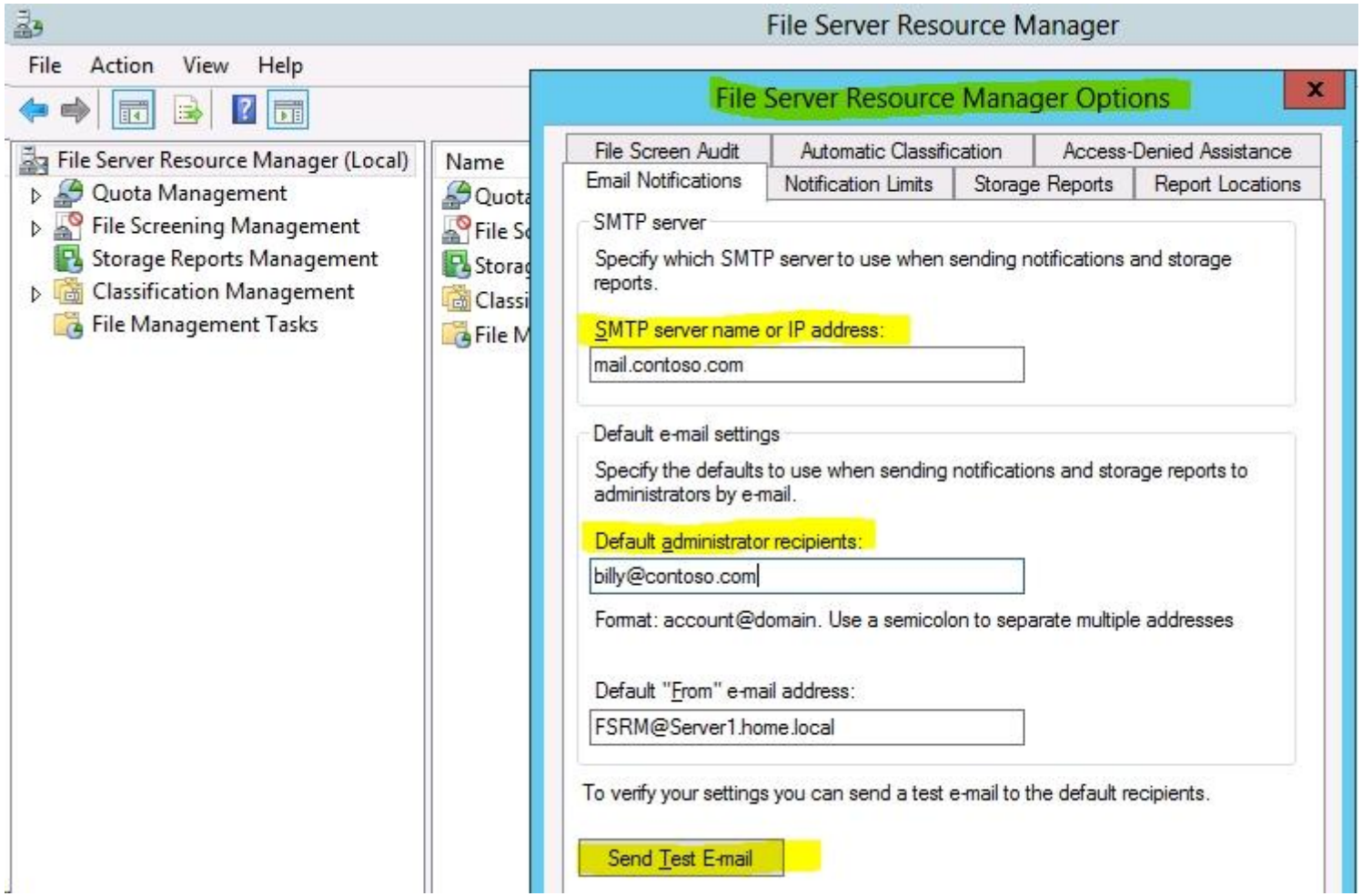
C. Create a performance counter alert.
D. Create a classification rule.

Correct Answer: A
Section: Configure file and print services
Explanation

Explanation/Reference:
When you create quotas and file screens, you have the option of sending e-mail notifications to users when their quota limit is approaching or after they have attempted to save files that have been blocked. If you want to routinely notify certain administrators of quota and file screening events, you can configure one or more default recipients.
To send these notifications, you must specify the SMTP server to be used for forwarding the e-mail messages.
To configure e-mail options
In the console tree, right-click File Server Resource Manager, and then click Configure options. The File Server Resource Manager Options dialog box opens.



On the E-mail Notifications tab, under SMTP server name or IP address, type the host name or the IP address of the SMTP server that will forward e-mail notifications.
If you want to routinely notify certain administrators of quota or file screening events, under Default administrator recipients, type each e-mail address.
Use the format account@domain. Use semicolons to separate multiple accounts.
To test your settings, click Send Test E-mail.



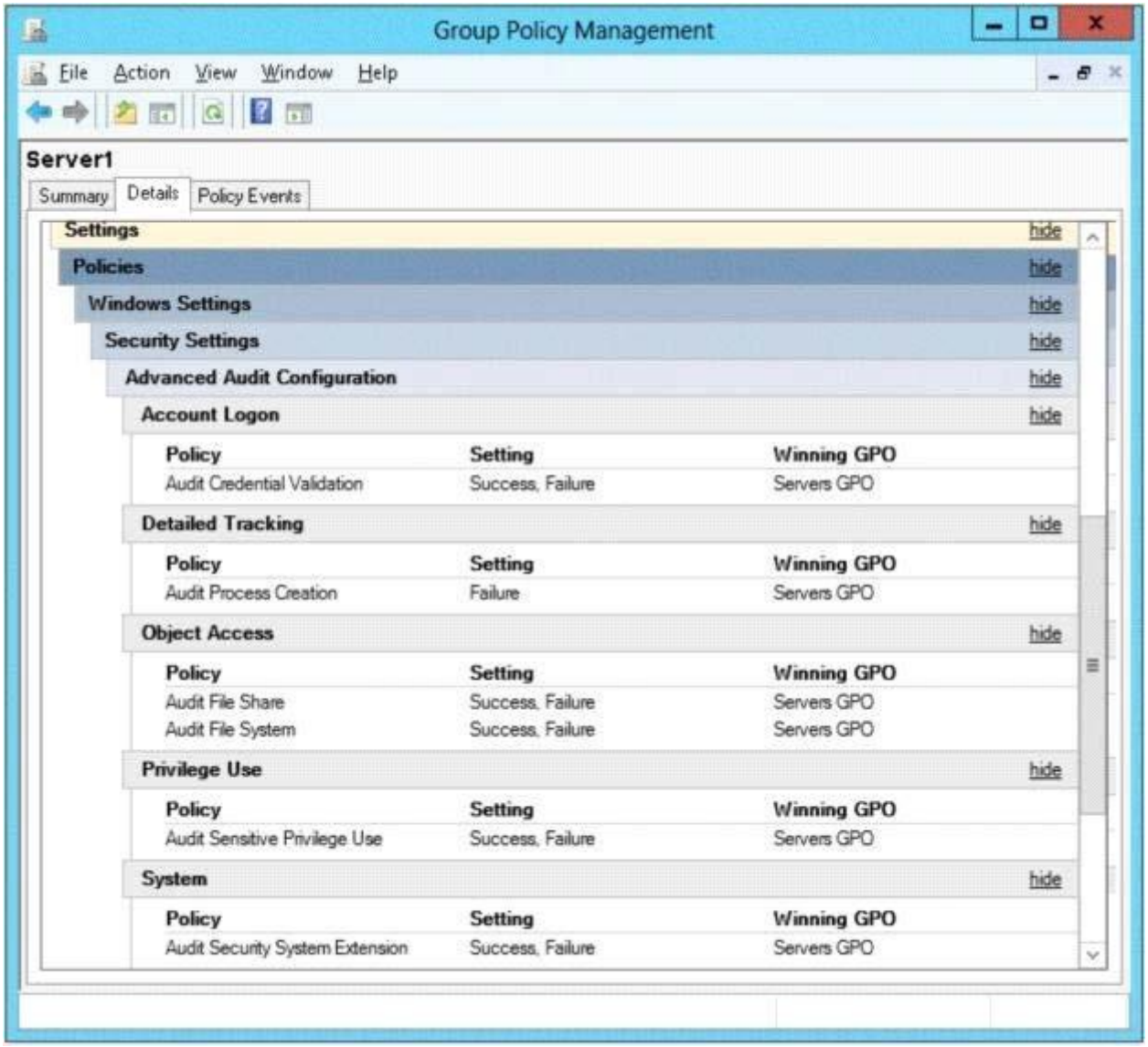
http://technet.microsoft.com/en-us/library/cc756031(v=ws.10).aspx

QUESTION 69

Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2012.
You view the effective policy settings of Server1 as shown in the exhibit. (Click the Exhibit button.)
On Server1, you have a folder named C:\Share1 that is shared as Share1. Share1 contains confidential data. A group named Group1 has full control of the content in Share1.
You need to ensure that an entry is added to the event log whenever a member of Group1 deletes a file in Share1.

What should you configure?

Exhibit:



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

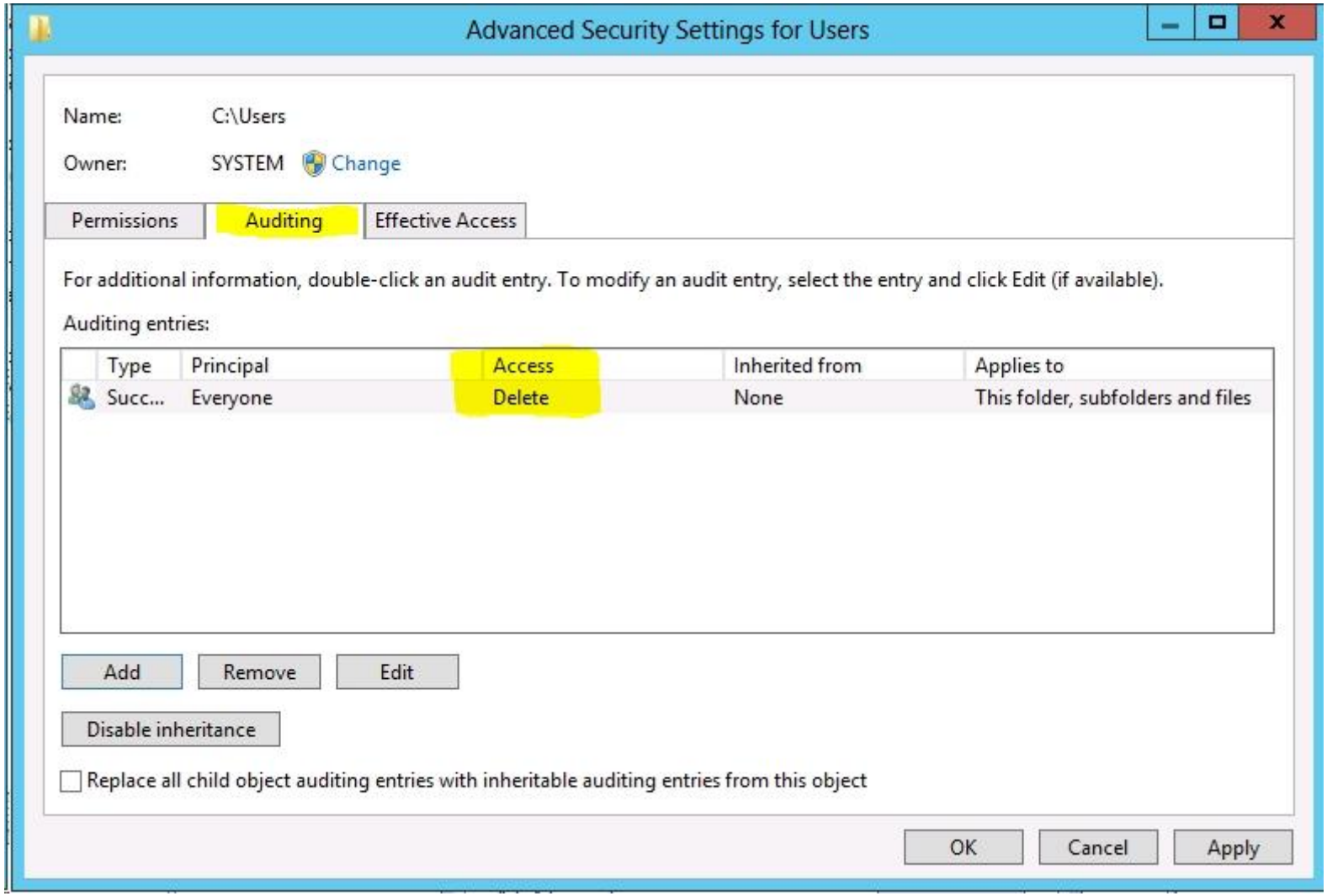
Correct Answer: C
Section: Configure file and print services
Explanation

Explanation/Reference:
You can use Computer Management to track all connections to shared resources on a Windows Server 2008 R2 system.
Whenever a user or computer connects to a shared resource, Windows Server 2008 R2 lists a connection in the Sessions node.

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

To view connections to shared resources, type net session at a command prompt or follow these steps:
1. In Computer Management, connect to the computer on which you created the shared resource.
2. In the console tree, expand System Tools, expand Shared Folders, and then select Sessions. You can now view connections to shares for users and computers.

To enable folder permission auditing, you can follow the below steps:
1. Click start and run "secpol.msc" without quotes.
2. Open the Local Policies\Audit Policy
3. Enable the Audit object access for "Success" and "Failure".
4. Go to target files and folders, right click the folder and select properties.
5. **Go to Security Page and click Advanced**.
6. Click Auditing and Edit.
7. Click add, type everyone in the Select User, Computer, or Group.
8. Choose Apply onto: This folder, subfolders and files.
9. Tick on the box “Change permissions”
10. Click OK.



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

http://social.technet.microsoft.com/Forums/en-US/winservergen/thread/13779c78-0c73-4477-8014-f2eb10f3f10f/
http://support.microsoft.com/kb/300549
http://www.windowsitpro.com/article/permissions/auditing-folder-permission-changes
http://www.windowsitpro.com/article/permissions/auditing-permission-changes-on-a-folder

QUESTION 70
You have a server named Server1 that runs Windows Server 2012. Server1 has the File Server Resource Manager role service installed.
Server1 has a folder named Folder1 that is used by the human resources department.
You need to ensure that an email notification is sent immediately to the human resources manager when a user copies an audio file or a video file to Folder1.

What should you configure on Server1?

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

Correct Answer: A
Section: Configure file and print services
Explanation

Explanation/Reference:
http://technet.microsoft.com/en-us/library/cc732349%28v=ws.10%29.aspx#BKMK_CreateFS
A) With File Server Resource Manager (FSRM) you can create file screens that prevent users from saving unauthorized files on volumes or folders.
File Screen Enforcement:
You can create file screens to prevent users from saving unauthorized files on volumes or folders. There are two types of file screen enforcement: active and passive enforcement. Active file screen enforcement does not allow the user to save an unauthorized file. Passive file screen enforcement **allows the user to save the file, but notifies the user that the file is not an authorized file. You can configure notifications, such as events logged to the event log or e-mails sent to users and administrators**, as part of active and passive file screen enforcement.
http://technet.microsoft.com/en-us/library/cc734419%28v=ws.10%29.aspx

B) Occasionally, you need to allow exceptions to file screening. For example, you might want to block video files from a file server, but you need to allow your training group to save the video files for their computer-based training. To allow files that other file screens are blocking, create a file screen exception.
A file screen exception is a special type of file screen that overrides any file screening that would otherwise apply to a folder and all its subfolders in a designated exception path. That is, it creates an exception to any rules derived from a parent folder.
You cannot create a file screen exception on a parent folder where a file screen is already defined. You must assign the exception to a subfolder or make changes to the existing file screen.
http://technet.microsoft.com/en-us/library/cc730822.aspx

C) A file group is used to define a namespace for a file screen, file screen exception, or Files by File Group storage report.
It consists of a set of file name patterns, which are grouped by the following:
- Files to include: files that belong in the group
- Files to exclude: files that do not belong in the group

For convenience, you can create and edit file groups while you edit the properties of file screens, file screen exceptions, file screen templates, and Files by File

Group reports. Any file group changes that you make from these property sheets are not limited to the current item that you are working on. http://technet.microsoft.com/en-us/library/cc770594.aspx

D) On the Storage Reports Management node of the File Server Resource Manager MMC snap-in, you can perform the following tasks:
- Schedule periodic storage reports that allow you to identify trends in disk usage.
- Monitor attempts to save unauthorized files for all users or a selected group of users.
- Generate storage reports instantly.

To set e-mail notifications and certain reporting capabilities, you must first configure the general File Server Resource Manager options.
To configure e-mail options
- In the console tree, right-click File Server Resource Manager, and then click Configure Options. The File Server Resource Manager Options dialog box opens.
- On the E-mail Notifications tab, under SMTP server name or IP address, type the host name or the IP address of the SMTP server that will forward e-mail notifications and storage reports.
- If you want to routinely notify certain administrators about quota or file screening events or e-mail storage reports, under Default administrator recipients, type each e-mail address.
- Use the format account@domain. Use semicolons to separate multiple accounts.
- To specify a different "From" address for e-mail notifications and storage reports sent from File Server Resource Manager, under Default "From" e-mail address, type the e-mail address that you want to appear in your message.
- To test your settings, click Send Test E-mail.
- Click OK.

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

QUESTION 71
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. Both servers have the File and Storage Services server role, the DFS Namespace role service, and the DFS Replication role service installed.

Server1 and Server2 are part of a Distributed File System (DFS) Replication group named Group1. Server1 and Server2 are connected by using a high-speed LAN connection.

You need to minimize the amount of processor resources consumed by DFS Replication.

What should you do?

A. Reduce the bandwidth usage.
B. Disable Remote Differential Compression (RDC).
C. Modify the staging quota.
D. Modify the replication schedule.

Correct Answer: B
Section: Configure file and print services
Explanation

Explanation/Reference:
B.
Because disabling RDC can help conserve disk input/output (I/O) and CPU resources, ***you might want to disable RDC on a connection if the sending and receiving members are in a local area network (LAN)***, ***and bandwidth use is not a concern***. However, in a LAN environment where bandwidth is contended, RDC can be beneficial when transferring large files.
Question tells it uses a high-speed LAN connection.
http://technet.microsoft.com/en-us/library/cc758825%28v=ws.10%29.aspx

C.
DFS Replication uses staging folders for each replicated folder to act as caches for new and changed files that are ready to be replicated from sending members to receiving members. These files are stored under the local path of the replicated folder in the DfsrPrivate\Staging folder.
If a staging folder quota is too small, DFS Replication might consume additional CPU and disk resources, and replication might slow down or even stop.
By default, the quota size of each staging folder is 4,096 MB, and the quota size of each Conflict and Deleted folder is 660 MB. The size of each folder on a member is cumulative per volume, so if there are multiple replicated folders on a member, DFS Replication creates multiple staging and Conflict and Deleted folders, each with its own quota.
Question doesn't tell replication might slow down or even stop.
http://technet.microsoft.com/en-us/library/cc754229.aspx

QUESTION 72
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.

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

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

You implement a Distributed File System (DFS) replication group named ReplGroup.

ReplGroup is used to replicate a folder on each file server. ReplGroup uses a hub and spoke topology. NYC-SVR1 is configured as the hub server.

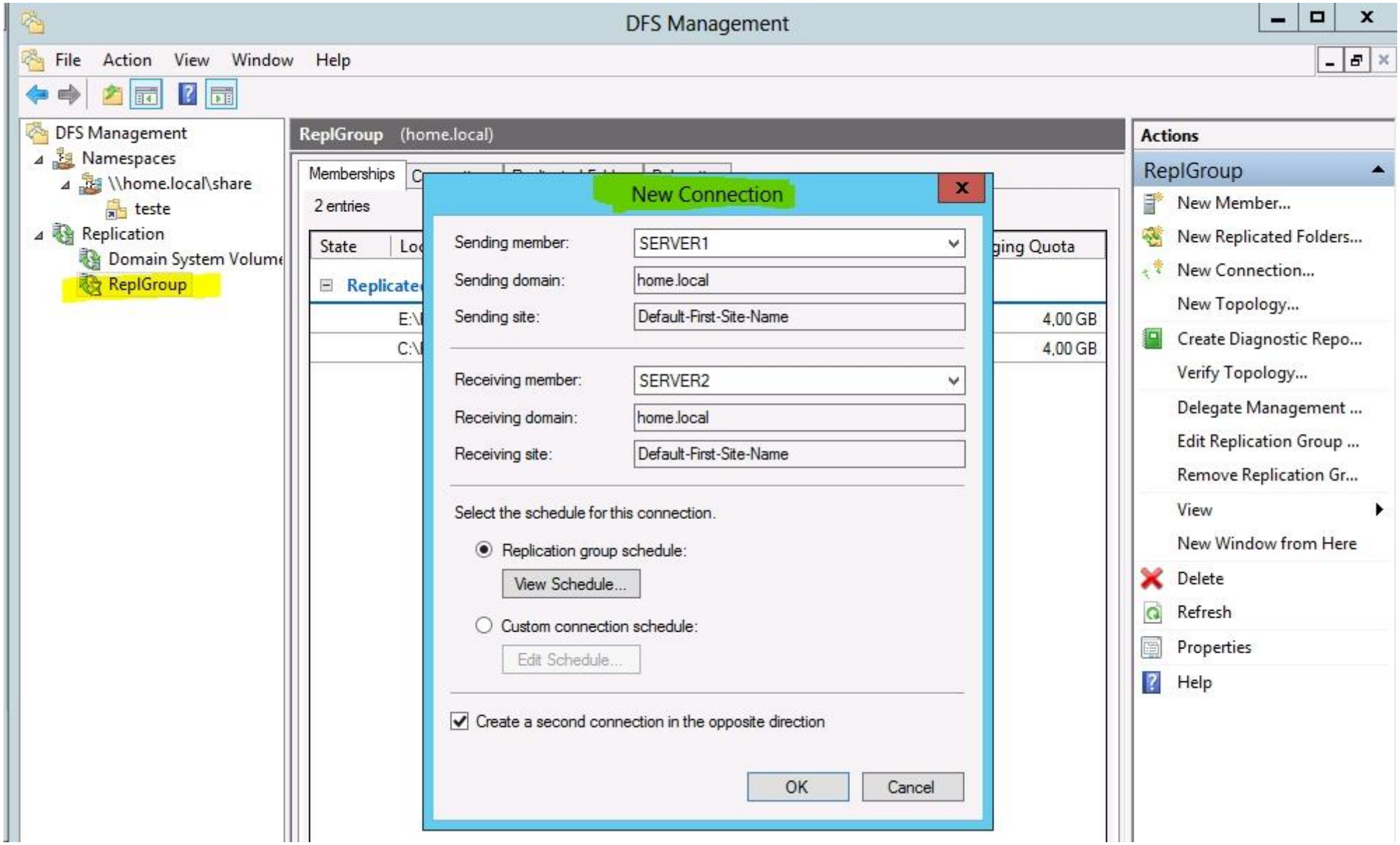
You need to ensure that replication can occur if NYC-SVR1 fails.

What should you do?

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

Correct Answer: D
Section: Configure file and print services
Explanation

Explanation/Reference:



http://faultbucket.ca/2012/08/fixing-a-dfsr-connection-problem/
http://technet.microsoft.com/en-us/library/cc771941.aspx

QUESTION 73
Your domain has contains a Windows 8 computer name Computer1 using BitLocker. The E:\ drive is encrypted and currently locked.

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

What should you run?

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

Correct Answer: A
Section: Configure file and print services
Explanation

Explanation/Reference:
Unlock-BitLocker - Restores access to data on a BitLocker volume.
The Unlock-BitLocker cmdlet restores access to encrypted data on a volume that uses BitLocker Drive Encryption.

http://technet.microsoft.com/en-us/library/jj649833(v=wps.620).aspx

QUESTION 74
Your network contains and active Directory domain named contoso.com. The doman contains a server named Server1 that runs Windows Server 2012
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 /category:"detailed tracking" /failure:enable
B. auditpol.exe /set /user:admin1 /failure:enable
C. auditpol.exe /resourcesacl /set /type:keyauditpol.exe /resourcesacl /set /type: /access:ga
D. auditpol.exe /resourcesacl /set /type:file /user:admin1 /failure

Correct Answer: D
Section: Configure file and print services
Explanation

Explanation/Reference:
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:

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:MYDOMAIN\myuser /success /failure /access:FRFW
```

```
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>]]
```

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

QUESTION 75
Your network contains and Active Directory domain named contoso.com.The domain contains a file server named server1 that runs windows Server 2012.
You view the effective policy settings of Server1 as shown in the exhibit.
You need to ensure that an entry is added to the event log whenever a local user account is created or deleted on Server1.
What should you do?

Exhibit:

Group Policy Management

File Action View Window Help

Server1

Summary | Details | Policy Events

Settings hide

Policies hide

Windows Settings hide

Security Settings hide

Local Policies/Audit Policy hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	Servers GPO
Audit account management	Failure	Servers GPO
Audit object access	Success, Failure	Servers GPO
Audit privilege use	Success, Failure	Servers GPO

Advanced Audit Configuration hide

Object Access hide

Policy	Setting	Winning GPO
Audit File Share	Success, Failure	Servers GPO
Audit File System	Success, Failure	Servers GPO

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

Correct Answer: A
Section: Configure file and print services
Explanation

Explanation/Reference:
When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. The following procedure shows how to prevent conflicts by blocking the application of any basic audit policy settings.
http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx#BKMK_step2

Enabling Advanced Audit Policy Configuration

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

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

Audit Policy settings
-Any changes to user account and resource permissions.
-Any failed attempts for user logon.
-Any failed attempts for resource access.
-Any modification to the system files.

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

-A group administrator has modified settings or data on servers that contain finance information.
-An employee within a defined group has accessed an important file.
-The correct system access control list (SACL) is applied to every file and folder or registry key on a computer or file share as a verifiable safeguard against undetected access.

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

http://blogs.technet.com/b/abizerh/archive/2010/05/27/tracing-down-user-and-computer-account-deletion-in-active-directory.aspx
http://technet.microsoft.com/en-us/library/dd772623%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/jj852202(v=ws.10).aspx
http://www.petri.co.il/enable-advanced-audit-policy-configuration-windows-server.htm
http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx

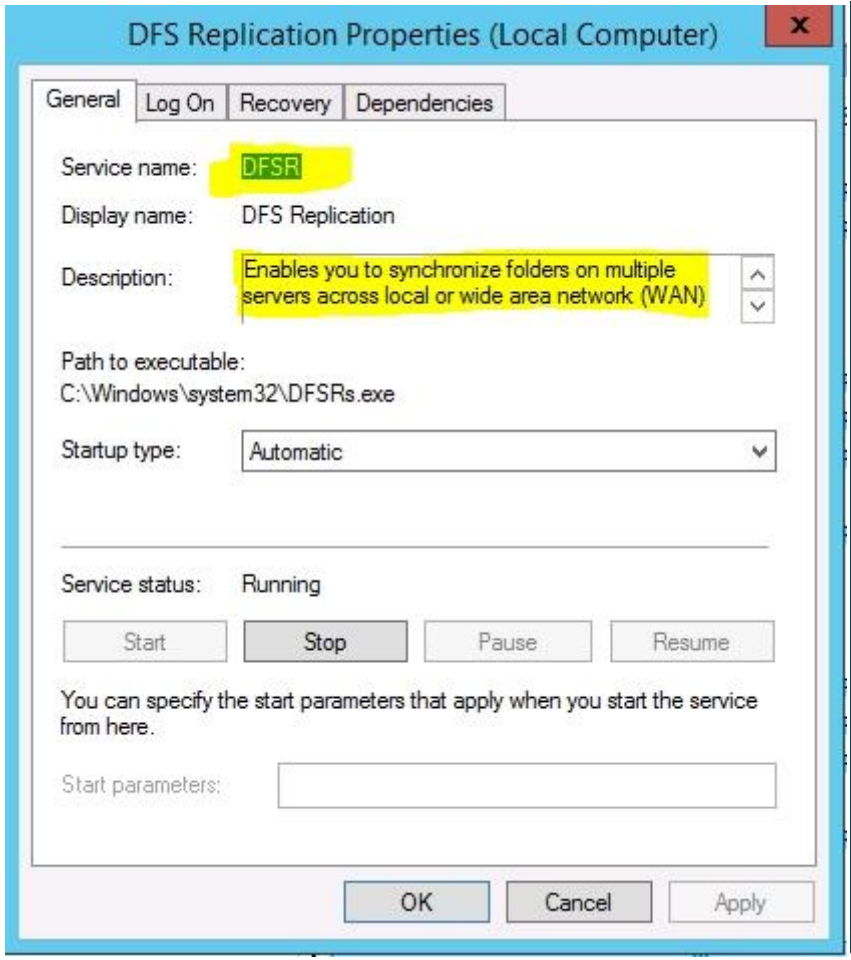
QUESTION 76
On the DFS replication your receive a wrap error on the sysvol on domain controller 4.
Which 3 steps should you do to recover this error in the correct order.

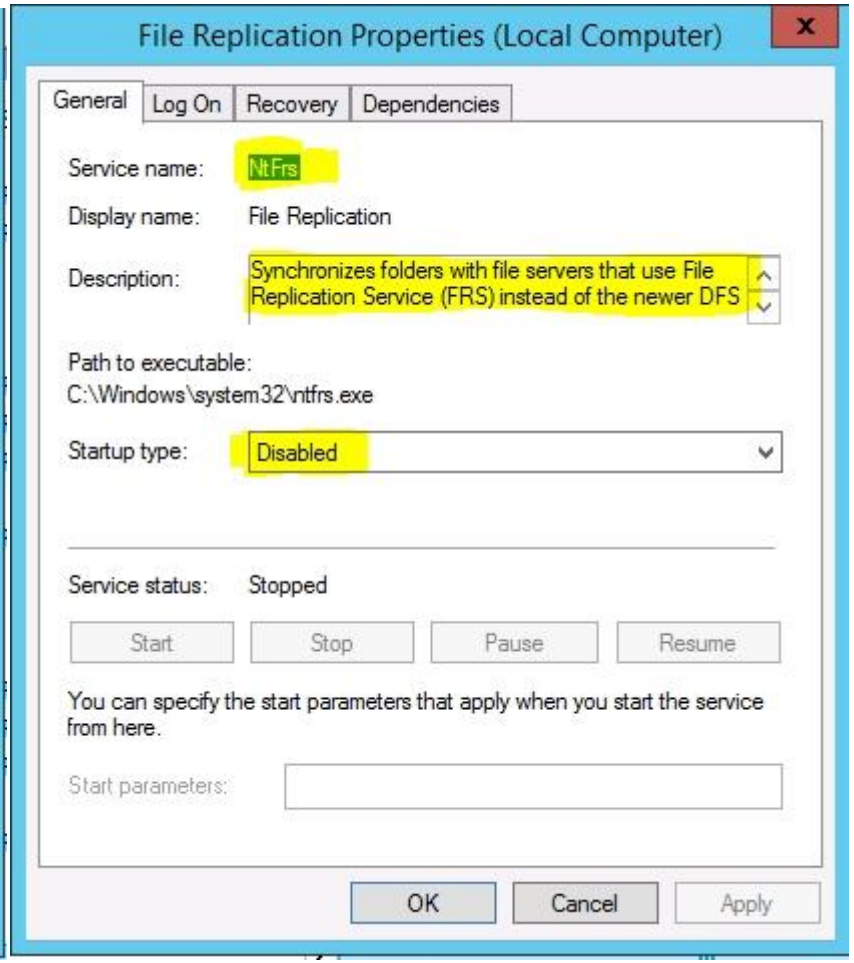
A. Stop FSR
B. Start FSR
C. Edit the computer object in AD
D. Edit the registry
E. Stop DFSR
F. Start DFRS

Correct Answer: DEF
Section: Configure file and print services
Explanation

Explanation/Reference:
http://technet.microsoft.com/pt-pt/library/dd640019%28v=ws.10%29.aspx

Domain controllers use a special shared folder named SYSVOL to replicate logon scripts and Group Policy object files to other domain controllers. Windows 2000 Server and Windows Server 2003 use File Replication Service (FRS) to replicate SYSVOL, whereas **Windows Server 2008 uses the newer DFS Replication service when in domains that use the Windows Server 2008 domain functional level**, and FRS for domains that run older domain functional levels. (if question doesn't tell functional level... I suppose it's 2012)





http://www.sysbiosis.com/blog/ntfrs-file-replication-service-journal-wrap-errors-on-domain-controller
Open the registry and navigate to “HKLM/System\CurrentControlSet\Services\NtFrs\Parameters” and there, create a new REG_DWORD key named “Enable Journal Wrap Automatic Restore” with value set to “1″. This will enable in the File Replication Service (once the service is restarted) the restoring procedure of the corrupted entities in the replica process.

Journal wrap errors occur if a sufficient number of changes that occur while FRS is turned off in such a way that the last USN change that FRS recorded during shutdown no longer exists in the USN journal during startup. The risk is that changes to files and folders for FRS replicated trees may have occurred while the

service was turned off, and no record of the change exists in the USN journal. To guard against data inconsistency, FRS asserts into a journal wrap state.

FRS is a service that must always be running on Windows domain controllers and members of FRS-replicated DFS sets.

If you increase the USN journal size, and therefore you increase the number of changes that the journal can hold before the journal "wraps," this reduces the possibility that the USN journal wrap will occur. The USN journal size can be changed by setting the following registry key:
HKLM\System\CCS\Services\NTFRS\Parameters\"Ntfs Journal size in MB" (REG_DWORD)
Valid settings range from 8 to 128 megabytes (MB). The default is 32 MB.

http://support.microsoft.com/kb/292438/en-us
http://blogs.technet.com/b/instan/archive/2009/07/14/what-happens-in-a-journal-wrap.aspx

QUESTION 77
Your network contains an Active Directory domain named contoso.com. The domain functional level is Windows Server 2008. All domain controllers run Windows Server 2008 R2.

The domain contains a file server named Server1 that runs Windows Server 2012.

Server1 has a BitLocker Drive Encryption (BitLocker)-encrypted drive. Server1 uses a Trusted Platform Module (TPM) chip.

You enable the Turn on TPM backup to Active Directory Domain Services policy setting by using a Group Policy object (GPO).

You need to ensure that you can back up the BitLocker recovery information to Active Directory.

What should you do?

A. Raise the forest functional level to Windows Server 2008 R2.
B. Enable the Configure the level of TPM owner authorization information available to the operating system policy setting and set the Operating system managed TPM authentication level to None.
C. Add a BitLocker data recovery agent.
D. Import the TpmSchemaExtension.ldf and TpmSchemaExtensionACLChanges.ldf schema extensions to the Active Directory schema.

Correct Answer: D
Section: Configure file and print services
Explanation

Explanation/Reference:
You can configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives and the Trusted Platform Module (TPM) to Active Directory Domain Services (AD DS). Recovery information includes the recovery password for each BitLocker-protected drive, the TPM owner password, and the information required to identify which computers and drives the recovery information applies to. Optionally, you can also save a package containing the actual keys used to encrypt the data as well as the recovery password required to access those keys.

Backing up recovery passwords for a BitLocker-protected drive allows administrators to recover the drive if it is locked. This ensures that encrypted data belonging to the enterprise can always be accessed by authorized users.

Backing up the TPM owner information for a computer allows administrators to locally and remotely configure the TPM security hardware on that computer. As an example, an administrator might want to reset the TPM to factory defaults when decommissioning or repurposing computers.

For Windows 8 a change to how the TPM owner authorization value is stored in AD DS was implemented in the AD DS schema.

The TPM owner authorization value is now stored in a separate object which is linked to the Computer object. This value was stored as a property in the Computer object itself for the default Windows Server 2008 R2 schemas. Windows Server 2012 domain controllers have the default schema to backup TPM owner authorization information in the separate object. If you are not upgrading your domain controller to Windows Server 2012 you need to extend the schema to support this change. If Active Directory backup of the TPM owner authorization value is enabled in a Windows Server 2008 R2 environment without extending the schema, the TPM provisioning will fail and the TPM will remain in a Not Ready state for computers running Windows 8.

Important

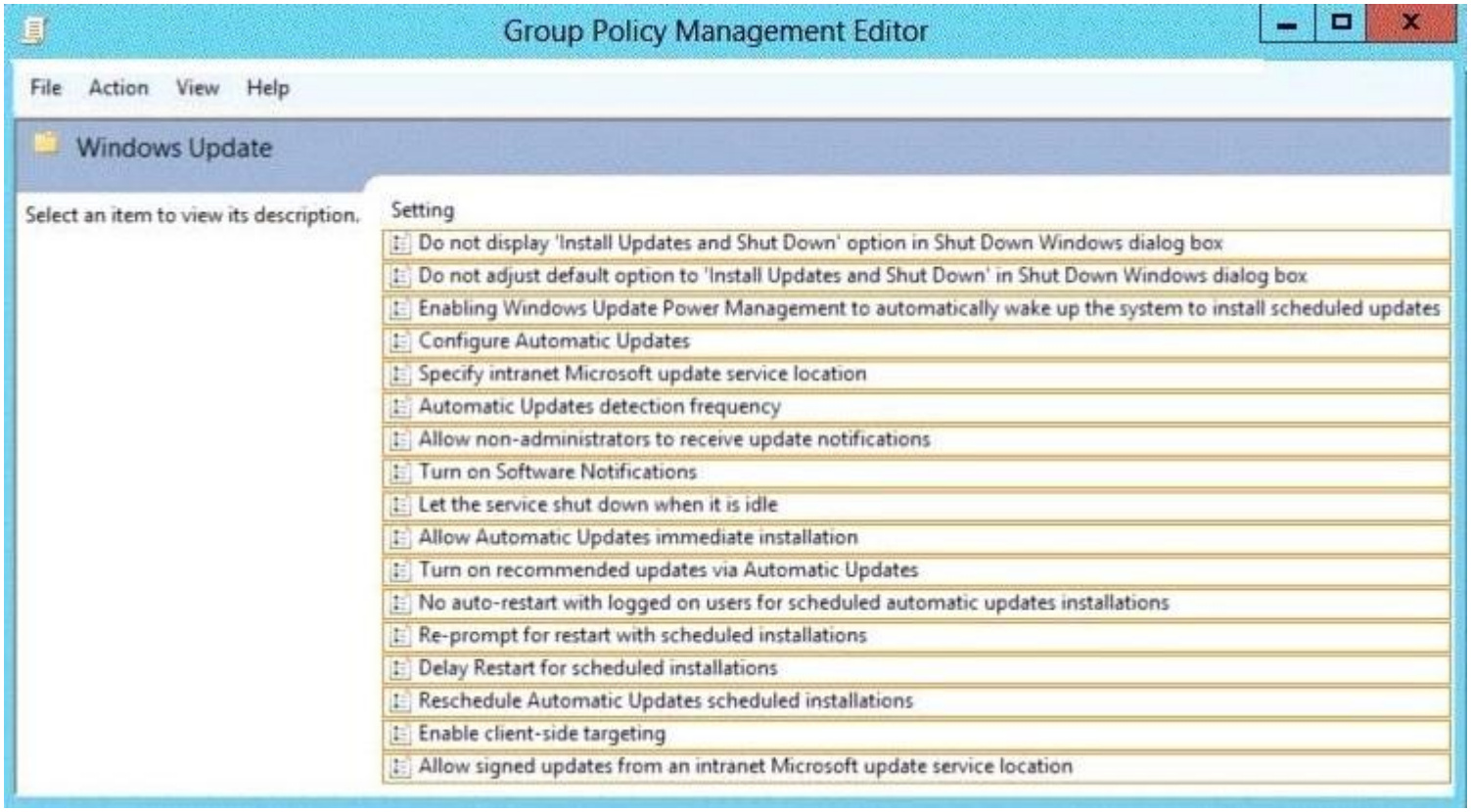
To back up TPM owner information from a computer running Windows 8.1 Preview or Windows 8,you might need to first set up appropriate schema extensions and access control settings on the domain so that the AD DS backup can succeed. Windows Server 2012 R2 Preview and Windows Server 2012 include the required schema extensions by default. For more information, see Schema Extensions for Windows Server 2008 R2 to support AD DS backup of TPM information from Windows 8 clients.

http://technet.microsoft.com/en-us/library/dd875529%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/jj635854.aspx
http://technet.microsoft.com/en-us/library/jj679889.aspx

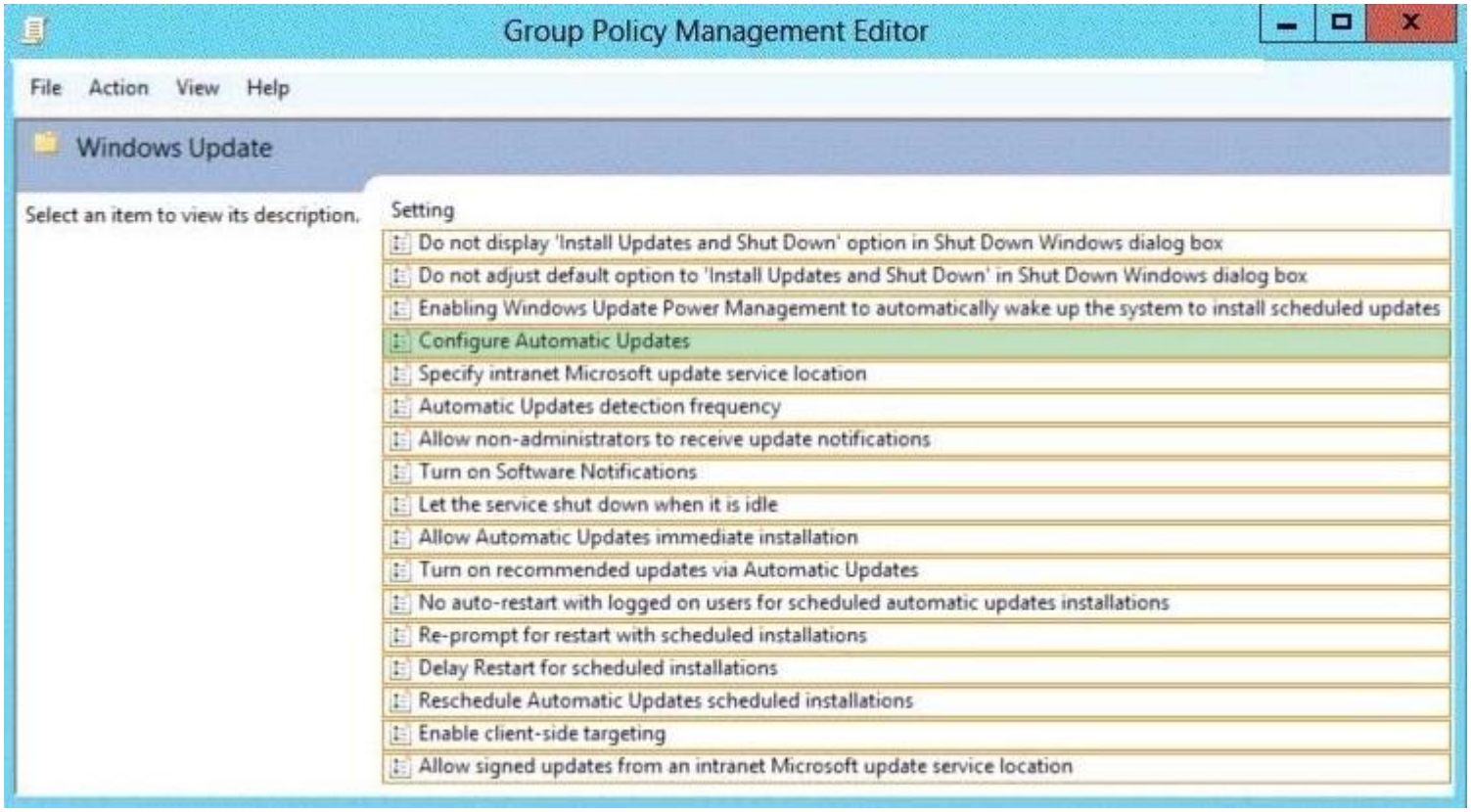
QUESTION 78
Your network contains an Active Directory domain named adatum.com. You have a Group Policy object (GPO) that configures the Windows Update settings. Currently, client computers are configured to download updates from Microsoft Update servers. Users choose when the updates are installed.
You need to configure all client computers to install Windows updates automatically.

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

Hot Area:

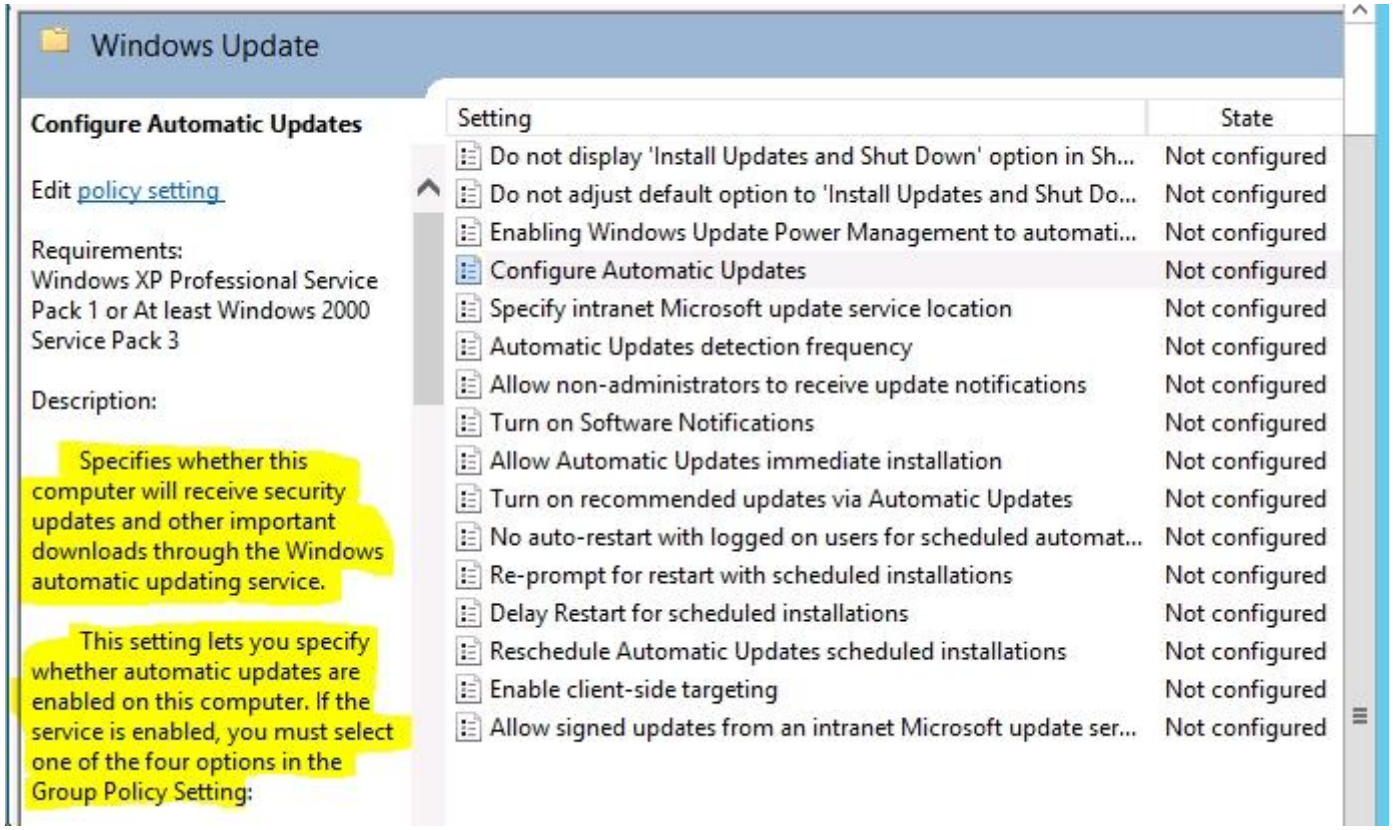


Correct Answer:



Section: D-Deploy, manage and maintain servers
Explanation

Explanation/Reference:



QUESTION 79
Your network contains and Active Directory domain named contoso.com. The domain contains a member server named Server1. All servers run Server 2012.
You need to collect the error events from all the servers on Server1.
The solution ensure that when new servers are added to the domain, their error events are collected automatically on Server1.

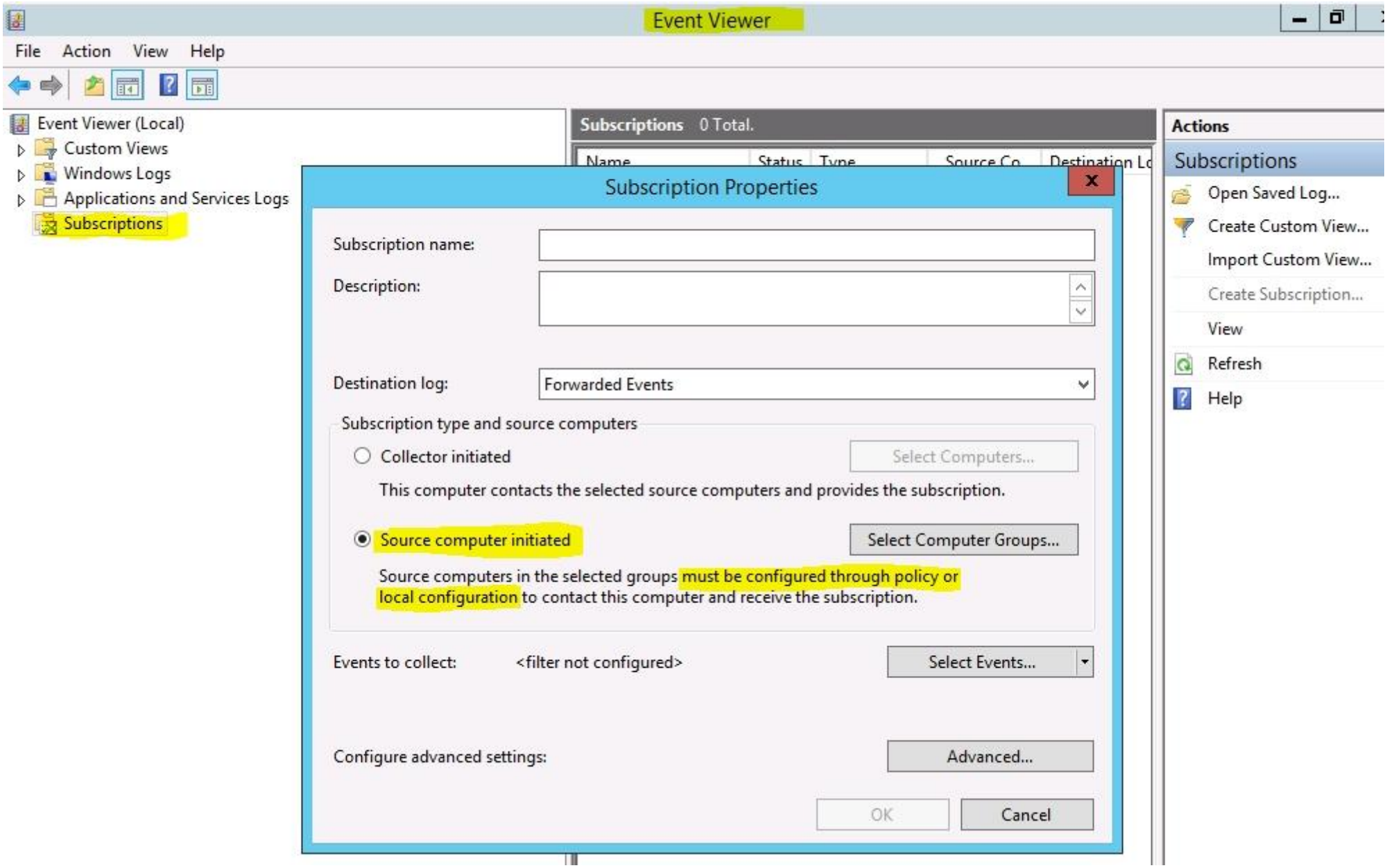
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

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


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Subscriptions
Subscriptions 0 Total.
Name
Status
Type
Source Co
Destination Lo
Actions
Subscriptions
Open Saved Log...
Create Custom View...
Import Custom View...
Create Subscription...
View
Refresh
Help
Subscription Properties
Subscription name:
Description:
Destination log:
Forwarded Events
Subscription type and source computers
Collector initiated
Select Computers...
This computer contacts the selected source computers and provides the subscription.
Source computer initiated
Select Computer Groups...
Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.
Events to collect:
<filter not configured>
Select Events...
Configure advanced settings:
Advanced...
OK
Cancel

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

Source-initiated subscriptions allow you to define a subscription on an event collector computer without defining the event source computers, and then multiple remote event source computers can be set up (using a group policy setting) to forward events to the event collector computer. This differs from a collector initiated subscription because in the collector initiated subscription model, the event collector must define all the event sources in the event subscription.
When setting up a source-initiated subscription, consider whether the event source computers are in the same domain as the event collector computer. The following sections describe the steps to follow when the event sources are in the same domain or not in the same domain as the event collector computer.

Note Any computer in a domain, local or remote, can be an event collector. However, when choosing an event collector, it is important to select a machine that is topologically close to where the majority of the events will be generated. Sending events to a machine at a distant network location on a WAN can reduce overall performance and efficiency in event collection.

http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973(v=vs.85).aspx

QUESTION 80
Your network contains an Active Directory domain called contoso.com. The domain contains a member server named Server1. Server1 runs Windows Server 2012.
You enable the EventLog-Application event trace session.
You need to set the maximum size of the log file used by the trace session to 10 MB.

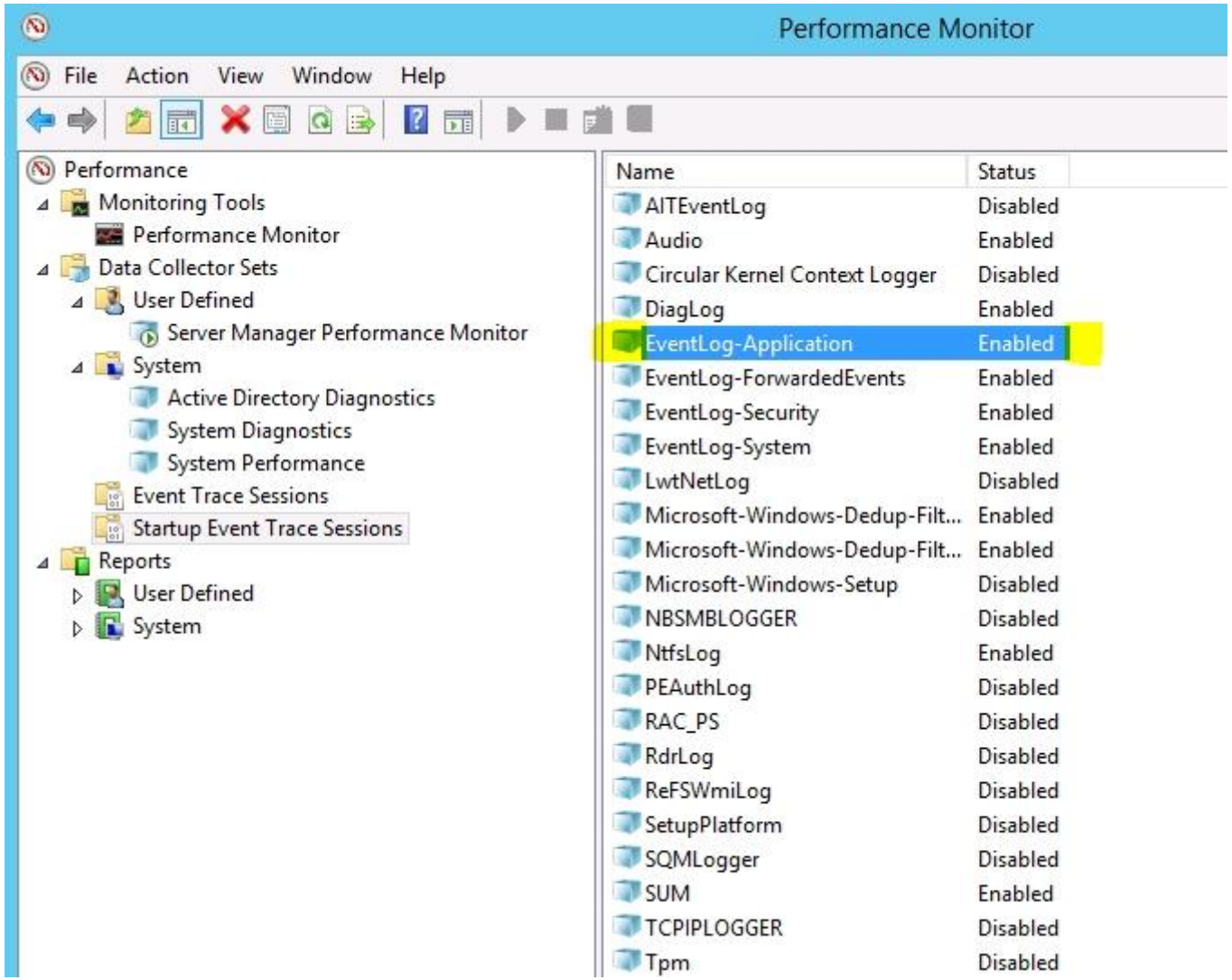
From which tab should you perform the configuration? To answer, select the appropriate tab in the answer area.

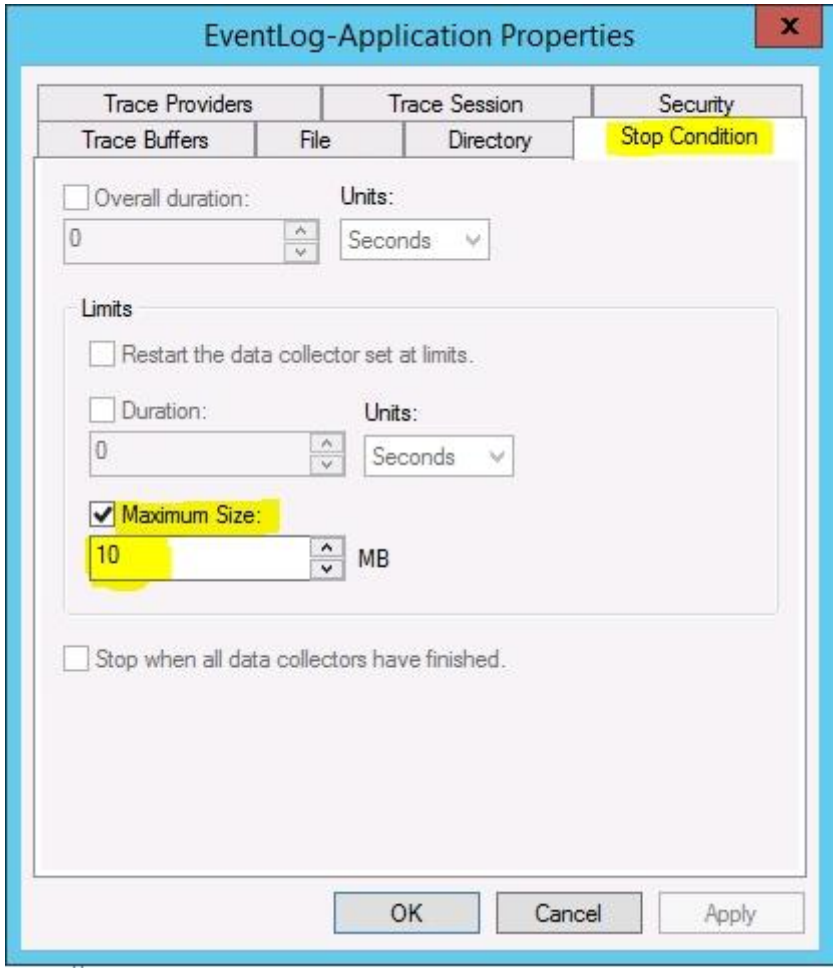
Hot Area:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

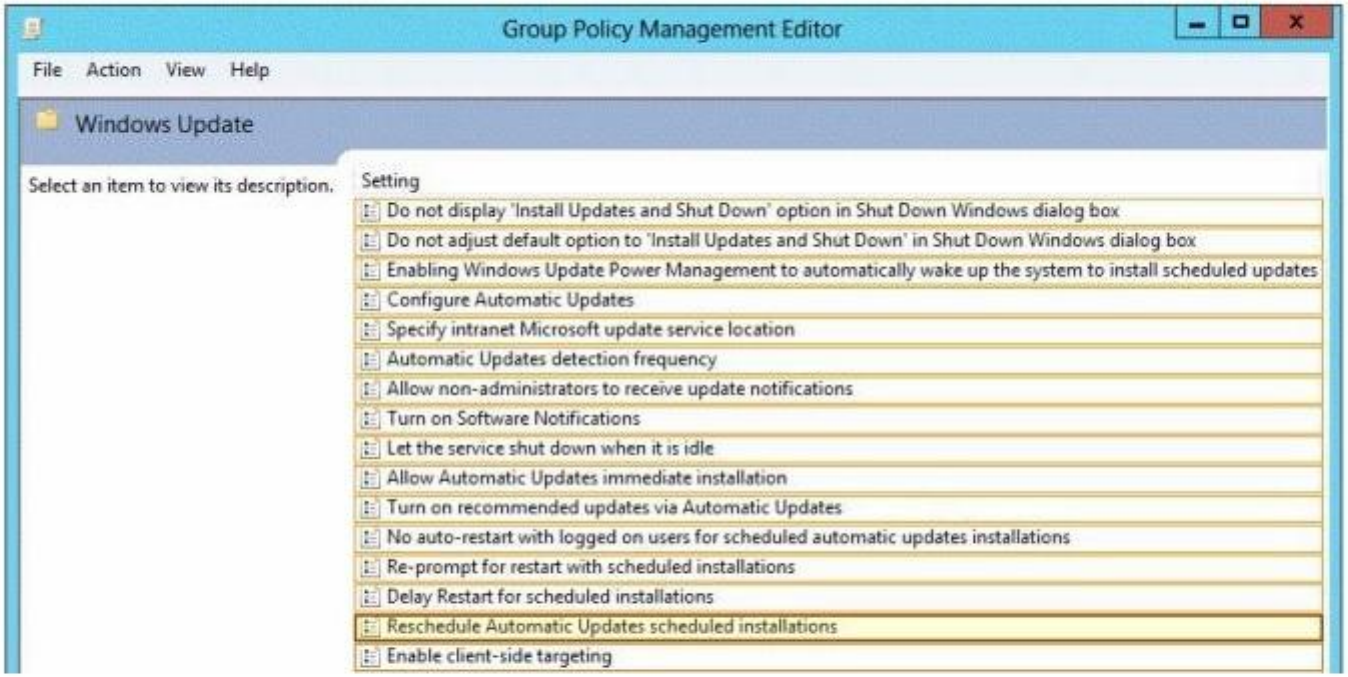

Performance Monitor
File
Action
View
Window
Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
Server Manager Performance Monitor
System
Active Directory Diagnostics
System Diagnostics
System Performance
Event Trace Sessions
Startup Event Trace Sessions
Reports
User Defined
System
Name
Status
AITEventLog Disabled
Audio Enabled
Circular Kernel Context Logger Disabled
DiagLog Enabled
EventLog-Application Enabled
EventLog-ForwardedEvents Enabled
EventLog-Security Enabled
EventLog-System Enabled
LwtNetLog Disabled
Microsoft-Windows-Dedup-Filt... Enabled
Microsoft-Windows-Dedup-Filt... Enabled
Microsoft-Windows-Setup Disabled
NBSMBLOGGER Disabled
NtfsLog Enabled
PEAuthLog Disabled
RAC_PS Disabled
RdrLog Disabled
ReFSWmiLog Disabled
SetupPlatform Disabled
SQMLogger Disabled
SUM Enabled
TCPIPLOGGER Disabled
Tpm Disabled



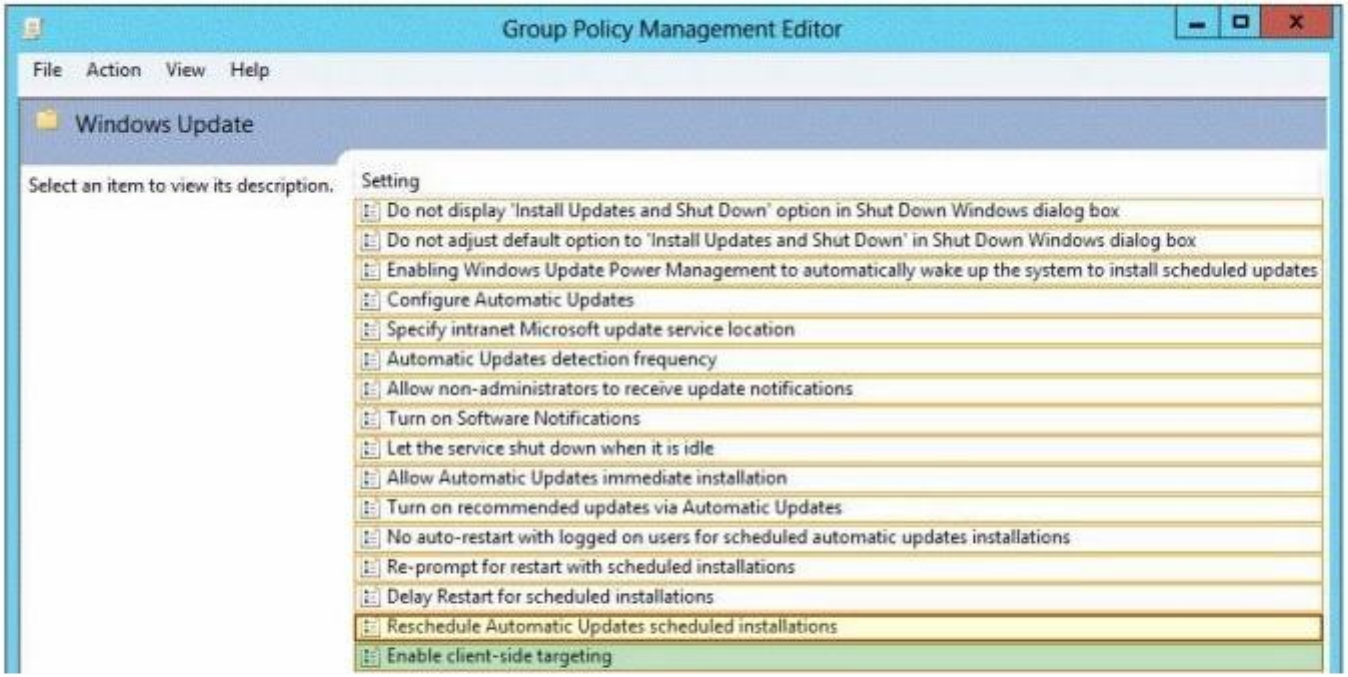
QUESTION 81
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows server 2012. Server1 has the Windows Server Update Services server role installed.
You need to use the Group Policy object (GPO) to assign members to a computer group.

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

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
WSUS enables you to target updates to groups of client computers. This capability can help you ensure that specific computers get the right updates at the most

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

By default, each computer is already assigned to the All Computers group. Computers will also be assigned to the Unassigned Computers group until you assign them to another group. Regardless of the group you assign a computer to, it will also remain in the All Computers group. A computer can be in only one other group in addition to the All Computers group.

You can assign computers to computer groups by using one of two methods, server-side or client-side targeting, depending on whether or not you want to automate the process. With server-side targeting, you use the Move the selected computer task on the Computers page to move one or more client computers to one computer group at a time. **With client-side targeting, you use Group Policy or edit the registry settings on client computers to enable those computers to automatically add themselves into the computer groups**. You must specify which method you will use by selecting one of the two options on the Computers Options page.

QUESTION 82
You have Windows Server 2012 installation media that contains a file named Install.wim. You need to identify which images are present in Install.wim.

What should you do?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Option: /Get-MountedImageInfo
Lists the images that are currently mounted and information about the mounted image such as whether the image is valid, read/write permissions, mount location, mounted file path, and mounted image index.
Example:
Dism /Get-MountedImageInfo

Option: /Get-ImageInfo
Arguments:
/ImageFile:<path_to_image.wim>
[{/Index:<Image_index> | /Name:<Image_name>}]
Displays information about the images that are contained in the .wim, .vhd or .vhdx file. When used with the /Index or /Name argument, information about the specified image is displayed. The /Name argument does not apply to VHD files. You must specify /Index:1 for VHD files.

Example:
Dism /Get-ImageInfo /ImageFile:C:\test\offline\install.wim
Dism /Get-ImageInfo /ImageFile:C:\test\images\myimage.vhd /Index:1

http://technet.microsoft.com/en-us/library/hh825224.aspx
http://technet.microsoft.com/en-us/library/hh825258.aspx

QUESTION 83
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. Server1 and Server2 are nodes in a Hyper-V cluster named Cluster1. Cluster1 hosts 10 virtual machines.
All of the virtual machines run Windows Server 2012 and are members of the domain.
You need to ensure that the first time a service named Service1 fails on a virtual machine, the virtual machine is moved to a different node.
You configure Service1 to be monitored from Failover Cluster Manager.

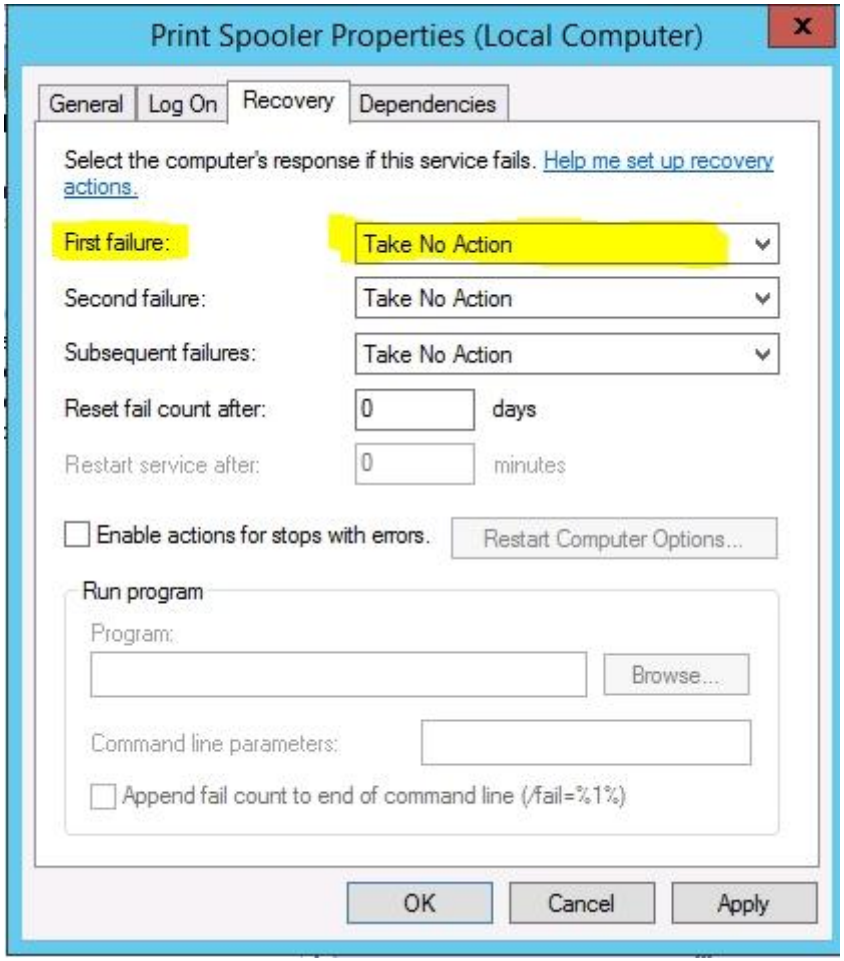
What should you configure on the virtual machine?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Virtual machine application monitoring and management
In clusters running Windows Server 2012, administrators can monitor services on clustered virtual machines that are also running Windows Server 2012. This functionality extends the high-level monitoring of virtual machines that is implemented in Windows Server 2008 R2 failover clusters. If a monitored service in a virtual machine fails, the service can be restarted, or the clustered virtual machine can be restarted or **moved to another node (depending on service restart settings and cluster failover settings).**
This feature increases the uptime of high availability services that are running on virtual machines within a failover cluster.

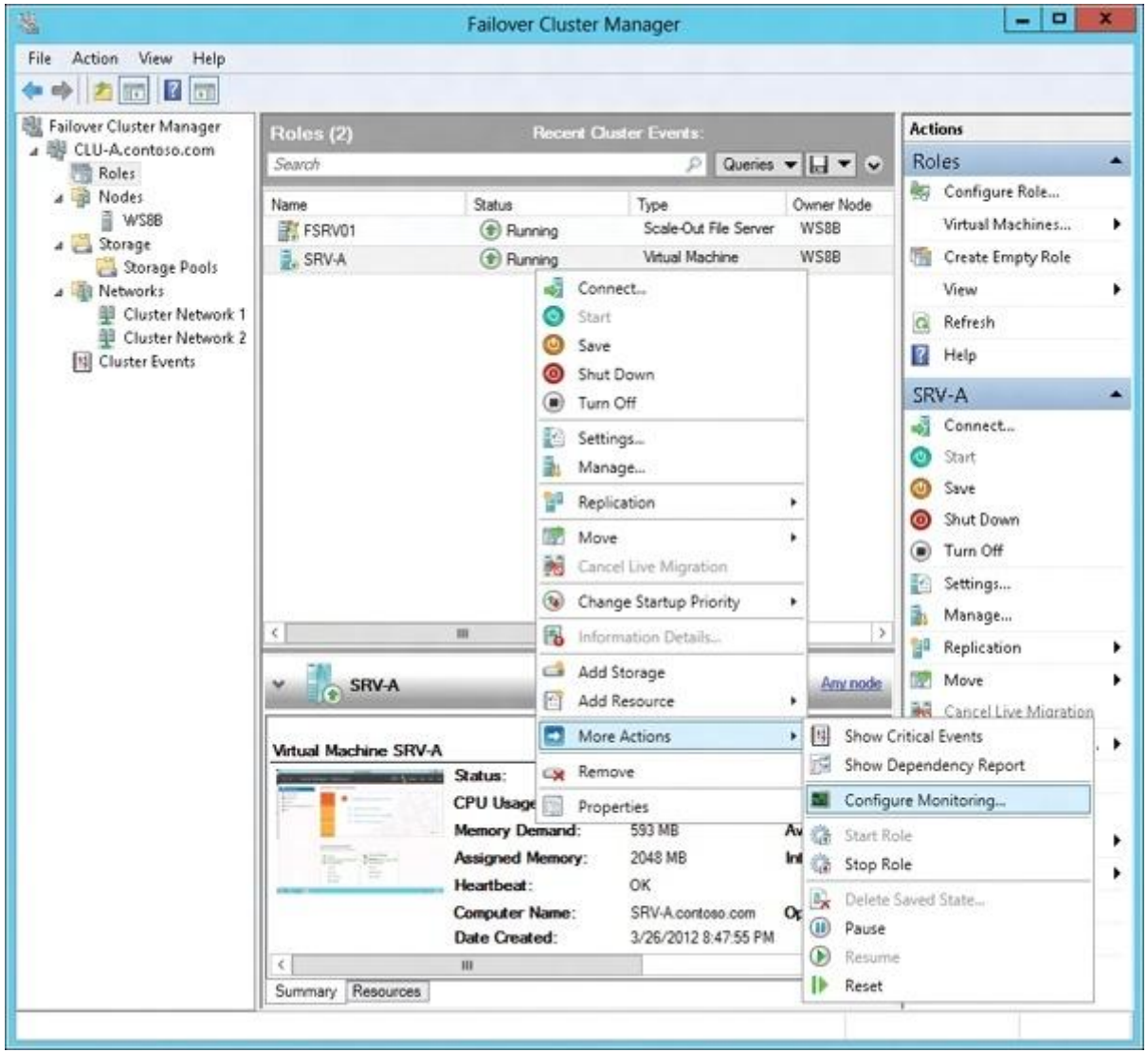
Windows Server 2012 Failover Cluster introduces a new capability for Hyper-V virtual machines (VMs), which is a basic monitoring of a service within the VM which causes the VM to be rebooted should the monitored service fail three times. For this feature to work the following must be configured:
- Both the Hyper-V servers must be Windows Server 2012 and the guest OS running in theVM must be Windows Server 2012.
- The host and guest OSs are in the same or at least trusting domains.
- The Failover Cluster administrator must be a member of the local administrator's group inside the VM.
- **Ensure the service being monitored is set to Take No Action** (see screen shot below) within the guest VM for Subsequent failures (which is used after the first and second failures) and is set via the Recovery tab of the service properties within the Services application (services.msc).



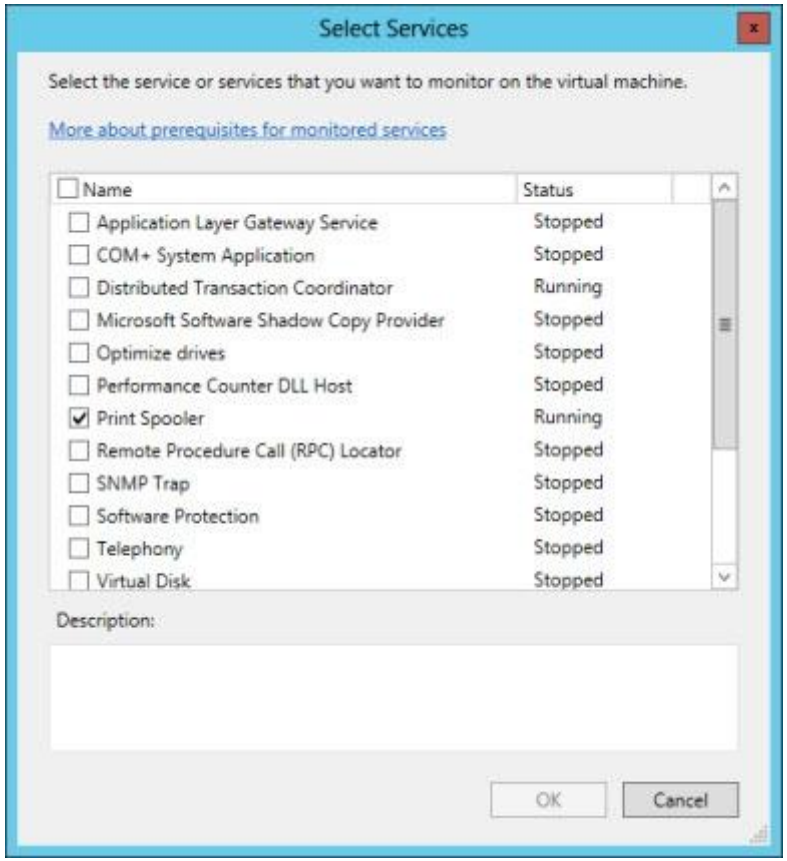
- Within the guest VM, ensure the Virtual Machine Monitoring firewall exception is enabled for the Domain network by using the Windows Firewall with Advanced Security application or by using the Windows PowerShell command below: Set-NetFirewallRule -DisplayGroup "Virtual Machine Monitoring" -Enabled True

After the above is true, enabling the monitoring is a simple process:

1. Launch the Failover Cluster Manager tool.
2. Navigate to the cluster - Roles.
3. Right click on the virtual machine role you wish to enable monitoring for and under More Actions select Configure Monitoring...



4. The services running inside the VM will be gathered and check the box for the services that should be monitored and click OK.



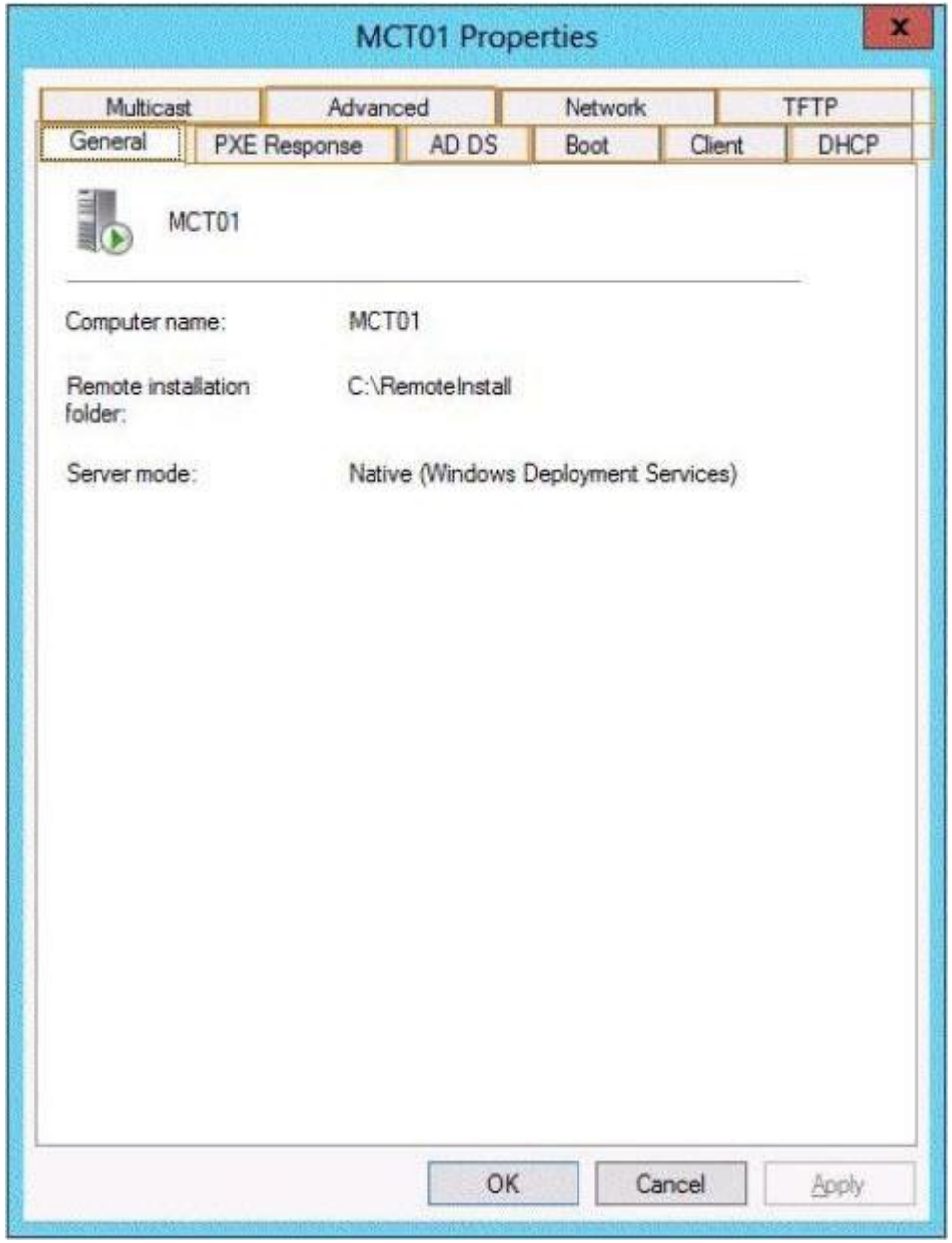
You are done!

Monitoring can also be enabled using the Add-ClusterVMMonitoredItem cmdlet and -VirtualMachine, with the -Service parameters, as the example below shows:
PS C:\Windows\system32> Add-ClusterVMMonitoredItem -VirtualMachine savdaltst01 -Service spooler
http://sportstoday.us/technology/windows-server-2012---continuous-availability-%28part-4%29---failover-clustering-enhancements---virtual-machine-monitoring-.aspx
http://windowsitpro.com/windows-server-2012/enable-windows-server-2012-failover-cluster-hyper-v-vm-monitoring

QUESTION 84
Your network contains an Active Directory domain named contoso.com. The domain contains a member server that runs Windows Server 2012 and has the Windows Deployment Services (WDS) server role installed. You create a new multicast session in WDS and connect 50 client computers to the session. When you open the Windows Deployment Services console, you discover that all of the computers are listed as pending devices.
You need to ensure that any of the computers on the network can join a multicast transmission without requiring administrator approval.

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

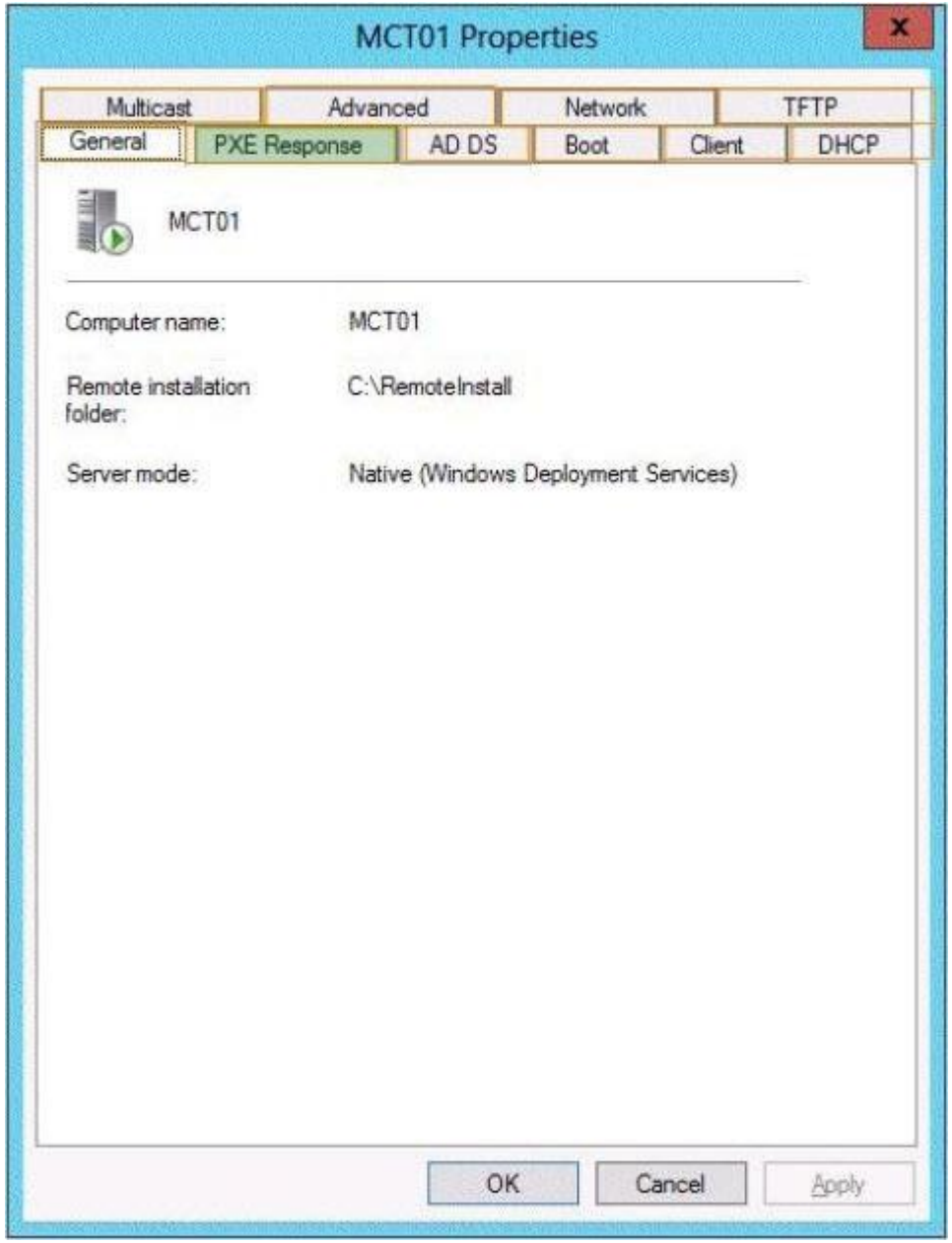
Hot Area:



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

Correct Answer:

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

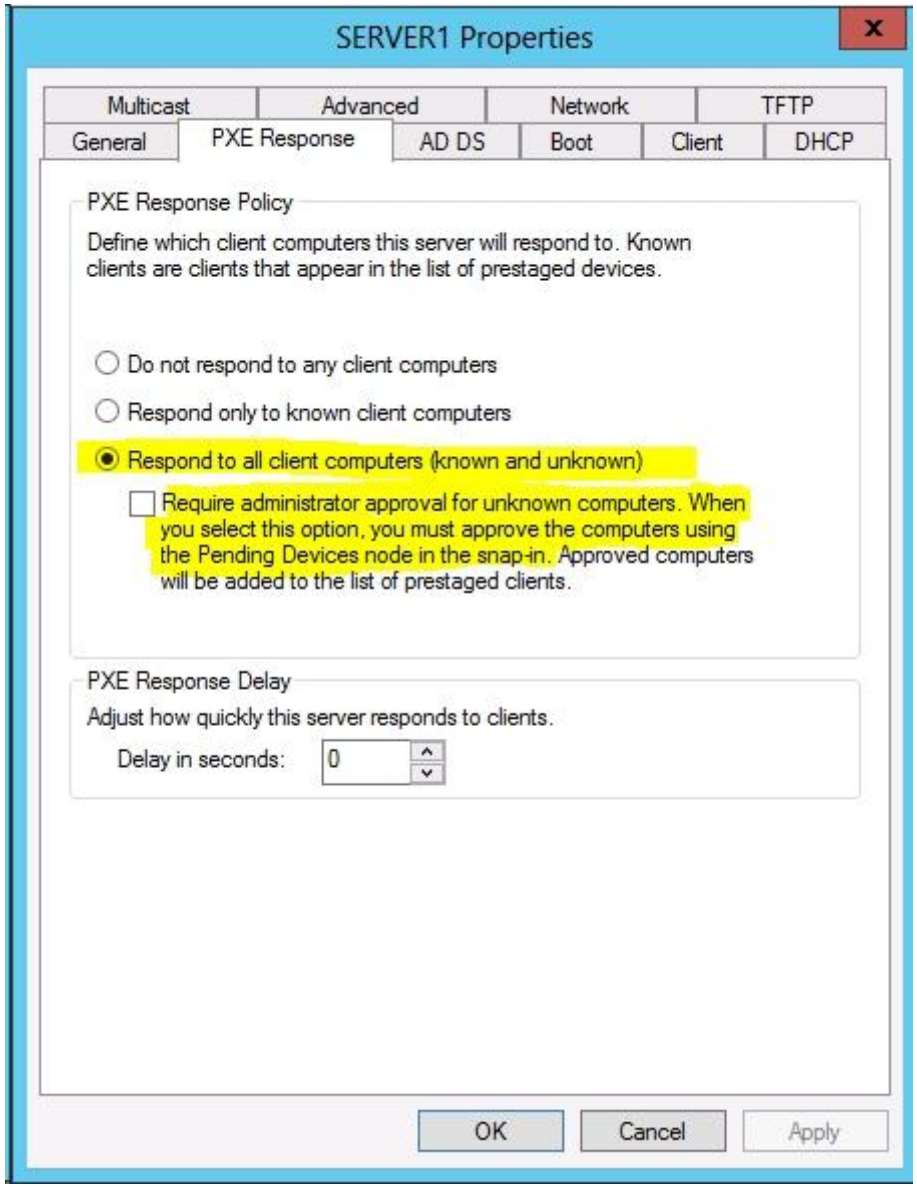


www.vceplus.com - Website designed to help IT pros advance their careers.

Section: (none)
Explanation

Explanation/Reference:

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


SERVER1 Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
PXE Response Policy
Define which client computers this server will respond to. Known clients are clients that appear in the list of prestaged devices.
Do not respond to any client computers
Respond only to known client computers
Respond to all client computers (known and unknown)
Require administrator approval for unknown computers. When you select this option, you must approve the computers using the Pending Devices node in the snap-in. Approved computers will be added to the list of prestaged clients.
PXE Response Delay
Adjust how quickly this server responds to clients.
Delay in seconds:
0
OK
Cancel
Apply

QUESTION 85

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

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

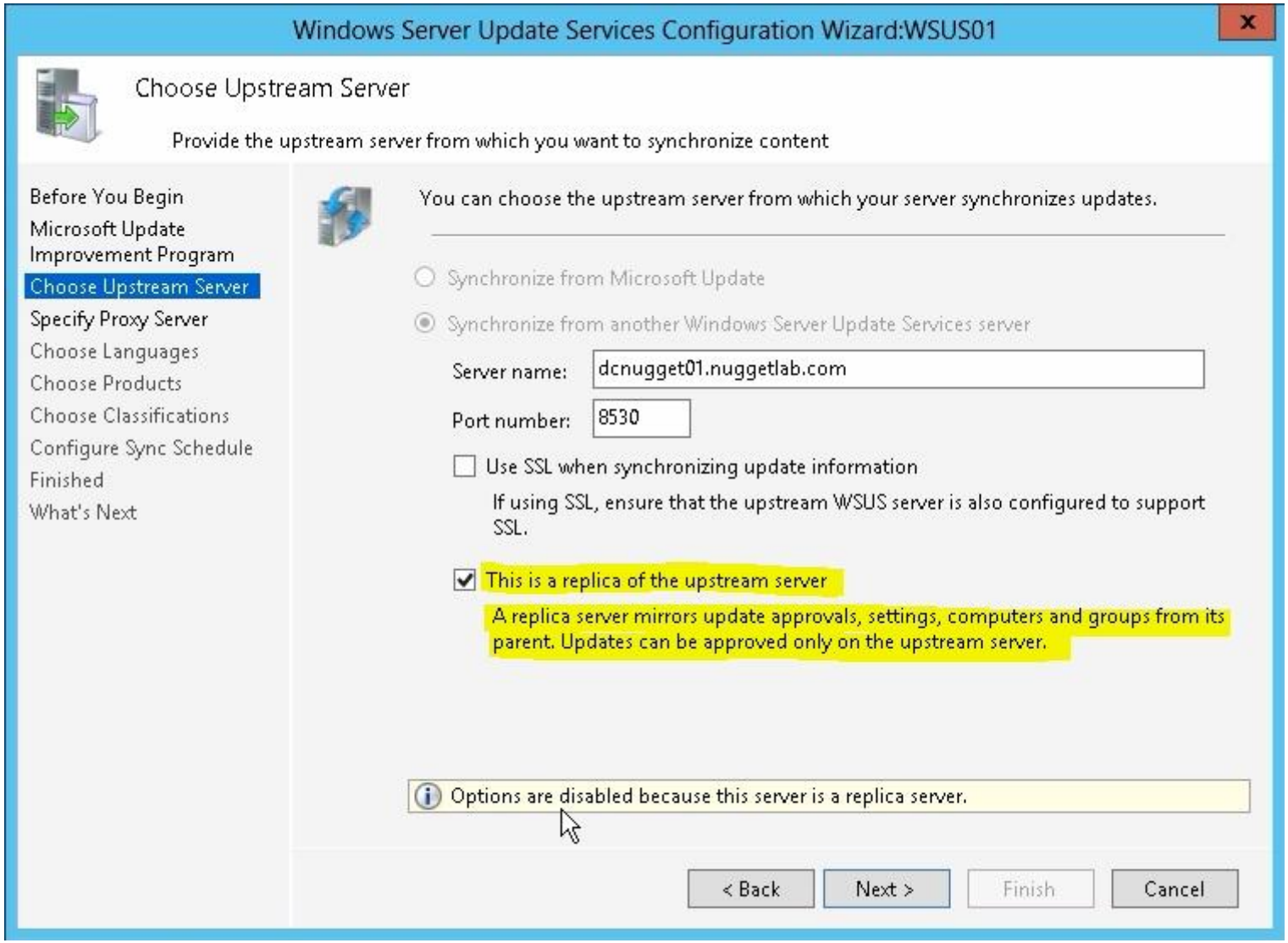
You need to configure replica downstream servers to send Server1 summary information about the computer update status.

What should you do?

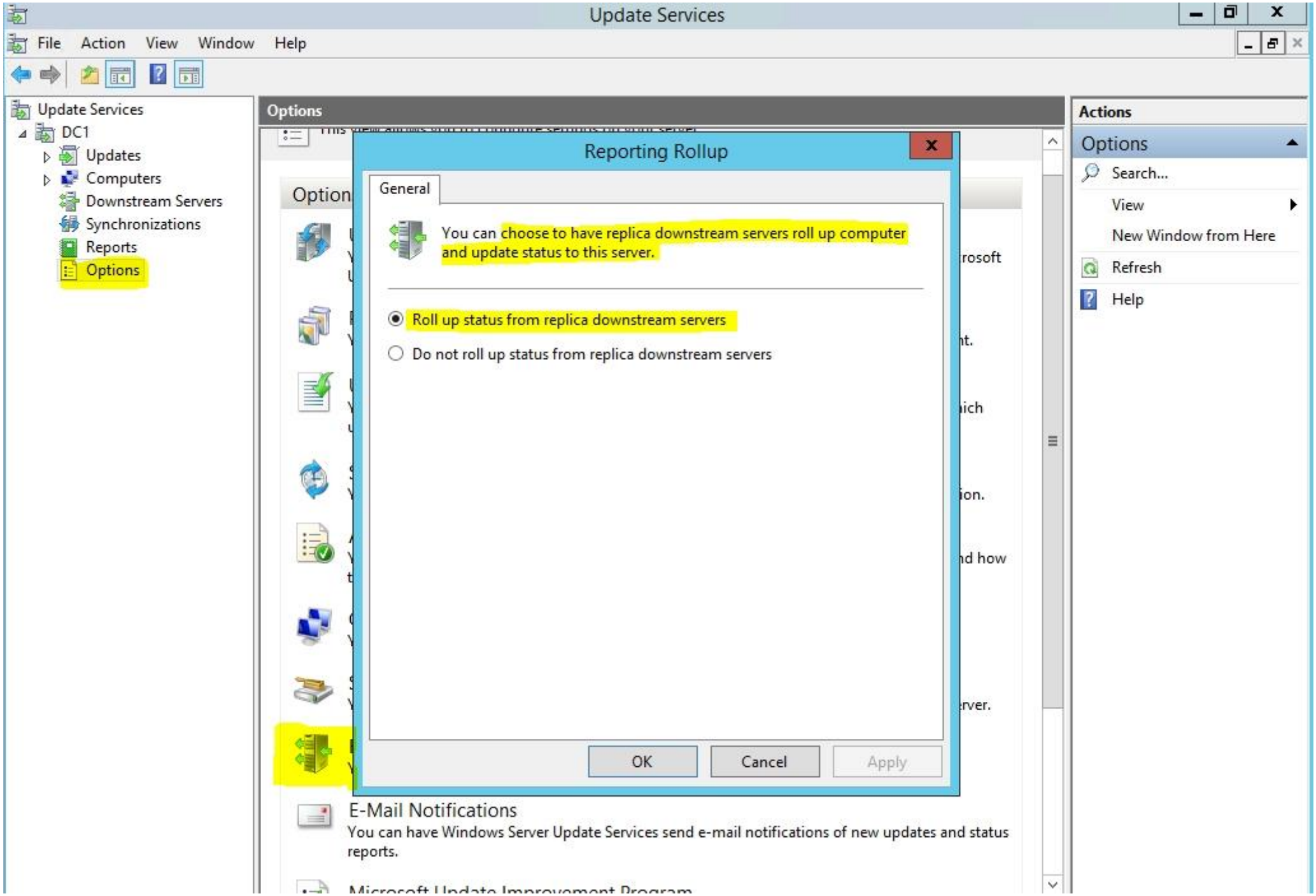
A. From Server1, configure Reporting Rollup.
B. From Server2, configure Reporting Rollup.
C. From Server1, configure Email Notifications.
D. From Server2, configure Email Notifications.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reports enable you to monitor different aspects of the WSUS network: updates, client computers, and downstream servers.
WSUS Reporting Rollup Sample Tool
This tool uses the WSUS application programming interface (API) to demonstrate centralized monitoring and reporting for WSUS. It creates a single report of update and computer status from the WSUS servers into your WSUS environment. The sample package also contains sample source files to customize or extend the tool functionality of the tool to meet specific needs. The WSUS Reporting Rollup Sample Tool and files are provided AS IS. No product support is available for this tool or sample files. For more information read the readme file.
http://technet.microsoft.com/en-us/windowsserver/bb466192.aspx
If a WSUS server has replica servers, **you can choose to roll up the replica servers' client status to the upstream server.**
SERVER2


Windows Server Update Services Configuration Wizard:WSUS01
Choose Upstream Server
Provide the upstream server from which you want to synchronize content
Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next
You can choose the upstream server from which your server synchronizes updates.
Synchronize from Microsoft Update
Synchronize from another Windows Server Update Services server
Server name:
dcnugget01.nuggetlab.com
Port number:
8530
Use SSL when synchronizing update information
If using SSL, ensure that the upstream WSUS server is also configured to support SSL.
This is a replica of the upstream server
A replica server mirrors update approvals, settings, computers and groups from its parent. Updates can be approved only on the upstream server.
Options are disabled because this server is a replica server.
< Back
Next >
Finish
Cancel

SERVER1


Update Services
File Action View Window Help
Update Services
DC1
Updates
Computers
Downstream Servers
Synchronizations
Reports
Options
Options
Reporting Rollup
General
You can choose to have replica downstream servers roll up computer and update status to this server.
Roll up status from replica downstream servers
Do not roll up status from replica downstream servers
OK
Cancel
Apply
E-Mail Notifications
You can have Windows Server Update Services send e-mail notifications of new updates and status reports.
Actions
Options
Search...
View
New Window from Here
Refresh
Help

WSUS Reporting Rollup Sample Tool

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

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

QUESTION 86
DRAG DROP

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.

You generalize Server2.

You install the Windows Deployment Services (WDS) server role on Server1.

You need to capture an image of Server2 on Server1.

Which three actions should you perform?

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

Select and Place:

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

Correct Answer:

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

Section: (none)
Explanation

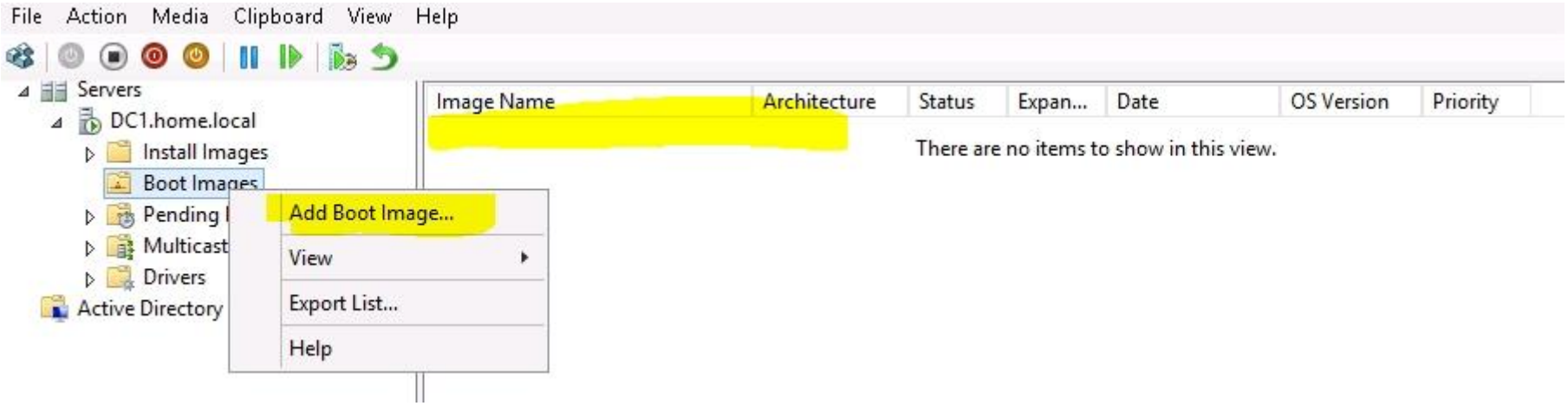
Explanation/Reference:
Explanation: Box 1: Start Server2 by using PXE.

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.



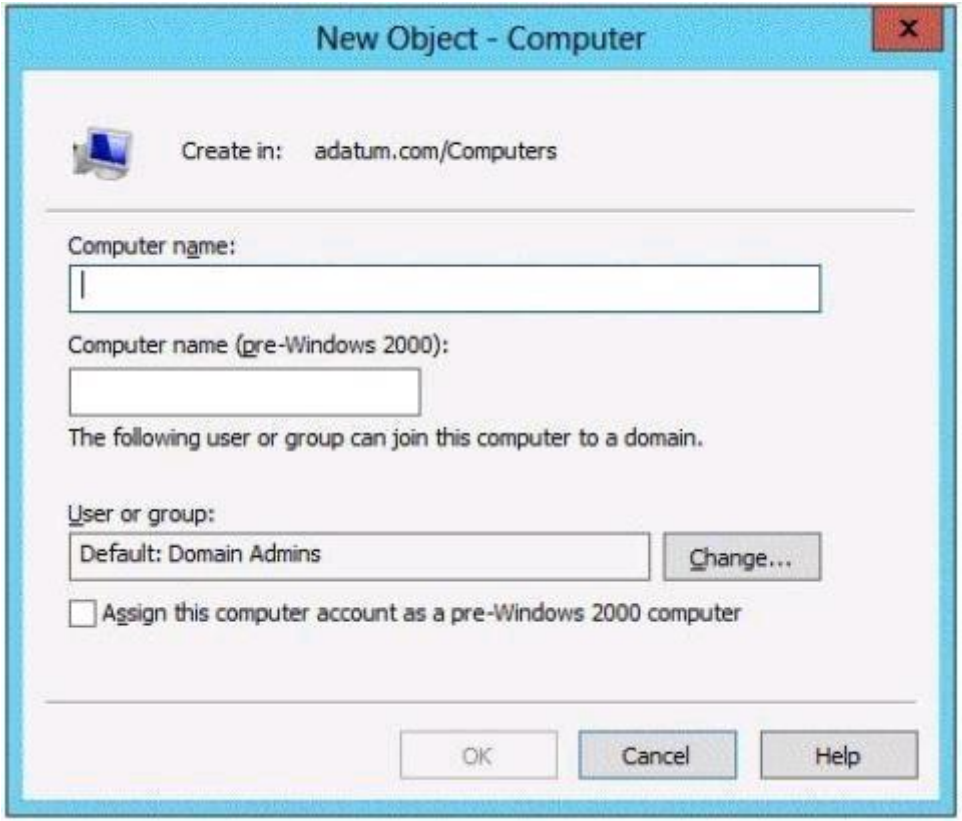
QUESTION 87
Your network contains an Active Directory domain named adatum.com. Client computers are deployed by using Windows Deployment Services (WDS).

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

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

What should you do on DC1?

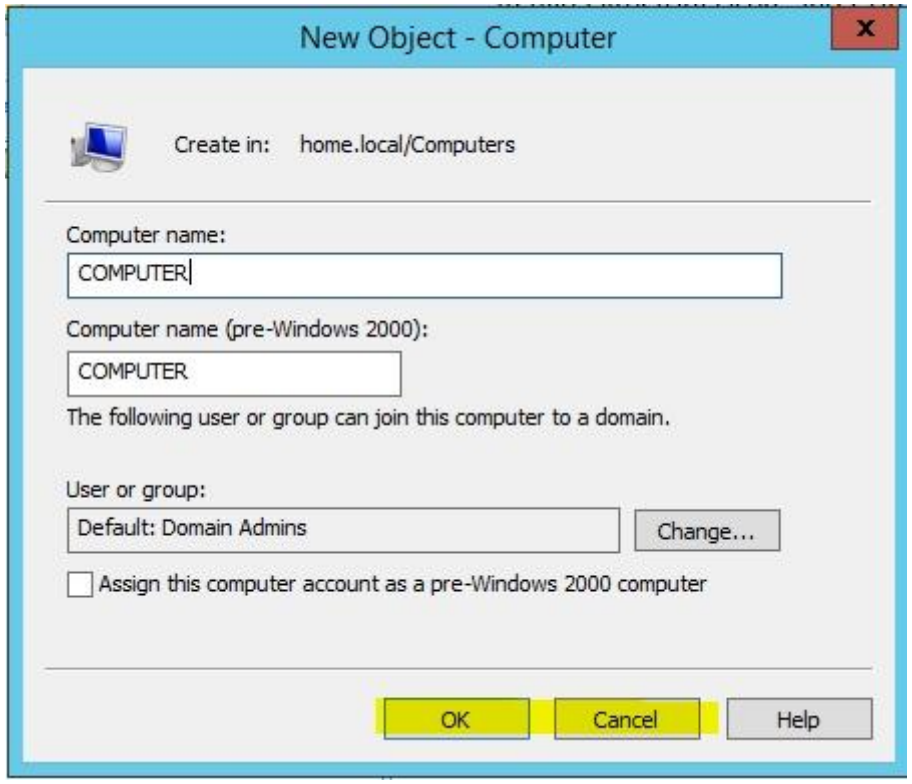
Exhibit:

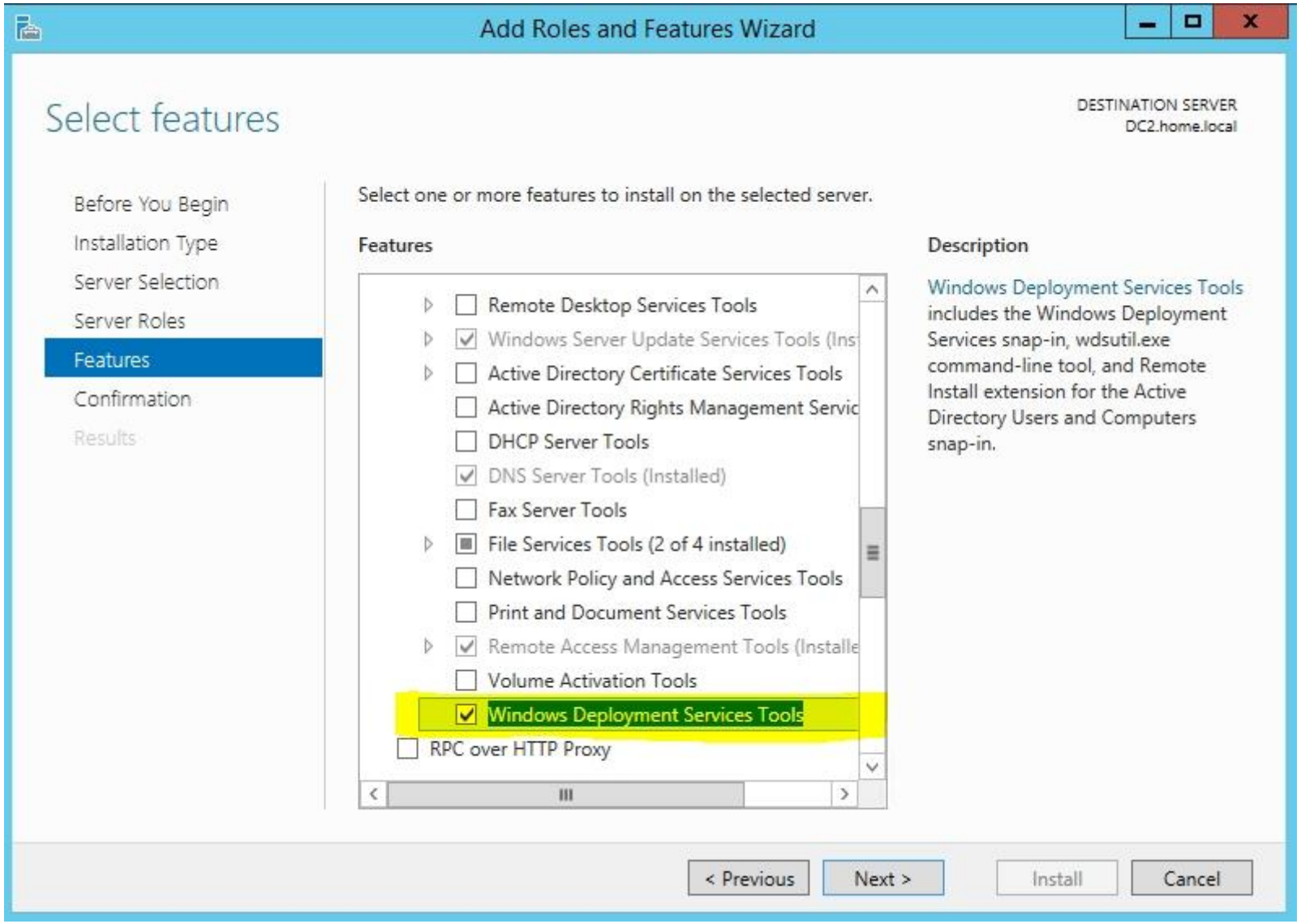


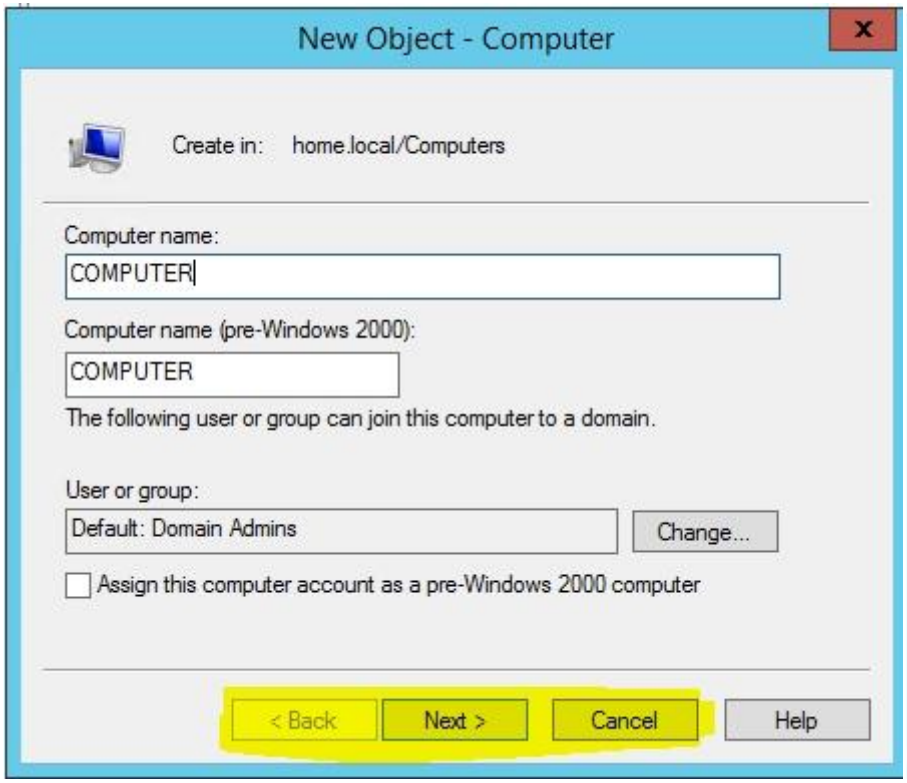
A. Install the User Interfaces and Infrastructure feature.
B. From the View menu in Active Directory Users and Computers, select Users, Contacts, Groups, and Computers as containers.
C. Install the Windows Deployment Services Tools role administration tool.
D. From the View menu in Active Directory Users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

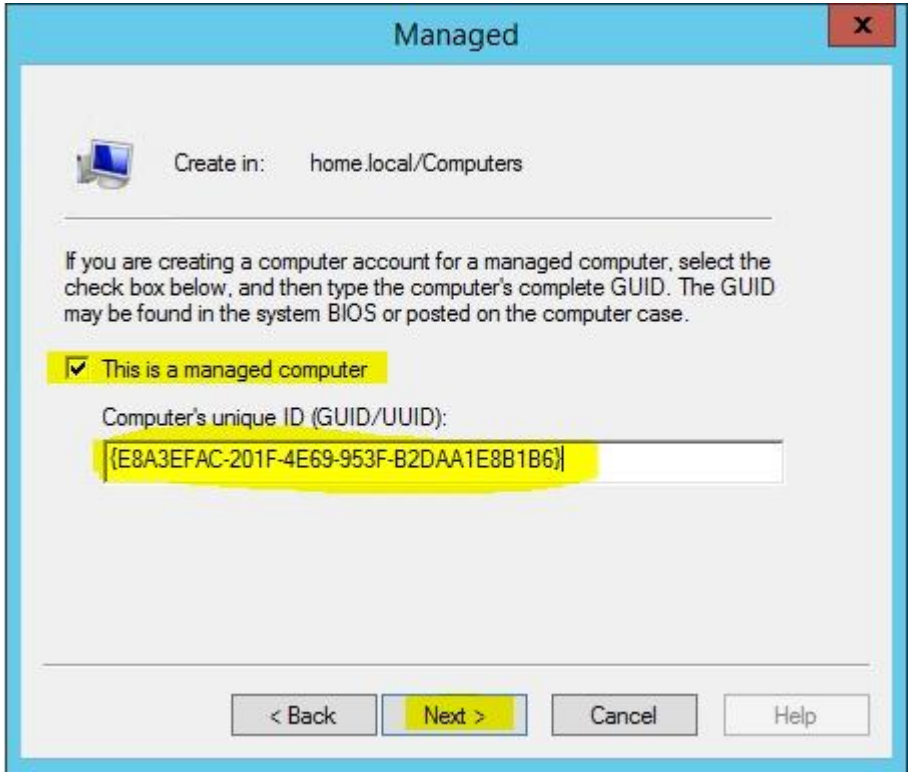
Correct Answer: C
Section: (none)
Explanation

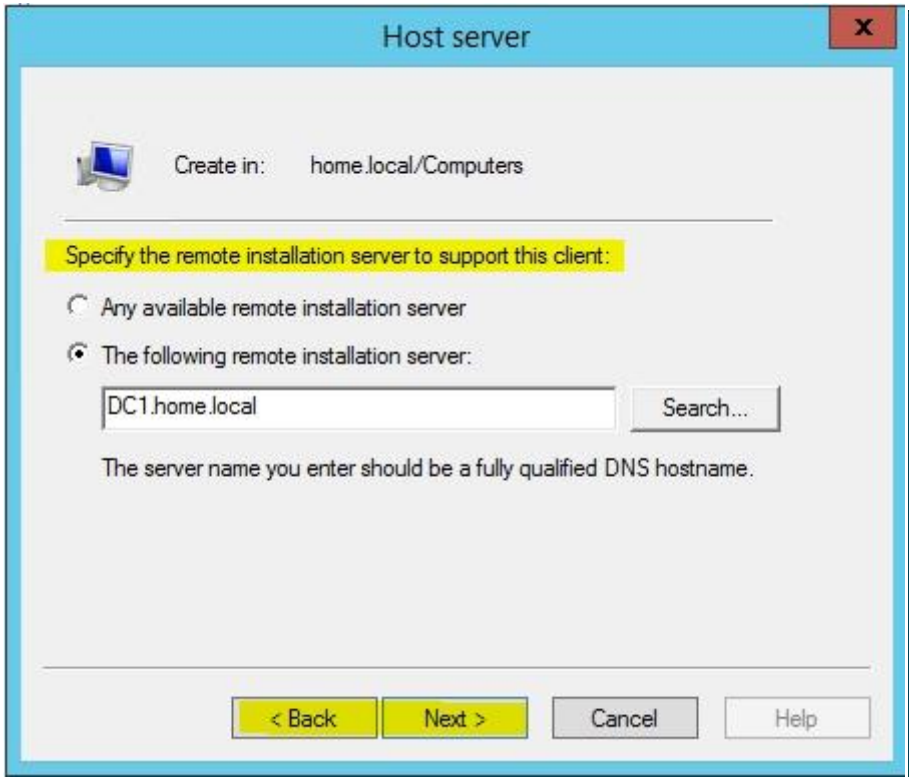
Explanation/Reference:

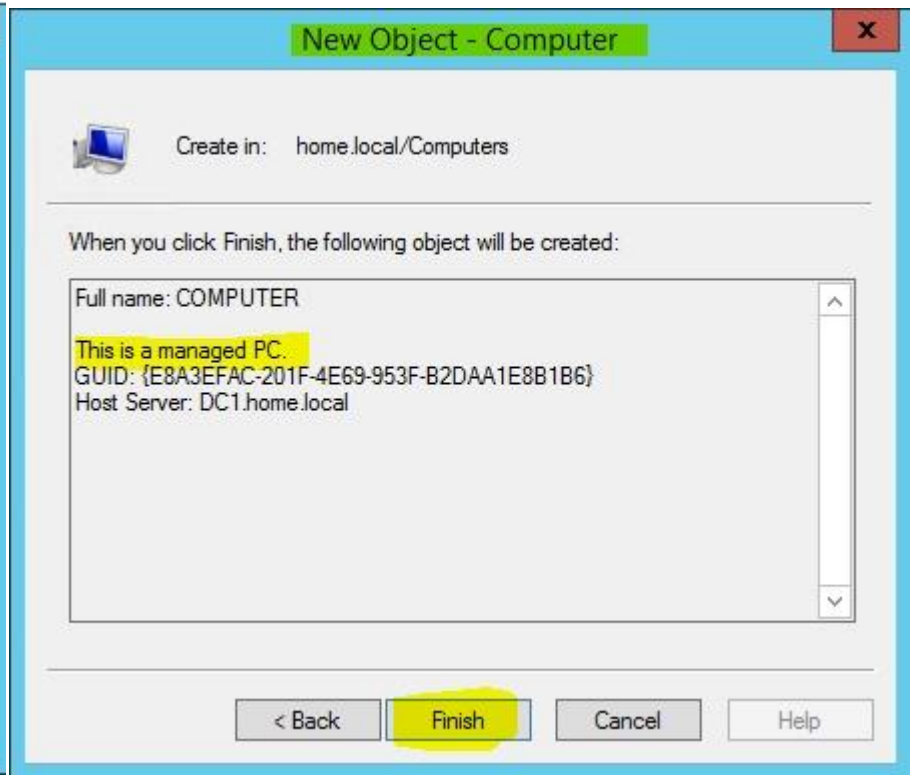

New Object - Computer
Create in: home.local/Computers
Computer name:
COMPUTER
Computer name (pre-Windows 2000):
COMPUTER
The following user or group can join this computer to a domain.
User or group:
Default: Domain Admins
Change...
Assign this computer account as a pre-Windows 2000 computer
OK
Cancel
Help


Add Roles and Features Wizard
Select features
DESTINATION SERVER
DC2.home.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more features to install on the selected server.
Features
Remote Desktop Services Tools
Windows Server Update Services Tools (Ins
Active Directory Certificate Services Tools
Active Directory Rights Management Servic
DHCP Server Tools
DNS Server Tools (Installed)
Fax Server Tools
File Services Tools (2 of 4 installed)
Network Policy and Access Services Tools
Print and Document Services Tools
Remote Access Management Tools (Installe
Volume Activation Tools
Windows Deployment Services Tools
RPC over HTTP Proxy
Description
Windows Deployment Services Tools includes the Windows Deployment Services snap-in, wdsutil.exe command-line tool, and Remote Install extension for the Active Directory Users and Computers snap-in.
< Previous
Next >
Install
Cancel


New Object - Computer
Create in: home.local/Computers
Computer name:
COMPUTER
Computer name (pre-Windows 2000):
COMPUTER
The following user or group can join this computer to a domain.
User or group:
Default: Domain Admins
Change...
Assign this computer account as a pre-Windows 2000 computer
< Back
Next >
Cancel
Help


Managed
Create in: home.local/Computers
If you are creating a computer account for a managed computer, select the check box below, and then type the computer's complete GUID. The GUID may be found in the system BIOS or posted on the computer case.
This is a managed computer
Computer's unique ID (GUID/UUID):
{E8A3EFAC-201F-4E69-953F-B2DAA1E8B1B6}
< Back
Next >
Cancel
Help





QUESTION 88
You have a server named Server1 that runs Windows Server 2012. On Server1, you configure a custom Data Collector Set (DCS) named DCS1.
You need to ensure that all performance log data that is older than 30 days is deleted automatically.

What should you configure?

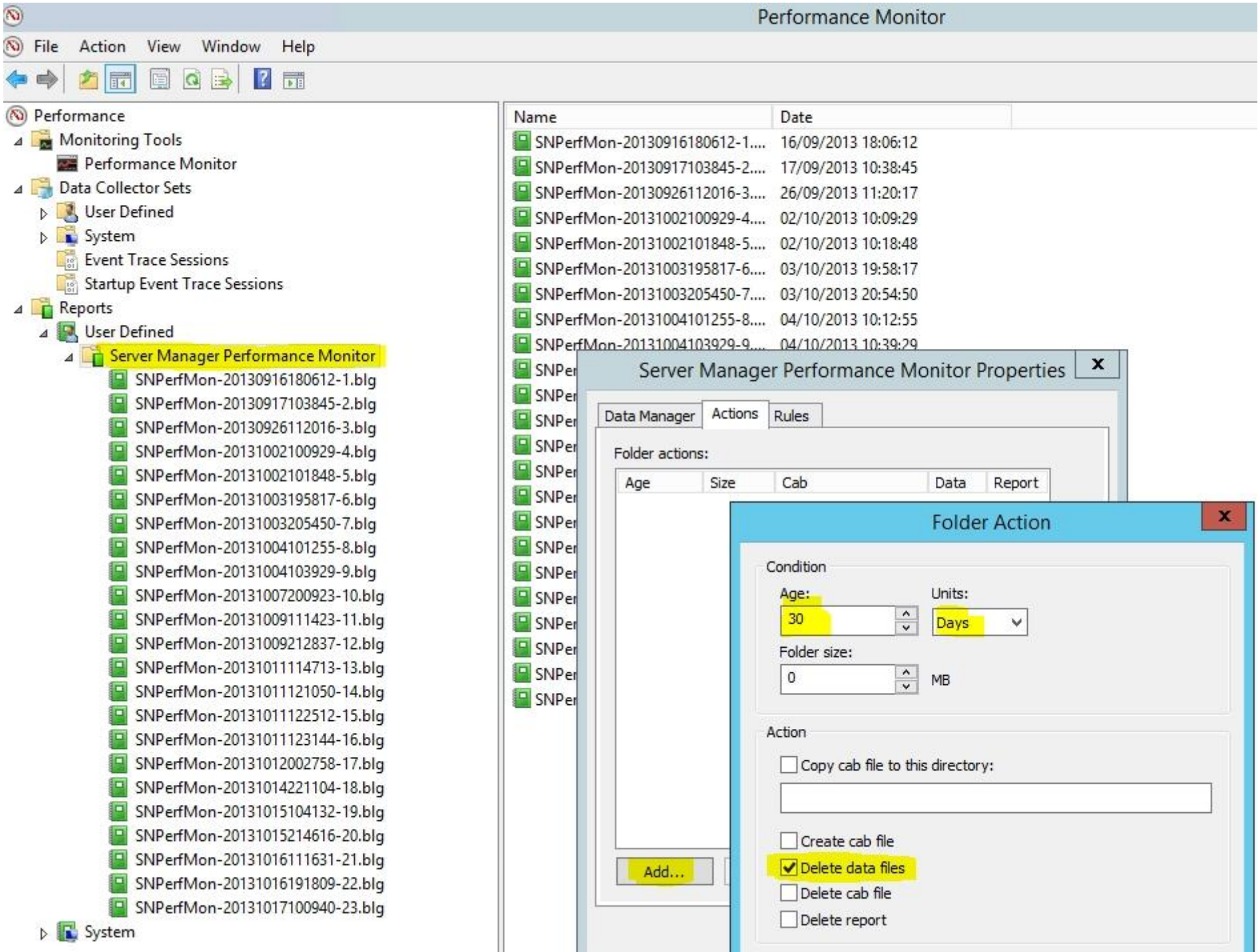
A. a File Server Resource Manager (FSRM) quota on the %Systemdrive%\PerfLogs folder
B. a schedule for DCS1
C. the Data Manager settings of DCS1
D. a File Server Resource Manager (FSRM) file screen on the %Systemdrive%\PerfLogs folder

Correct Answer: C
Section: (none)

Explanation

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

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


Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
System
Event Trace Sessions
Startup Event Trace Sessions
Reports
User Defined
Server Manager Performance Monitor
SNPerfMon-20130916180612-1.blg
SNPerfMon-20130917103845-2.blg
SNPerfMon-20130926112016-3.blg
SNPerfMon-20131002100929-4.blg
SNPerfMon-20131002101848-5.blg
SNPerfMon-20131003195817-6.blg
SNPerfMon-20131003205450-7.blg
SNPerfMon-20131004101255-8.blg
SNPerfMon-20131004103929-9.blg
SNPerfMon-20131007200923-10.blg
SNPerfMon-20131009111423-11.blg
SNPerfMon-20131009212837-12.blg
SNPerfMon-20131011114713-13.blg
SNPerfMon-20131011121050-14.blg
SNPerfMon-20131011122512-15.blg
SNPerfMon-20131011123144-16.blg
SNPerfMon-20131012002758-17.blg
SNPerfMon-20131014221104-18.blg
SNPerfMon-20131015104132-19.blg
SNPerfMon-20131015214616-20.blg
SNPerfMon-20131016111631-21.blg
SNPerfMon-20131016191809-22.blg
SNPerfMon-20131017100940-23.blg
System
Name
Date
SNPerfMon-20130916180612-1.... 16/09/2013 18:06:12
SNPerfMon-20130917103845-2.... 17/09/2013 10:38:45
SNPerfMon-20130926112016-3.... 26/09/2013 11:20:17
SNPerfMon-20131002100929-4.... 02/10/2013 10:09:29
SNPerfMon-20131002101848-5.... 02/10/2013 10:18:48
SNPerfMon-20131003195817-6.... 03/10/2013 19:58:17
SNPerfMon-20131003205450-7.... 03/10/2013 20:54:50
SNPerfMon-20131004101255-8.... 04/10/2013 10:12:55
Server Manager Performance Monitor Properties
Data Manager
Actions
Rules
Folder actions:
Age
Size
Cab
Data
Report
Add...
Folder Action
Condition
Age:
30
Units:
Days
Folder size:
0
MB
Action
Copy cab file to this directory:
Create cab file
Delete data files
Delete cab file
Delete report

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

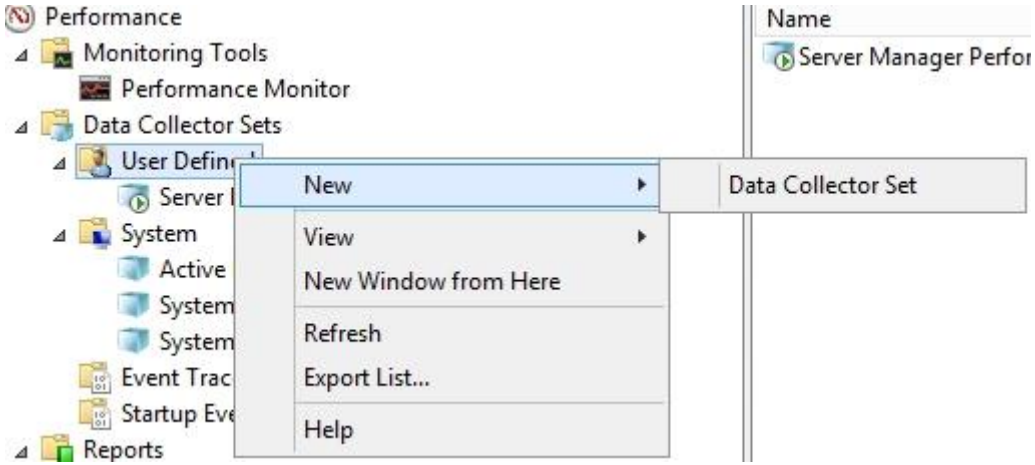
QUESTION 89
You have a server named Server1 that runs Windows Server 2012. You create a custom Data Collector Set (DCS) named DCS1.
You need to configure DCS1 to meet the following requirements:
· Automatically run a program when the amount of total free disk space on Server1 drops below 10 percent of capacity.
· Log the current values of several registry settings.

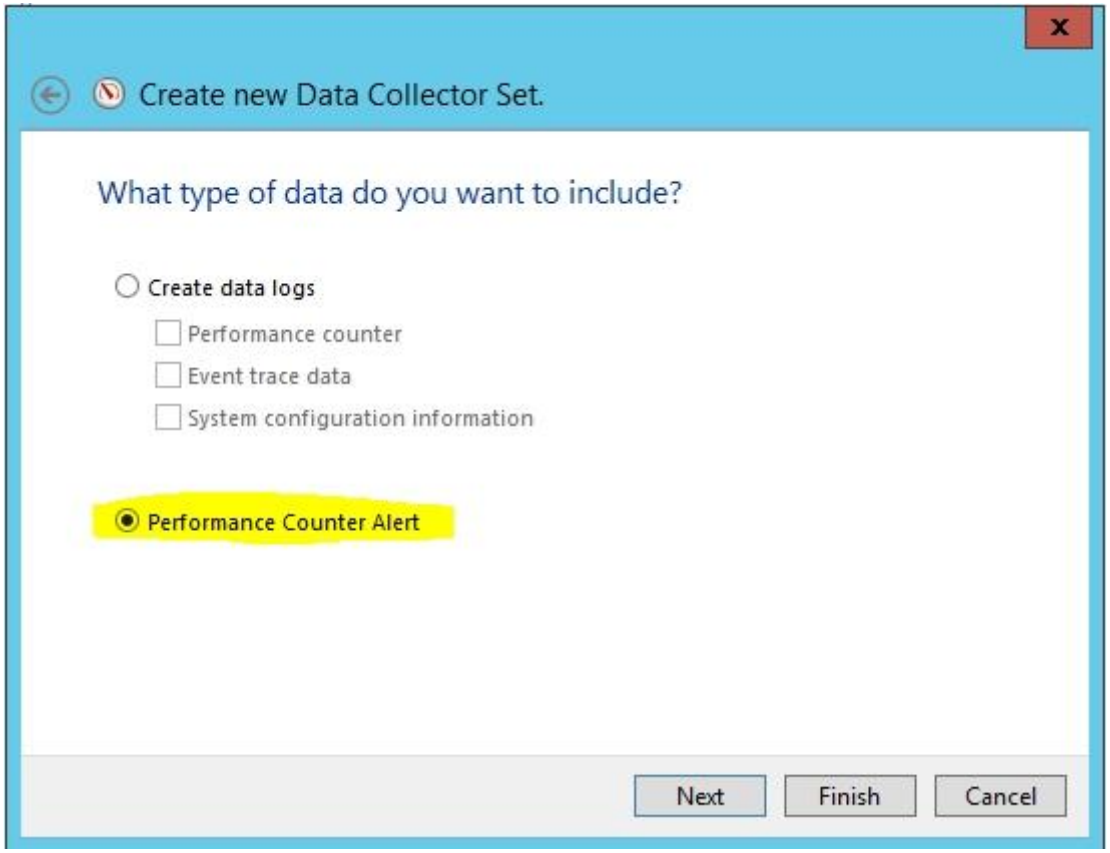
Which two should you configure in DCS1? (Each correct answer presents part of the solution. Choose two.)

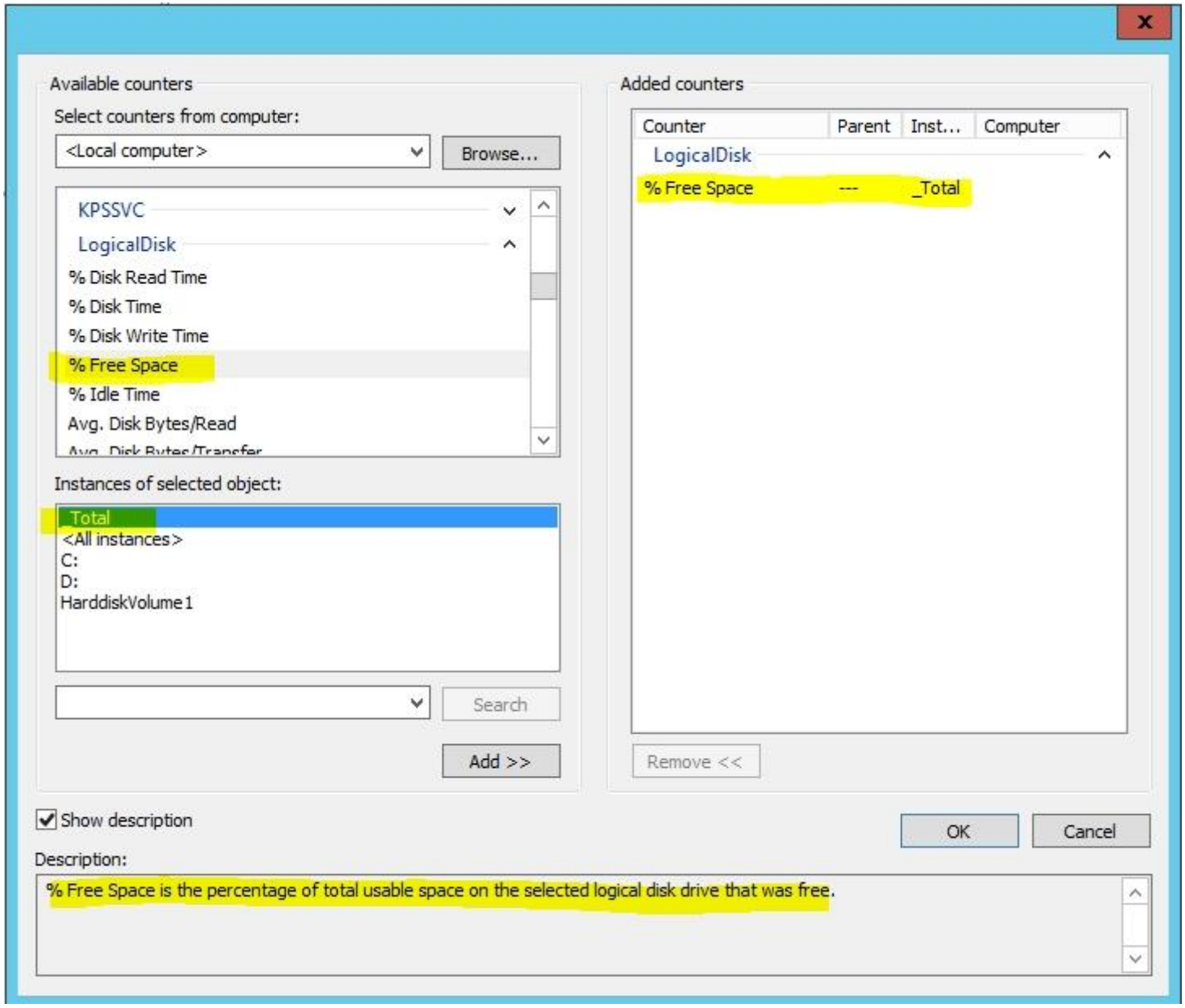
A. System configuration information
B. A performance counter
C. Event trace data
D. A Performance Counter Alert

Correct Answer: AD
Section: (none)
Explanation

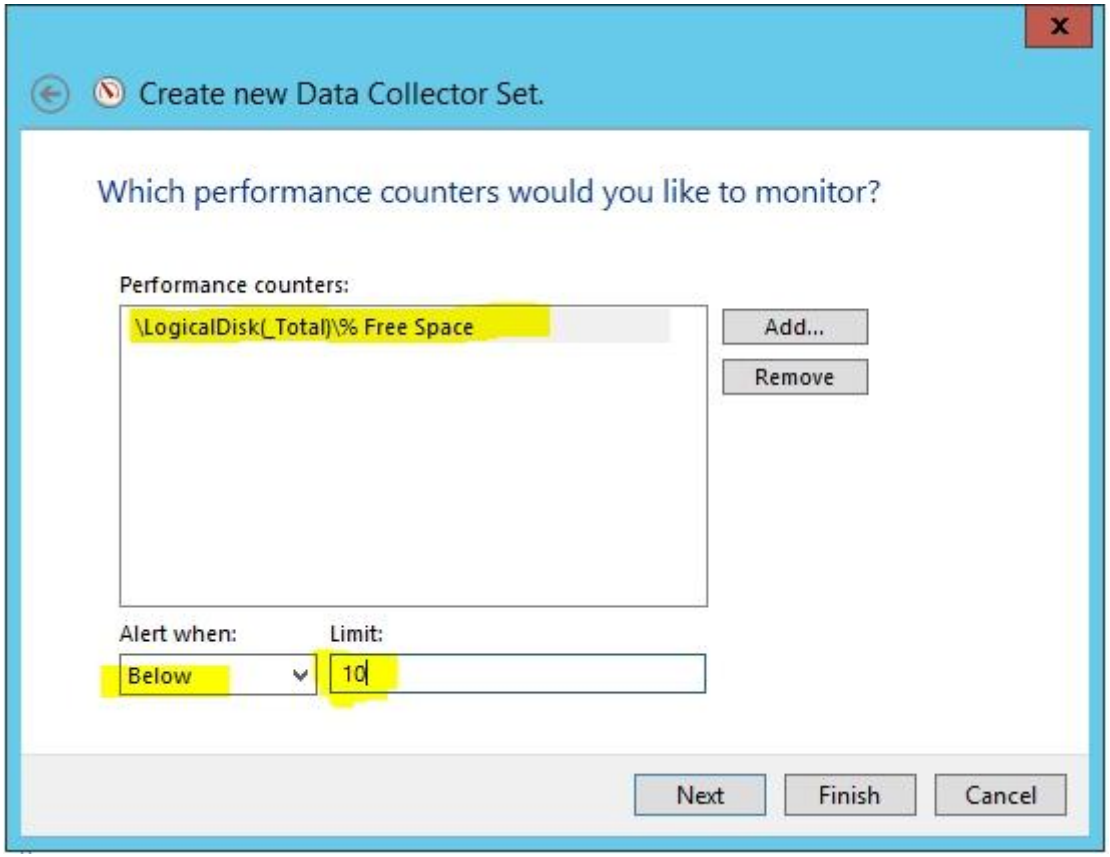
Explanation/Reference:
· Automatically run a program when the amount of total free disk space on Server1 drops below 10 percent of capacity.
- You can also configure alerts to start applications and performance logs
· Log the current values of several registry settings.
System configuration information allows you to record the state of, and changes to, registry keys.

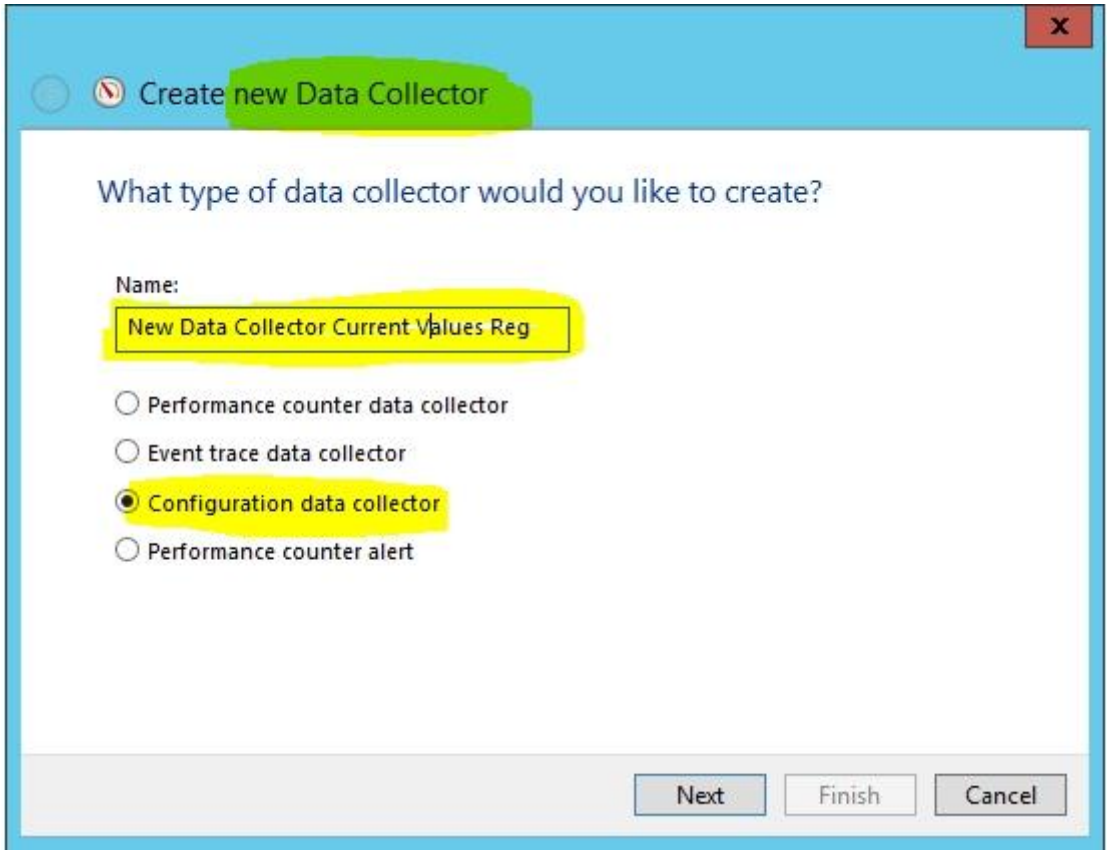


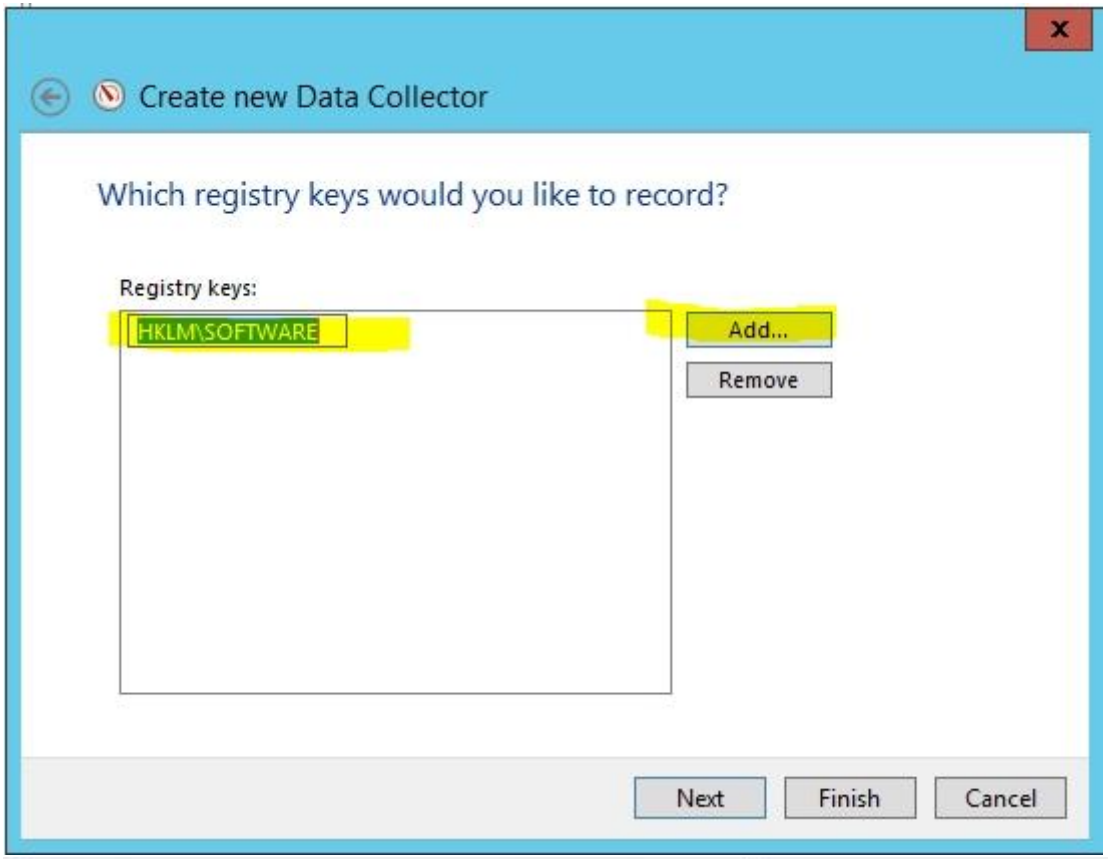

Create new Data Collector Set.
What type of data do you want to include?
Create data logs
Performance counter
Event trace data
System configuration information
Performance Counter Alert
Next
Finish
Cancel

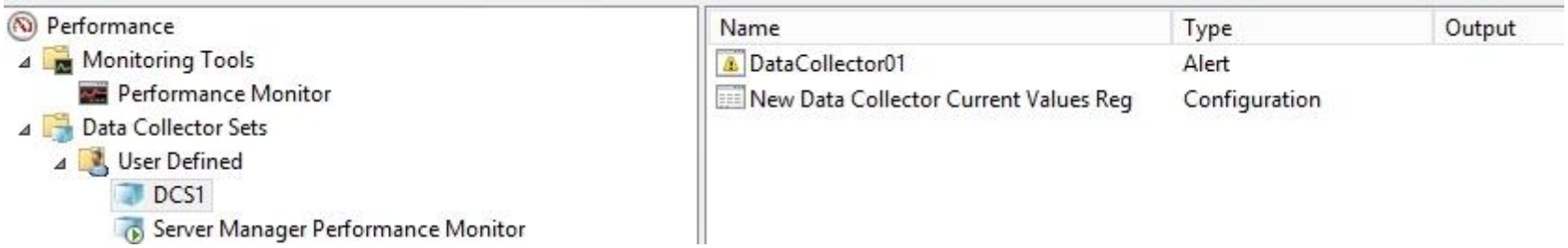

Available counters
Select counters from computer:
<Local computer>
Browse...
KPSSVC
LogicalDisk
% Disk Read Time
% Disk Time
% Disk Write Time
% Free Space
% Idle Time
Avg. Disk Bytes/Read
Instances of selected object:
Total
<All instances>
C:
D:
HarddiskVolume1
Search
Add >>
Added counters
Counter
Parent
Inst...
Computer
LogicalDisk
% Free Space

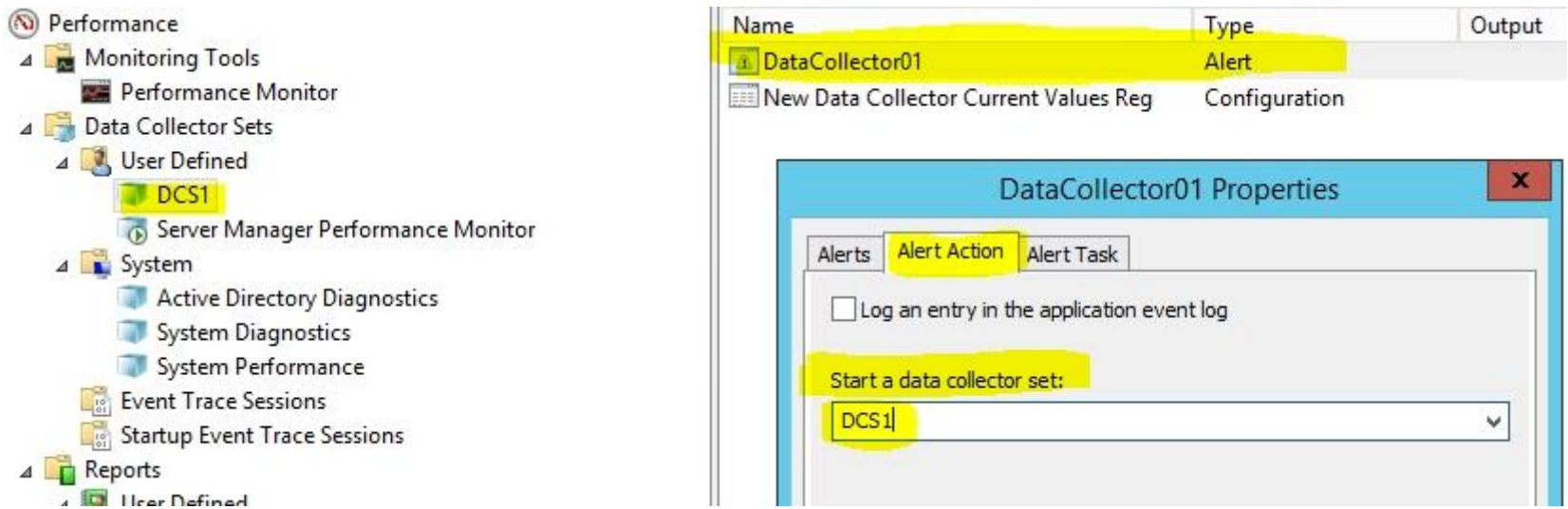
_Total
Remove <<
Show description
OK
Cancel
Description:
% Free Space is the percentage of total usable space on the selected logical disk drive that was free.

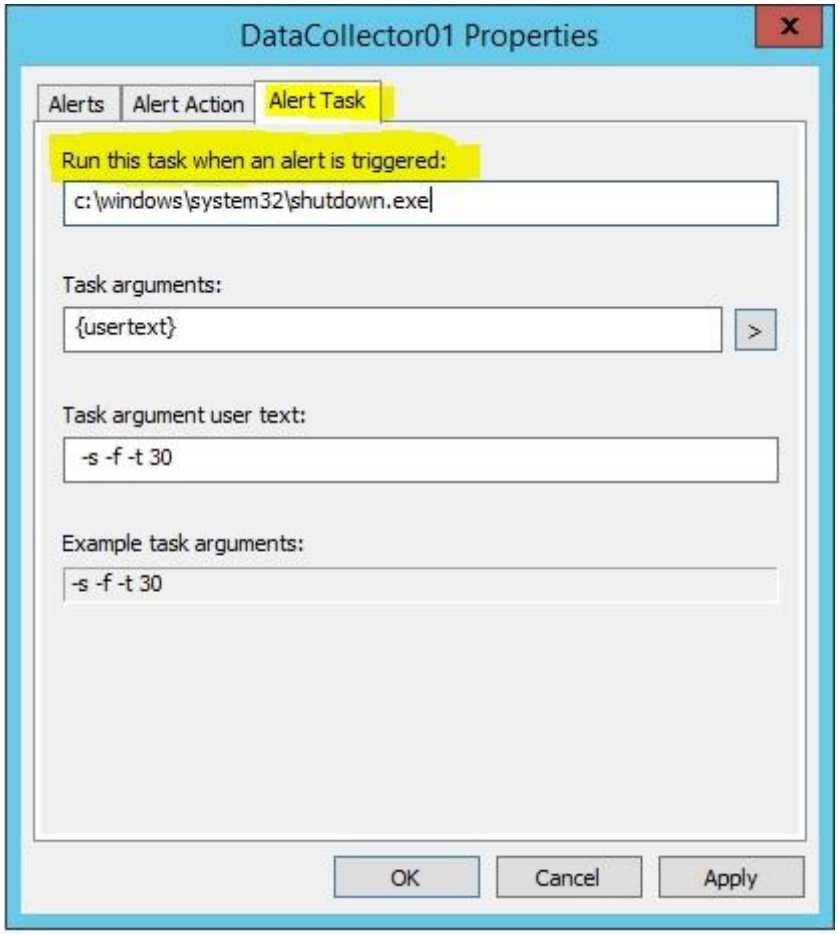

Create new Data Collector Set.
Which performance counters would you like to monitor?
Performance counters:
\LogicalDisk(_Total)\% Free Space
Add...
Remove
Alert when:
Limit:
Below
10
Next
Finish
Cancel


Create new Data Collector
What type of data collector would you like to create?
Name:
New Data Collector Current Values Reg
Performance counter data collector
Event trace data collector
Configuration data collector
Performance counter alert
Next
Finish
Cancel


Create new Data Collector
Which registry keys would you like to record?
Registry keys:
HKLM\SOFTWARE
Add...
Remove
Next
Finish
Cancel


Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
DCS1
Server Manager Performance Monitor
Name
Type
Output
DataCollector01
Alert
New Data Collector Current Values Reg
Configuration


Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
DCS1
Server Manager Performance Monitor
System
Active Directory Diagnostics
System Diagnostics
System Performance
Event Trace Sessions
Startup Event Trace Sessions
Reports
Name
Type
Output
DataCollector01
Alert
New Data Collector Current Values Reg
Configuration
DataCollector01 Properties
Alerts
Alert Action
Alert Task
Log an entry in the application event log
Start a data collector set:
DCS1

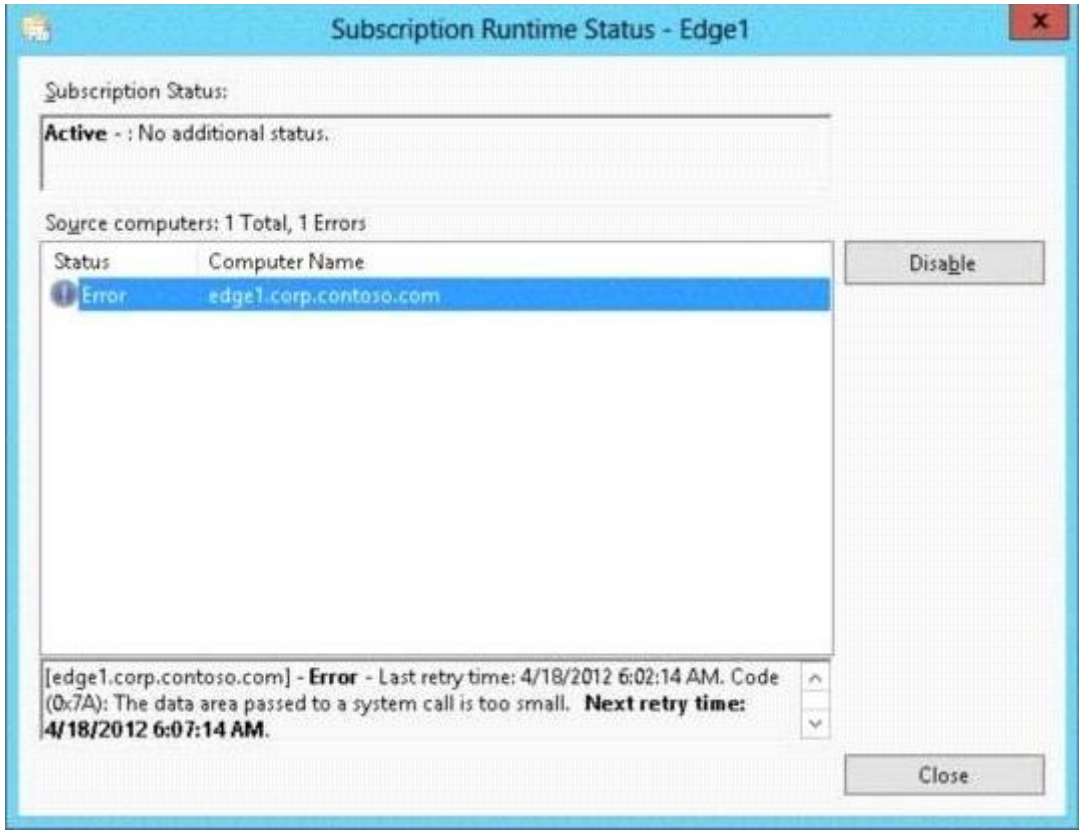


http://technet.microsoft.com/en-us/library/cc766404.aspx

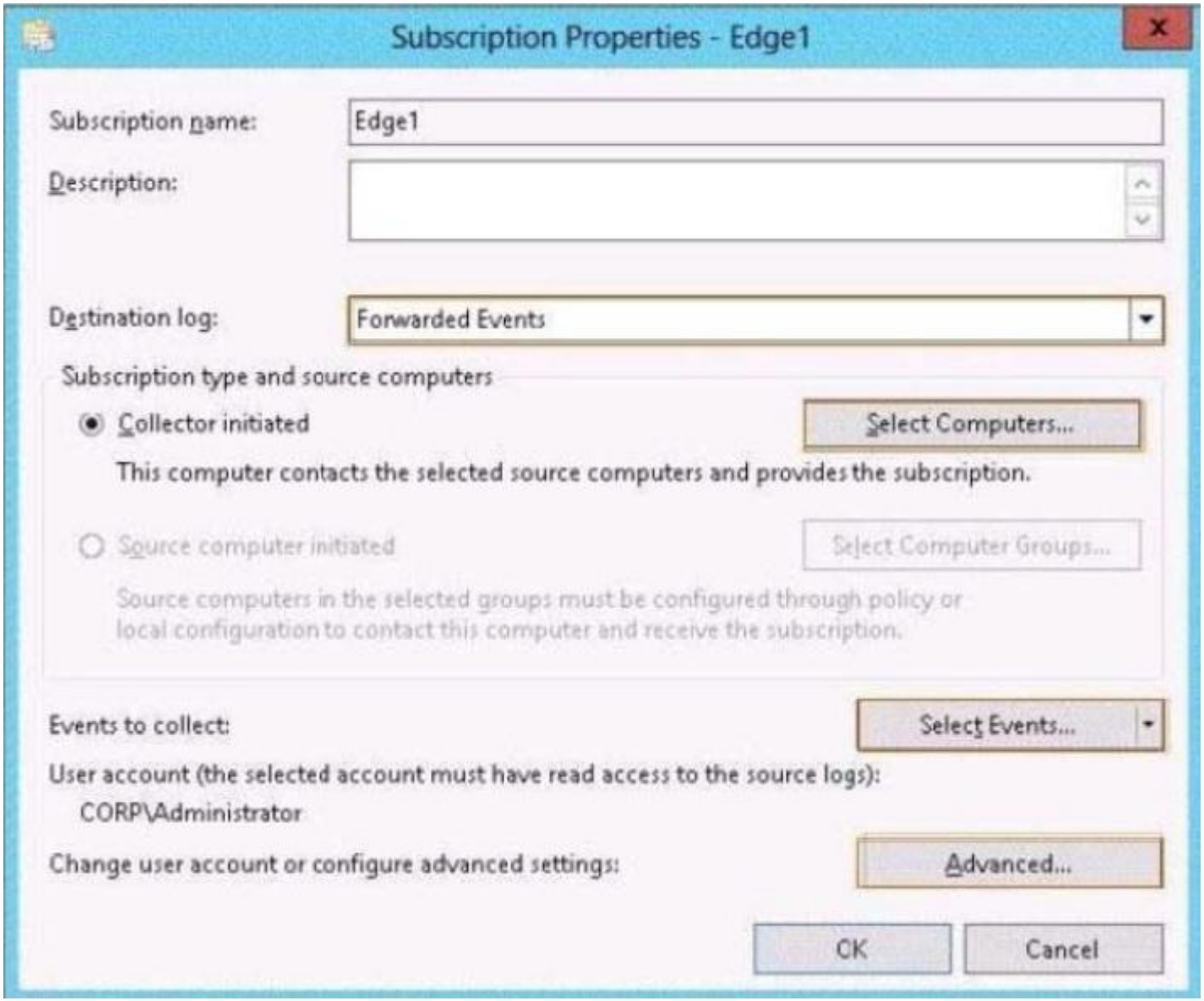
QUESTION 90
Your network contains an Active Directory domain named corp.contoso.com. The domain contains two member servers named Server1 and Edge1.
Both servers run Windows Server 2012. Your company wants to implement a central location where the system events from all of the servers in the domain will be collected.
From Server1, a network technician creates a collector-initiated subscription for Edge1. You discover that Server1 does not contain any events from Edge1.
You view the runtime status of the subscription as shown in the exhibit. (Click the Exhibit button.)
You need to ensure that the system events from Edge1 are collected on Server1.

What should you modify? To answer, select the appropriate object in the answer area.

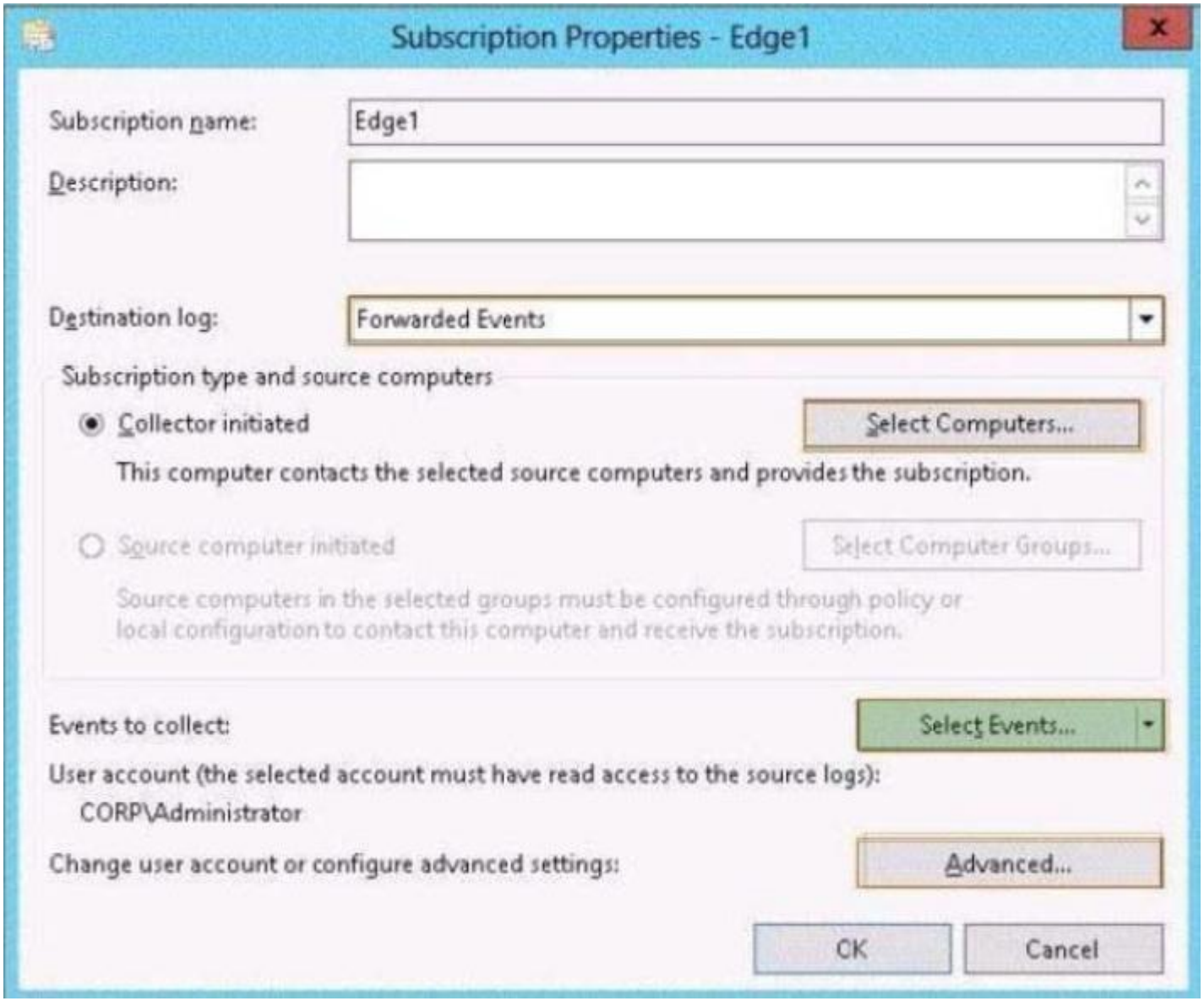
Exhibit:



Hot Area:



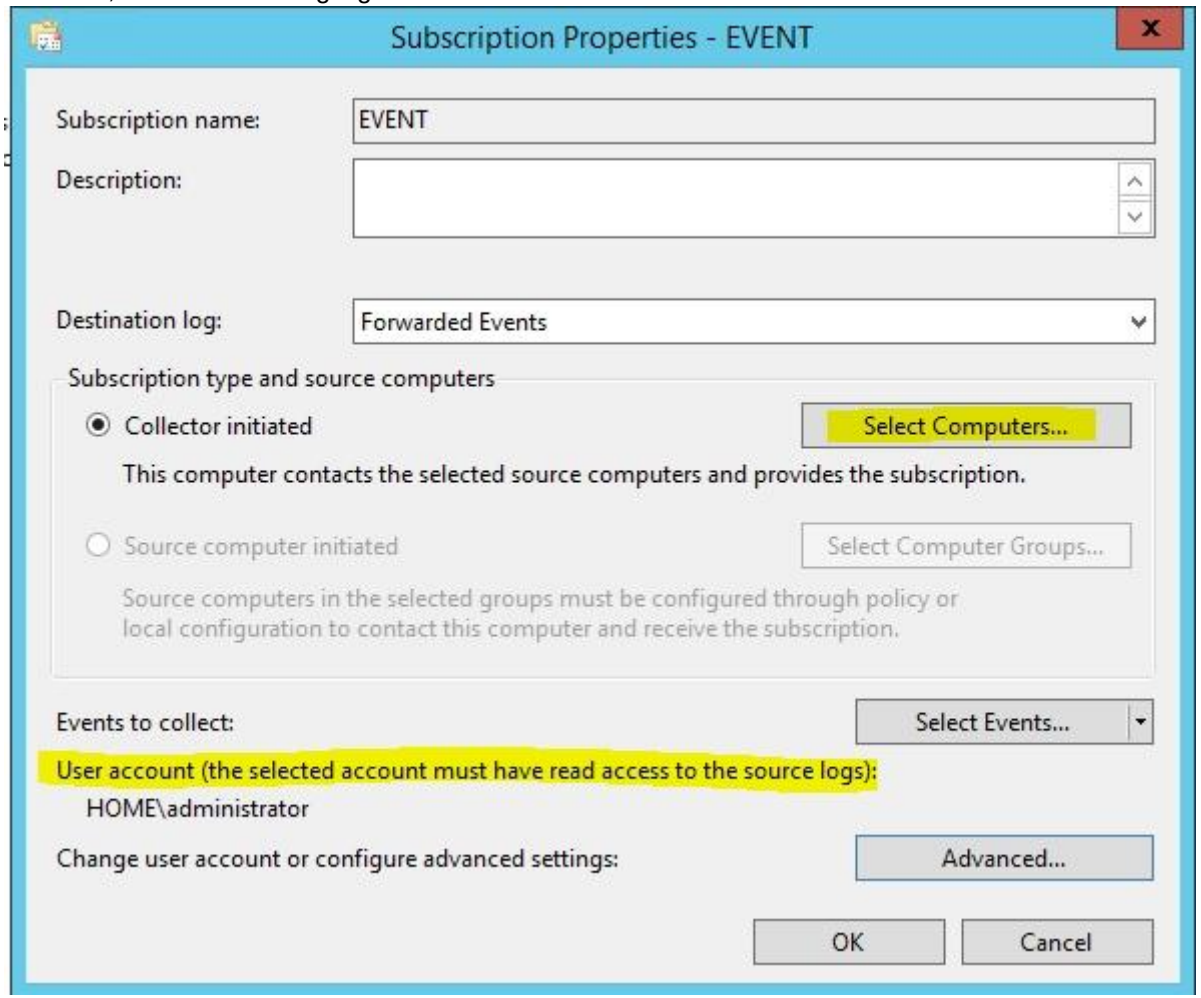
Correct Answer:

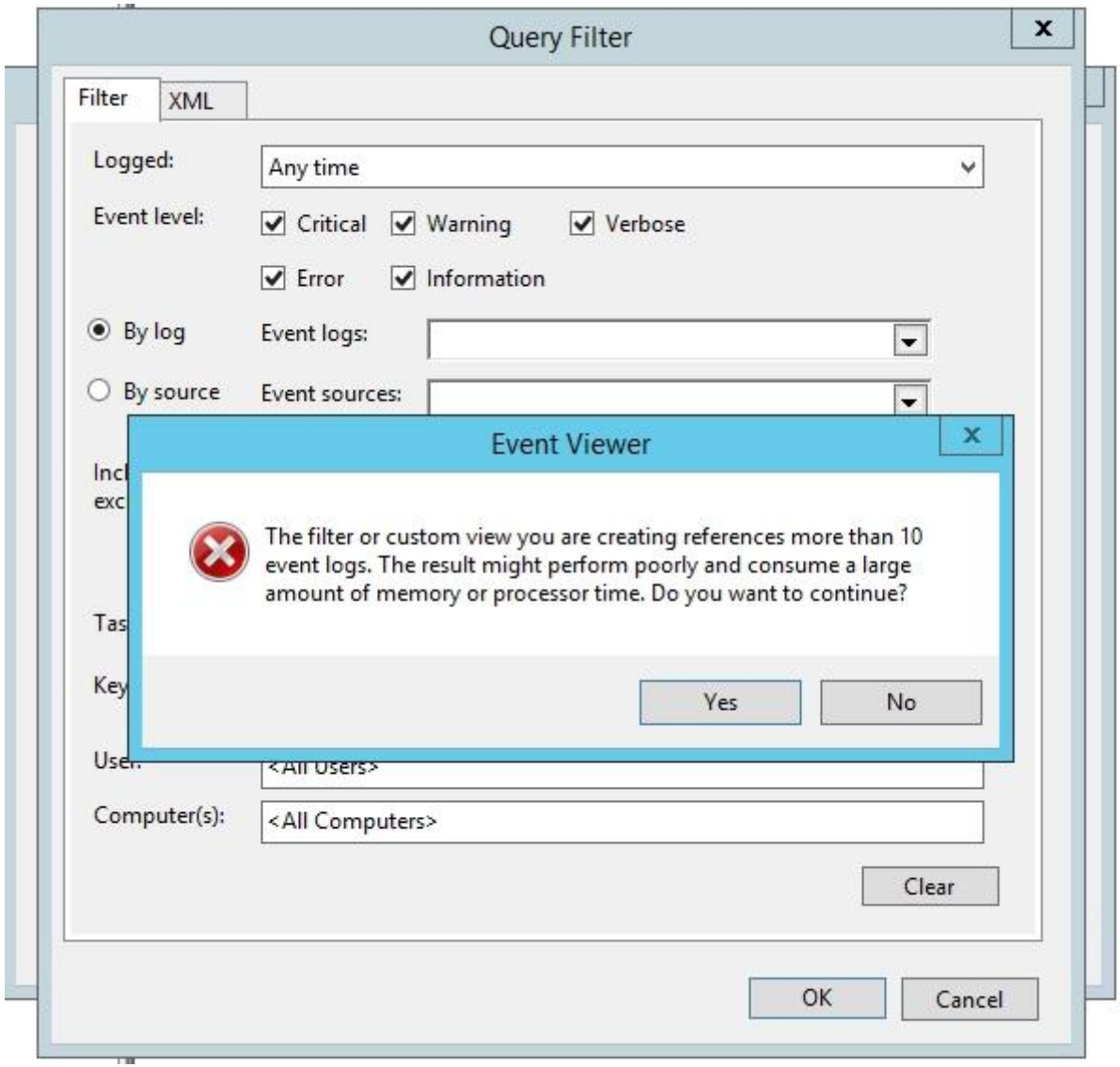


Section: (none)

Explanation

Explanation/Reference:
On Advanced window there is buttons for changing account, event delivery optimization and protocol only. I think this error may be produced by wrong event selection, so we need to highlight the Select Events button.





too many logs to collect in the filter???

http://www.sysadminlab.net/windows/forward-event-log-from-several-server-to-a-central-windows-2008-server

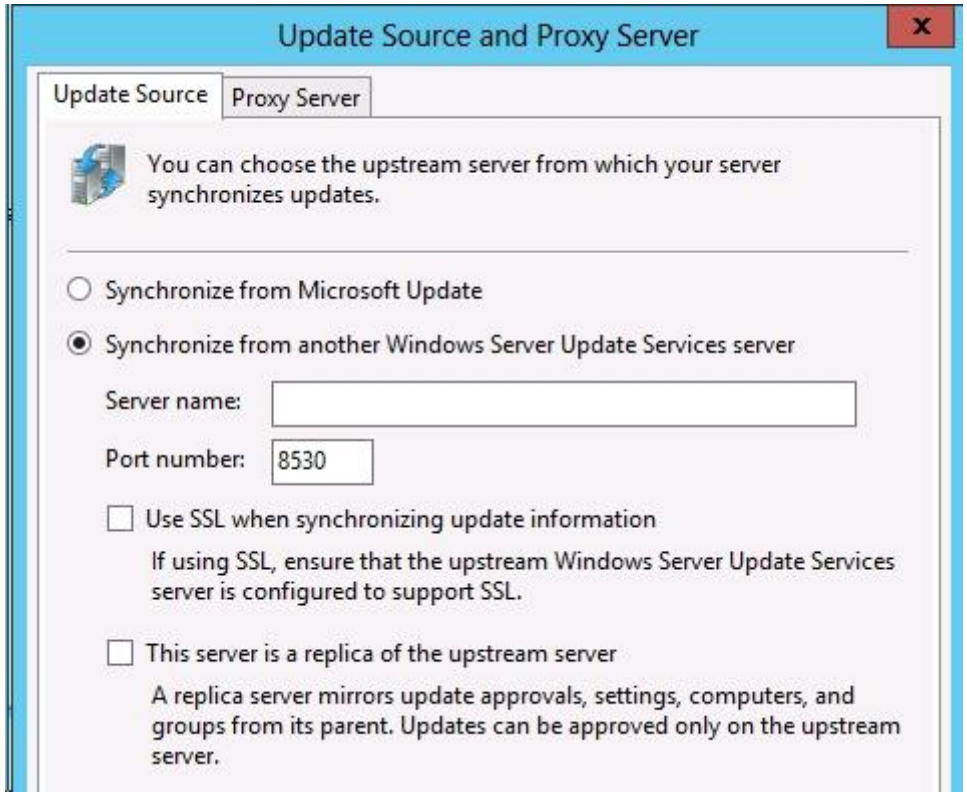
QUESTION 91
Your network contains an Active Directory domain named contoso.com. All client computers connect to the Internet by using a server that has Microsoft Forefront Threat Management Gateway (TMG) installed. You deploy a server named Server1 that runs Windows Server 2012.
You install the Windows Server Update Services server role on Server1. From the Windows Server Update Services Configuration Wizard, you click Start Connecting and you receive an HTTP error message.
You need to configure Server1 to download Windows updates from the Internet.

What should you do?

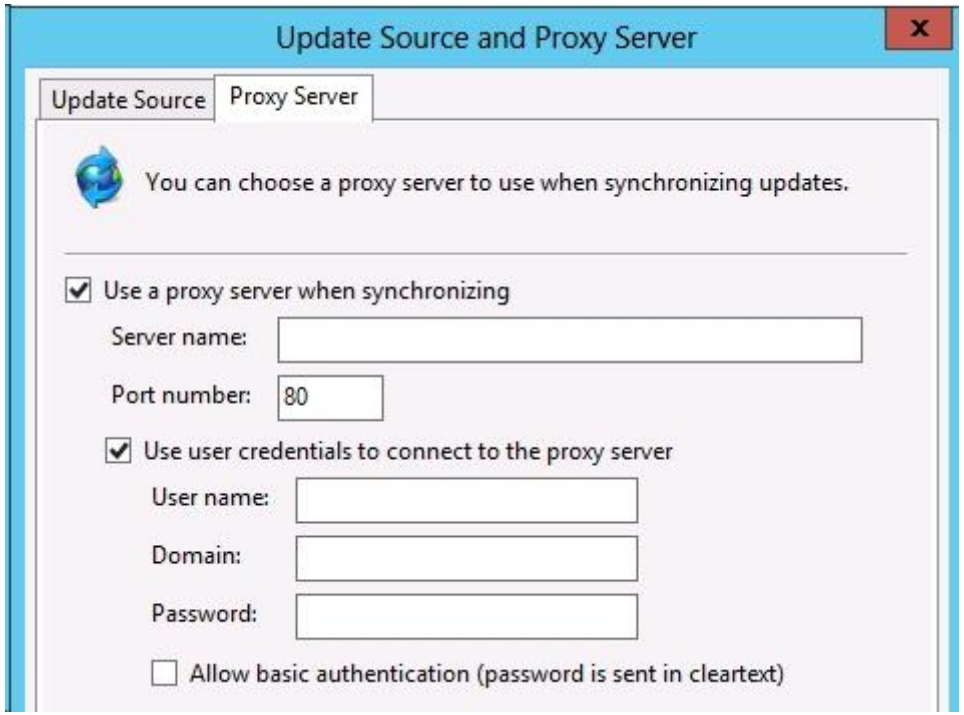
A. From the Update Services console, modify the Synchronization Schedule options.
B. From Windows Internet Explorer, modify the Connections settings.
C. From Windows Internet Explorer, modify the Security settings.
D. From the Update Services console, modify the Update Source and Proxy Server options.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:



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



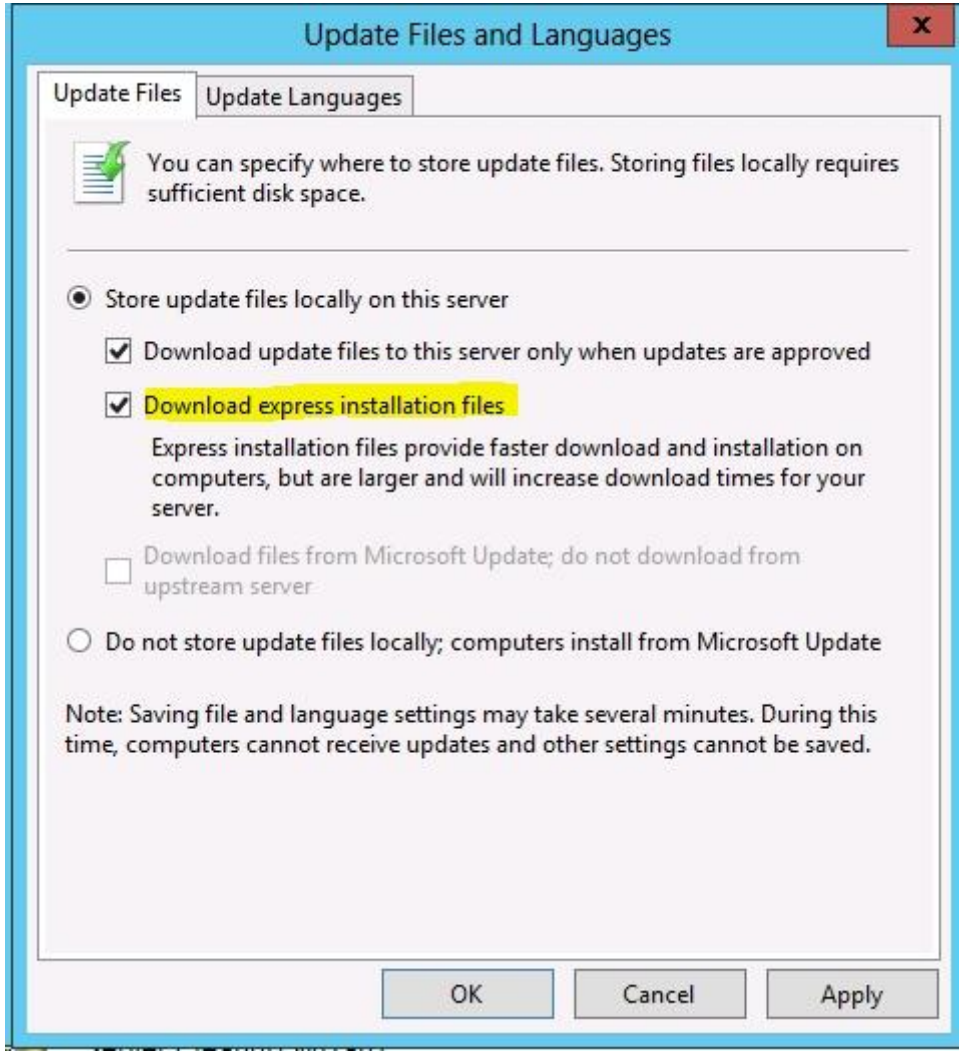
QUESTION 92
Your network contains a single Active Directory domain named contoso.com. The domain contains a member server named Server1 that runs Windows Server 2012.
Server1 has the Windows Server Updates Services server role installed and is configured to download updates from the Microsoft Update servers.
You need to ensure that Server1 downloads express installation files from the Microsoft Update servers.

What should you do from the Update Services console?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
To specify whether express installation files are downloaded during synchronization
In the left pane of the WSUS Administration console, click **Options**.
In **Update Files and Languages**, click the **Update Files** tab.
If you want to download express installation files, select the **Download express installation files** check box. If you do not want to download express installation files, clear the check box.



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

QUESTION 93
You have a VHD that contains an image of Windows Server 2012. You plan to apply updates to the image.
You need to ensure that only updates that can install without requiring a restart are installed.

Which DISM option should you use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
/PreventPending - Skips the installation of the package if the package or Windows image has pending online actions.

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

http://technet.microsoft.com/en-us/library/hh852164.aspx
http://technet.microsoft.com/en-us/library/hh825265.aspx

QUESTION 94
Your network contains an Active Directory domain named adatum.com. The domain contains a server named WDS1 that runs Windows Server 2012.
You install the Windows Deployment Services server role on WDS1. You have a virtual machine named VM1 that runs Windows Server 2012.
VM1 has several line-of-business applications installed.
You need to create an image of VM1 by using Windows Deployment Services.

Which type of image should you add to VM1 first?

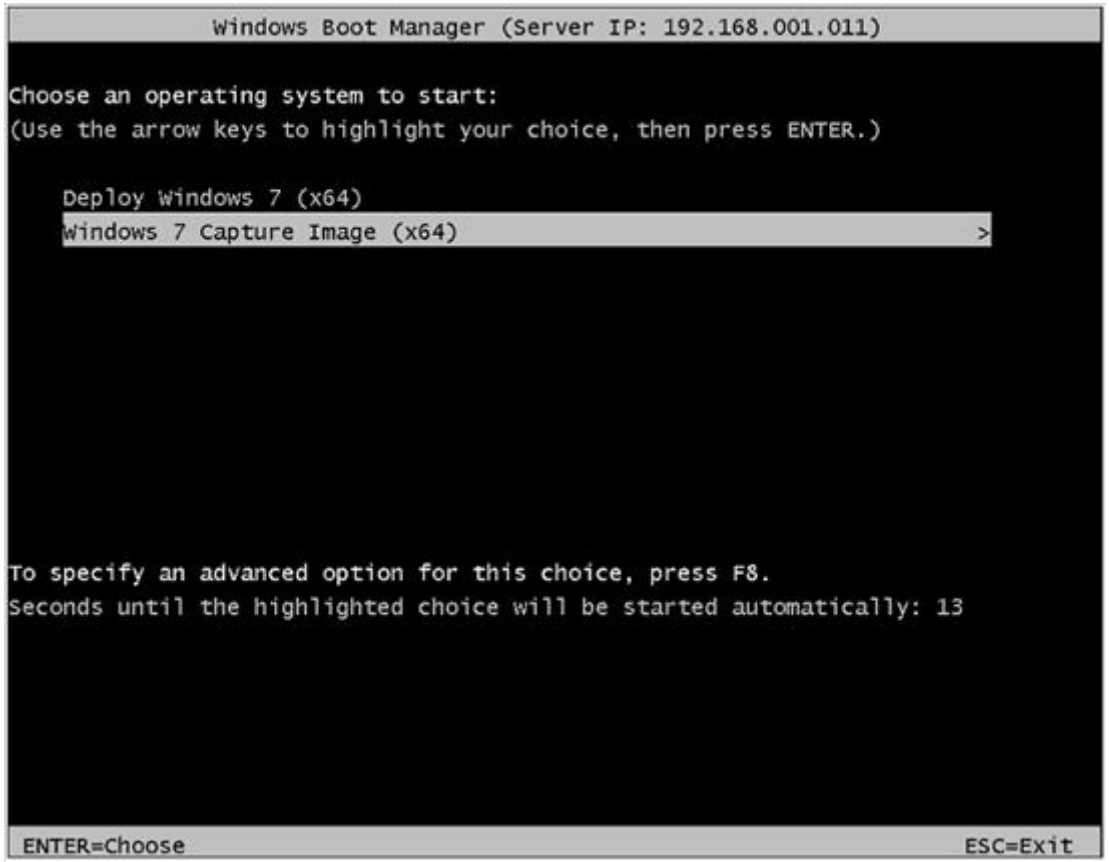
A. Capture
B. Install
C. Discovery
D. Boot

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Before you can make use of the PXE server, you must have a boot and capture image. This boot image contains the necessary files to install windows, such as setup.exe, which gives you the GUI that you see when installing windows. Boot images don't really need to be 'created' you simply get a Vista or Server 2008 Install disc and use the 'boot.wim' file located in the \sources directory. Note that in order to join a multicast; your boot image will need to be either the server 2008 boot.wim, a boot.wim from a Vista SP1 CD, or a Windows 7 Boot.wim. A normal Vista CD's boot.wim cannot join a multicast. I suggest using the server 2008 boot.wim. Multicasting will be explained later in this document.

"**A capture image is created from an existing boot image**. **You will create a new capture image by right-clicking on an existing boot image** and then selecting Create Capture Image option (see the following figure). The Create Capture Image Wizard will start."
"The source boot image will be used as a template for the new capture image file. The new capture image WIM file will be added in the location that you have specified."



http://social.technet.microsoft.com/wiki/contents/articles/11680.creating-a-capture-image-in-wds.aspx
http://itadmintips.wordpress.com/2011/05/19/wds-setup-guide-part-2-boot-image-setup/

QUESTION 95
You have a server named Server1 that runs Windows Server 2012. Server1 has the Windows Server Update Services server role installed.
You need to configure Windows Server Update Services (WSUS) to support Secure Sockets Layer (SSL).

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

A. Run the wsusutil.exe command.
B. From Internet Information Services (IIS) Manager, modify the bindings of the WSUS website.
C. From Internet Information Services (IIS) Manager, modify the connection strings of the WSUS website.

D. Run the iisreset.exe command.
E. Install a server certificate.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Certficate needs to be installed to IIS, Bindings modifies and wsutil run.

http://www.vkernel.ro/blog/configure-wsus-to-use-ssl

1- first we need to request a certificate for the WSUS web site, so open IIS, click the server name, then open Server Certificates.
On the Actions pane click Create Domain Certificate.

2- To add the signing certificate to the WSUS Web site in IIS 7.0
On the WSUS server, open Internet Information Services (IIS) Manager.
Expand Sites, right-click the WSUS Web site, and then click Edit Bindings.
In the Site Binding dialog box, select the https binding, and click Edit to open the Edit Site Binding dialog box.
Select the appropriate Web server certificate in the SSL certificate box, and then click OK.
Click Close to exit the Site Bindings dialog box, and then click OK to close Internet Information Services (IIS) Manager.

3- WSUSUtil.exe configuressl <FQDN of the software update point site system> (the name in your certificate)

WSUSUtil.exe configuressl <Intranet FQDN of the software update point site system>.

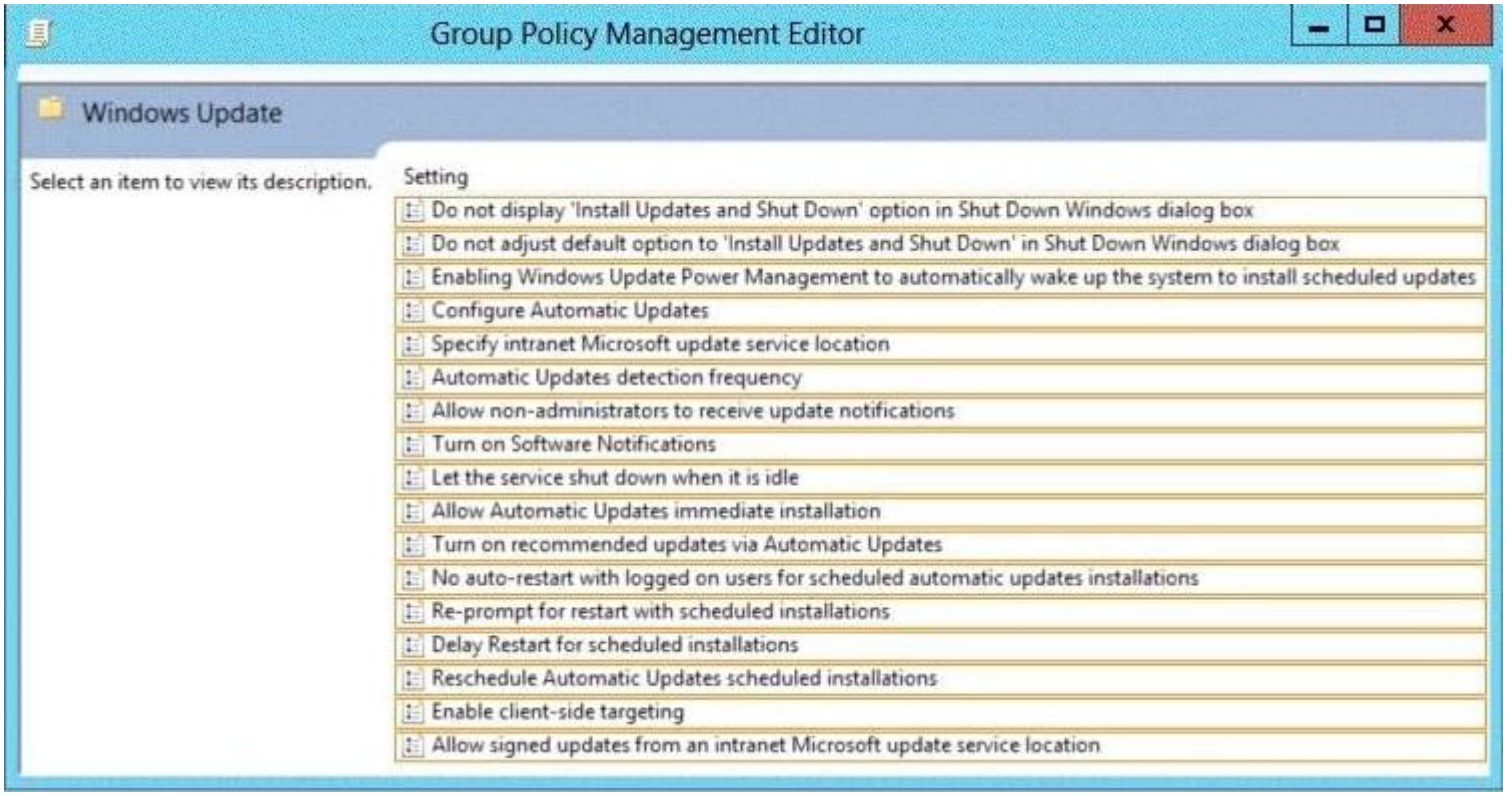
4- The next step is to point your clients to the correct url, by modifying the existing GPO or creating a new one. Open the policy Specify intranet Microsoft update service location and type the new url in the form https://YourWSUSserver.
The gpupdate /force command will just download all the GPO's and re-apply them to the client, it won't force the client to check for updates. For that you need to use **wuauclt /resetautorization /detectnow** followed by **wuauclt /reportnow**

http://technet.microsoft.com/en-us/library/bb680861.aspx

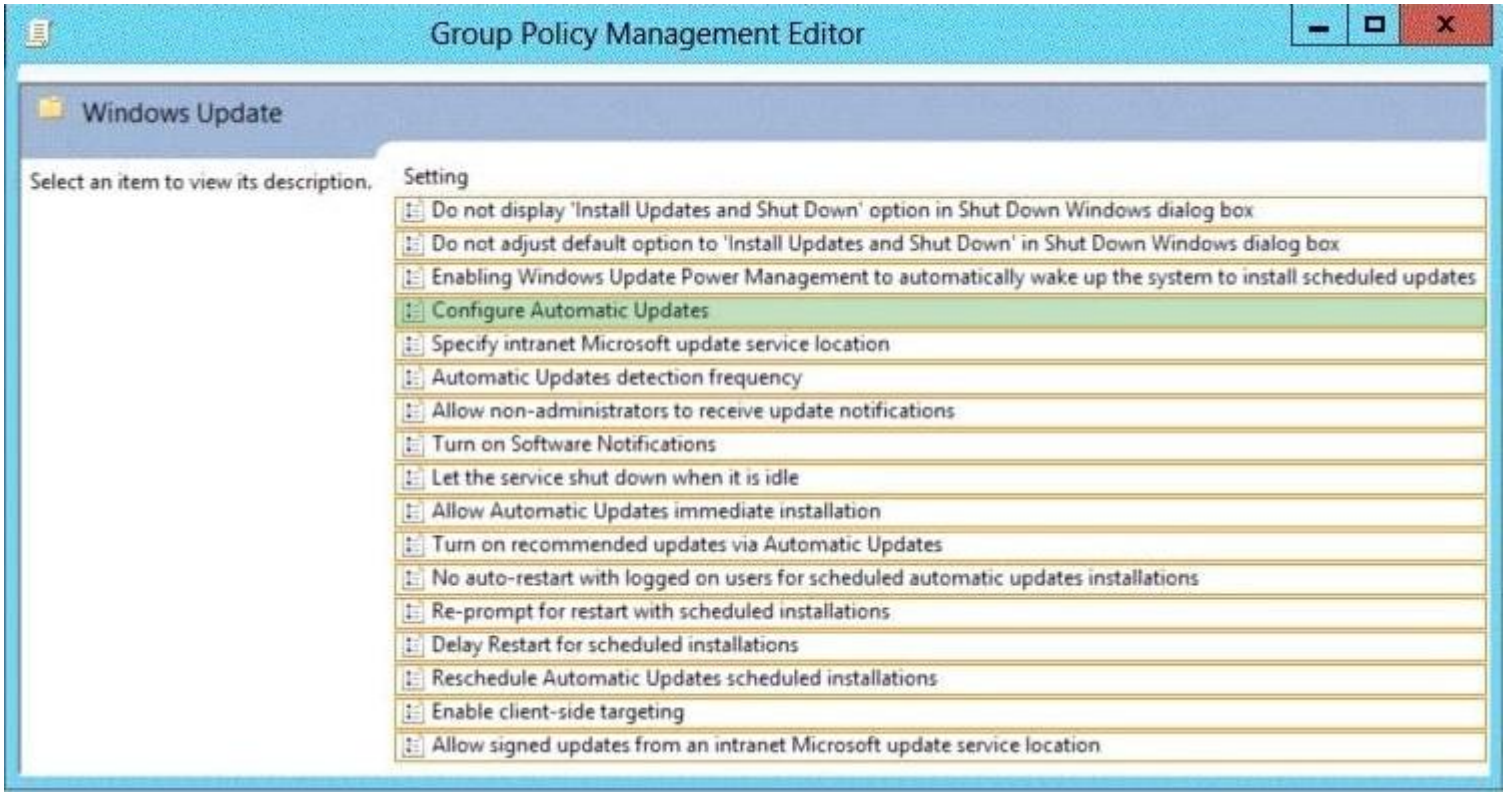
QUESTION 96
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012. Server1 has the Windows Server Update Services server role installed. You have a Group Policy object (GPO) that configures the Windows Update settings. You need to modify the GPO to configure all client computers to install Windows updates every Wednesday at 01:00.

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

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

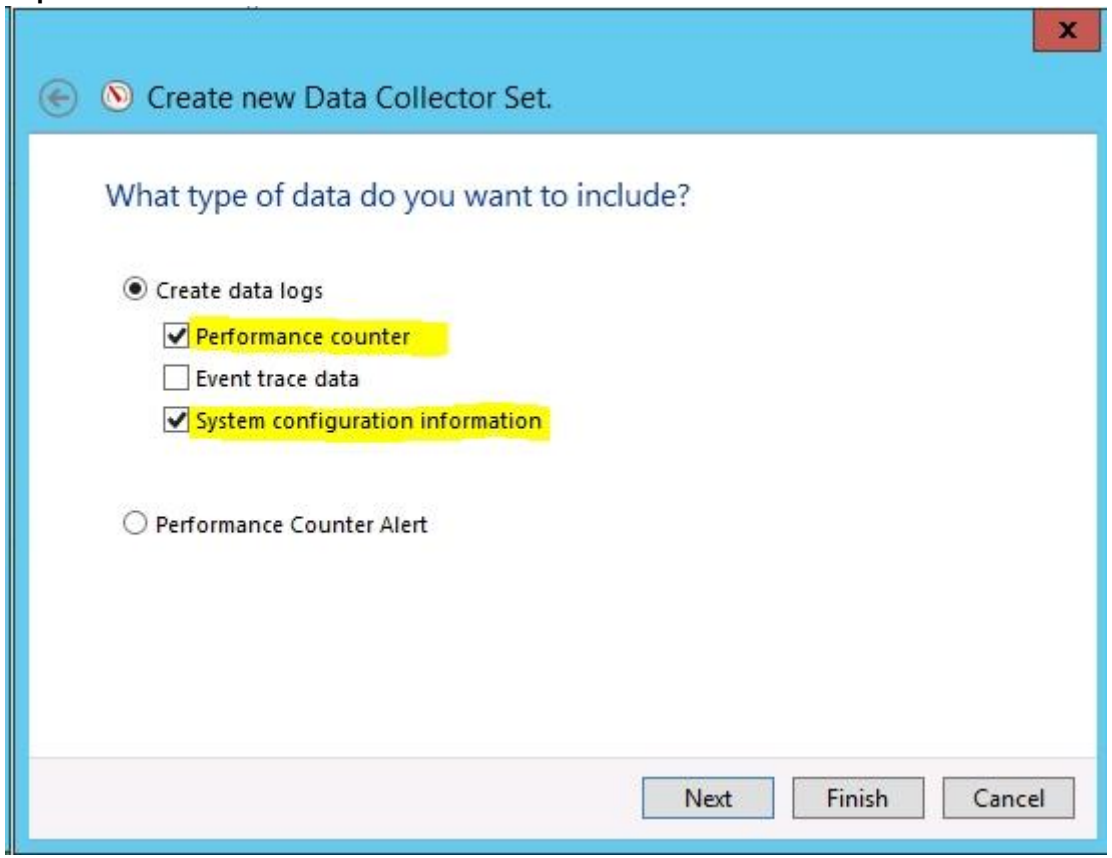
QUESTION 97
Your network contains a domain controller named DC1 that runs Windows Server 2012. You create a custom Data Collector Set (DCS) named DCS1.
You need to configure DCS1 to collect the following information:
· The amount of Active Directory data replicated between DC1 and the other domain controllers
· The current values of several registry settings

Which two should you configure in DCS1? (Each correct answer presents part of the solution. Choose two.)

A. Event trace data
B. System configuration information
C. A Performance Counter Alert
D. A Performance Counter

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:



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

QUESTION 98
You have a VHD that contains an image of Windows Server 2012.
You need to apply an update package to the image.

Which DISM option should you use?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Apply the update package (.msu) file by typing the following at a command prompt, replacing **<file_path>** with the full path to the configuration set:

At a command prompt, type the following command to add a specific package to the image. You can add multiple packages on one command line. They will be installed in the order listed in the command line.

```
Dism /Image:C:\test\offline /Add-Package /PackagePath:C:\packages\package1.cab /PackagePath:C:\packages\package2.cab
```

http://msdn.microsoft.com/en-us/library/ff794819.aspx
http://technet.microsoft.com/en-us/library/dd744559%28v=ws.10%29.aspx

QUESTION 99
You have Site1 with 400 desktops and Site2 with 150 desktops. You have a WSUS Server to deploy updates for both sites.

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

What should you configure?

A. Computer Groups
B. Security Groups
C. Synchronization Options

D. Classifications

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
WSUS allows you to target updates to groups of client computers, so you can ensure that specific computers always get the right updates at the most convenient times. For example, if all the computers in one department (such as the Accounting team) have a specific configuration, you can set up a group for that team, decide which updates their computers need and what time they should be installed, and then use WSUS reports to evaluate the updates for the team.

http://technet.microsoft.com/en-us/library/hh328559(v=ws.10).aspx

QUESTION 100
You have a WDS server named Server1 on Windows Server 2012.

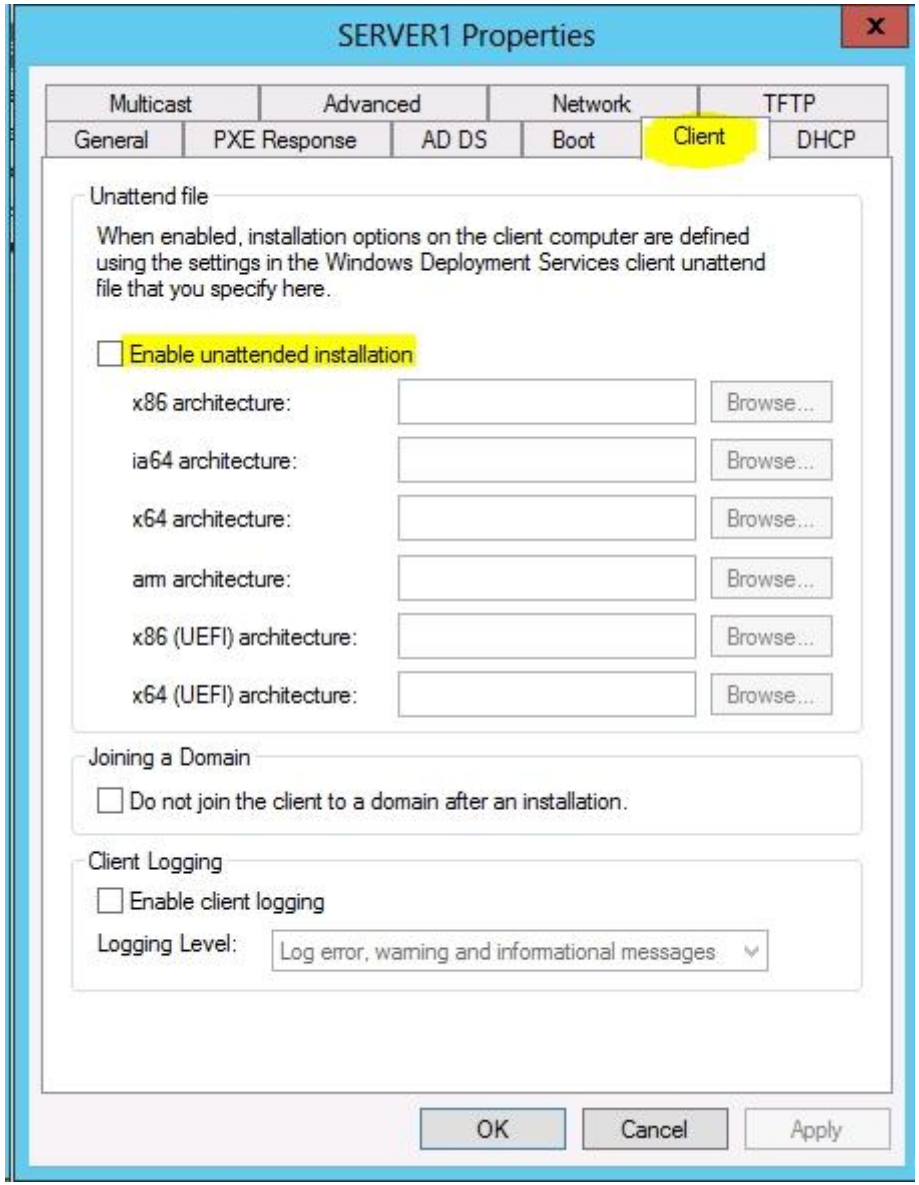
You need to automate the WDS deployment.

Which Tab should you configure?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
On the Client tab, select Enable unattended installation, browse to the appropriate unattend file, and then click Open.



http://technet.microsoft.com/en-us/library/dd637990(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/hh974416.aspx

QUESTION 101
WDS. how to import GUID and MAC address?

A. /get-AutoAddDevices
B. /get-Device
C. /add
D. /enable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Retrieves Windows Deployment Services information about a prestaged computer (that is, a physical computer that has been lined to a computer account in Active Directory Domain Services.

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

GUIDs can be confusing, as you can enter them in as binary strings or as a GUID string, and the only difference is the byte ordering and the absence of hyphens. MAC addresses can be entered with or without hyphens using either of the following lines of code:

wdsutil /get-device /id:01-23-45-67-89-AB
wdsutil /get-device /id:0123456789AB

You can get device information by binary string using this command:

wdsutil /get-device /id:ACEFA3E81F20694E953EB2DAA1E8B1B6

Or you can get-device information by GUID string using this command:

wdsutil /get-device /id:E8A3EFAC-201F-4E69-953-B2DAA1E8B1B6

http://technet.microsoft.com/pt-pt/magazine/2008.09.desktopfiles%28en-us%29.aspx
http://technet.microsoft.com/en-us/library/cc742044.aspx

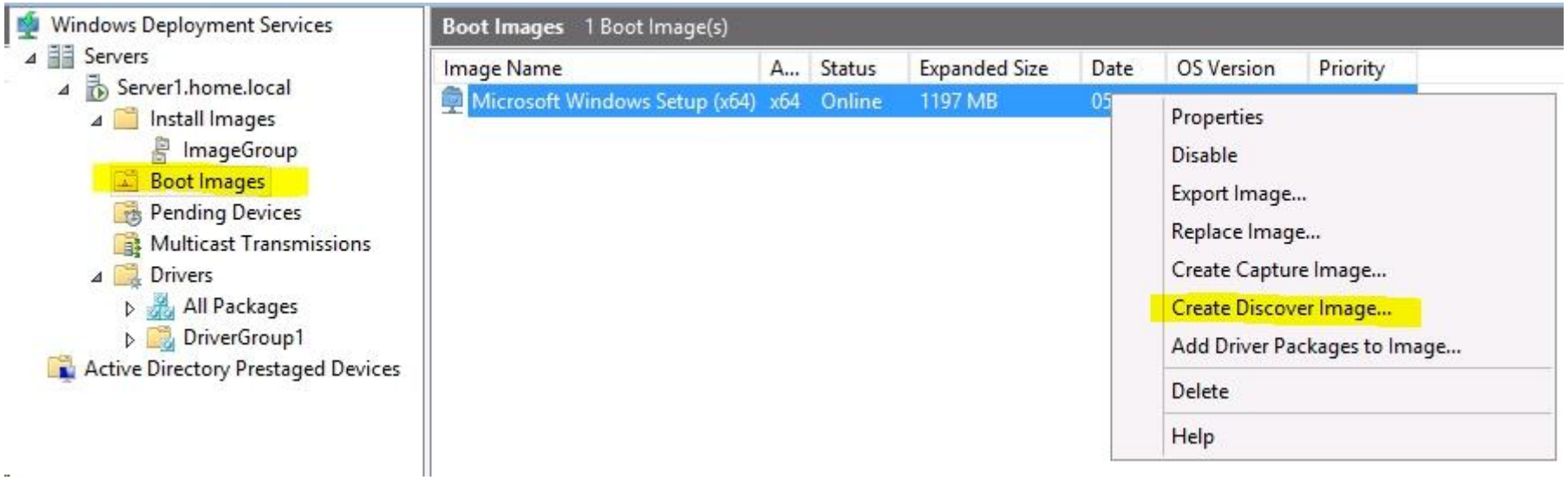
QUESTION 102
about not support PXE, you should first add mirrors

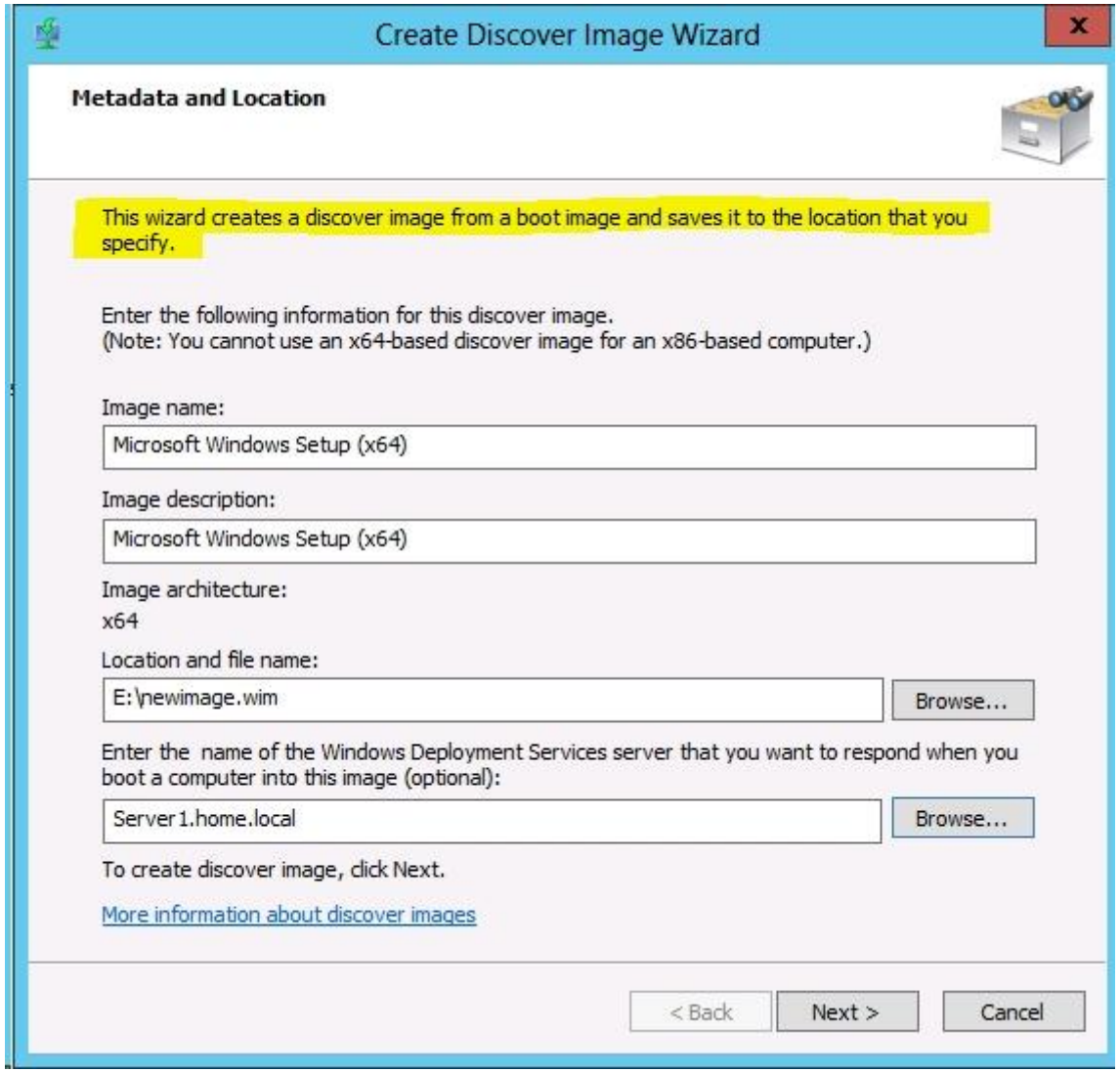
A. boot
B. install
C. discovery
D. capture

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://technet.microsoft.com/en-us/library/dd637996(v=ws.10).aspx

`WDSUTIL /New-DiscoverImage /Image:<name> /Architecture:{x86|x64|ia64} /DestinationImage /FilePath:<path and name to new file>`. To specify which server the discover image connects to, append `/WDSServer:<server name or IP>`.



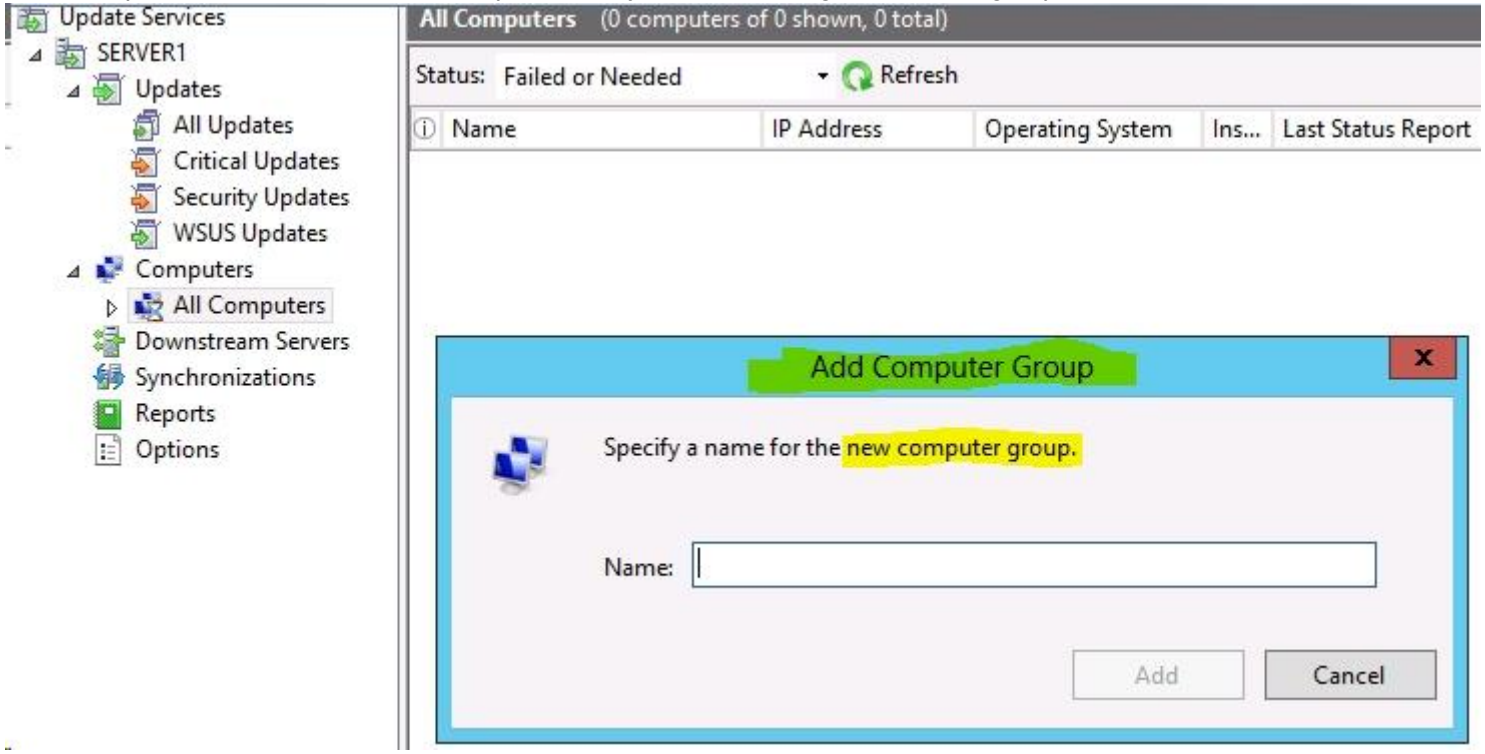


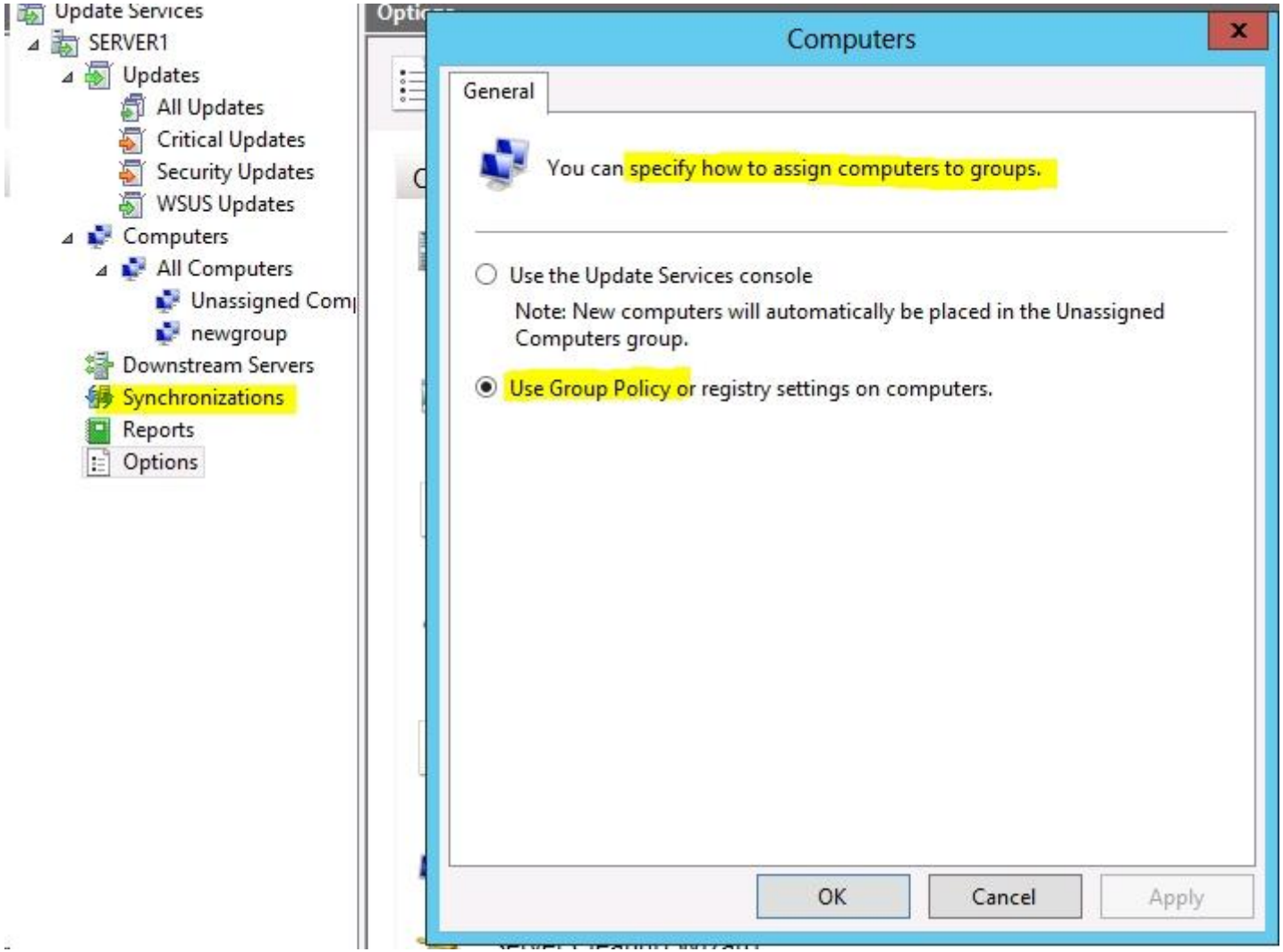
QUESTION 103
You are a admin (what a suprise huh?) you have wsus with 2 sites wich contain computers.
you want to have the ability to update the computers per site or together.
wich 3 steps do you do?

A. Create computer groups in wsus
B. Create synchronization options
C. Create GPO and configure updates
D. Under **Tasks**, click **Synchronize now**

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
In the WSUS Administration Console, under Update Services, expand the WSUS server, expand Computers, right-click All Computers, and then click Add Computer Group.
In the Add Computer Group dialog box, in Name, specify the name of the new group, and click then Add.
Click Computers, and then select the computers that you want to assign to this new group.





http://technet.microsoft.com/en-us/library/hh852346.aspx
http://technet.microsoft.com/en-us//library/cc708455%28v=ws.10%29.aspx

QUESTION 104

Which of the options should you configure for a WDS pre-staged computer name? You should select 2 of the 4 check boxes.

A. GUID o MAC-address preceding with nulls
B. `WdsClientUnattend`
C. `give the minimum required permission to a user who wants to promote a RODC.`
D. `ReferralServer`

Correct Answer: AC
Section: to review
Explanation

Explanation/Reference:
You can use Windows Deployment Services to link physical computers to computer account objects in Active Directory Domain Services (AD DS). This is called prestaging the client. Prestaged clients are also called known computers. Prestaging the client allows you to configure properties to control the installation for the client. For example, you can configure the network boot program and the unattend file that the client should receive, as well as the server from which the client should download the network boot program.

You can create a computer account object and associate it with a physical computer using the following methods:

- Using **WDSUTIL**. You can prestage client computers before they have attempted a network boot using the command line. For instructions, see the second procedure below. Note that you cannot prestage computers by using the Windows Deployment Services MMC snap-in, but you can set the Configure the Auto-Add Policy and approve or reject pending computers.

- Using the Active Directory Users and Computers snap-in. You can prestage client computers before they have attempted a network boot using AD DS. For instructions, see the first procedure below.

- Enabling the Auto-Add policy. If you enable this policy, when you approve the installation for an unknown client, the installation will proceed and a computer account will be created in AD DS for the client. For more information, see Configure the Auto-Add Policy.

- Using Windows Deployment Services as part of the image installation. By default, all operating system installations using Windows Deployment Services result in a client computer that is joined to a domain. You can disable this functionality using the Client tab of the server's properties page.

WDSUTIL /Add-Device /Device:Computer1 /ID: GUID / MAC

```
WDSUTIL /add-device /device:<devicename> /ID:<GUIDorMACAddress> <options>

For example: WDSUTIL /Add-Device /Device:Computer1 /ID:{E8A3EFAC-201F-4E69-953F-B2DAA1E8B1B6}
/ReferralServer:WDSServer1 /BootProgram:boot\x86\pxeboot.com /WDSClientUnattend:WDSClientUnattend\unattend.xml
/User:Domain\MyUser/JoinRights:Full /BootImagePath:boot\x86\images\boot.wim
/OU:"OU=MyOU,CN=Test,DC=Domain,DC=com"
```

http://technet.microsoft.com/en-us/library/cc754469.aspx

Click Start, right-click Command Prompt, and then click Run as administrator.

Type the following, where <devicename> is the name and <GUIDorMACAddress> is the identifier of the new computer. If you use a MAC address with the /ID option, you must precede it with twenty zeros (0).

WDSUTIL /add-device /device:<devicename> /ID:<GUIDorMACAddress> <options>

For example: WDSUTIL /Add-Device /Device:Computer1 /ID:{E8A3EFAC-201F-4E69-953F-B2DAA1E8B1B6} **/ReferralServer:**WDSServer1 /BootProgram:boot\x86\pxeboot.com **/WDSClientUnattend**:WDSClientUnattend\unattend.xml **/User:**Domain\MyUser/JoinRights:Full **/BootImagePath**:boot\x86\images\boot.wim /OU:"OU=MyOU,CN=Test,DC=Domain,DC=com"

Note:
Before you can prestage computers, you need to update your Active Directory Users and Computers console. The following update will enable the screen which allows you to input the GUID when creating new computer accounts.

You need the following files from your server and they have to be the same architecture, so if your workstation is x64, then so does the server.
%systemroot%\system32\imadmui.dll
%systemroot%\system32\en-US\imadmui.dll.mui
Copy those files to the same location on your workstation.
Register the dll using the following command as an administrator (remember UAC):regsvr32 imadmui.dll

http://technet.microsoft.com/en-us/library/cc754289%28v=ws.10%29.aspx

To prestage a client computer to boot from a different server

Using the MMC	Using WDSUTIL
N/A	1. Click **Start**, right-click **Command Prompt**, and click **Run as administrator**. 2. Run `WDSUTIL /Set-Device /Device:<name> /ReferralServer:<ServerName>`.

To prestage a client computer to use an unattend file other than the default for the Windows PE phase of unattended setup

Using the MMC	Using WDSUTIL
N/A	1. Click **Start**, right-click **Command Prompt**, and click **Run as administrator**. 2. Run `WDSUTIL /Set-Device /Device:<name> /WDSClientUnattend:<path>`, where the path is relative to the unattend file you want from the RemoteInstall folder.

QUESTION 105

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2008 R2.

You plan to test Windows Server 2012 by using native-boot virtual hard disks (VHDs).

You attach a new VHD to Server1.

You need to install Windows Server 2102 in the VHD.

What should you do?

A. Run dism.exe and specify the /apply-image parameter.
B. Run dism.exe and specify the /append-image parameter.
C. Run imagex.exe and specify the /export parameter.
D. Run imagex.exe and specify the /append parameter.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Imagex is included in the Windows Automated Installation Kit or WAIK for short.
As of Windows 8's release **imagex has been deprecated**. The imaging functionality has been added to the dism tool. DISM stands for "Deployment Image Servicing and Management"

Dism /Append-Image /ImageFile:install.wim /CaptureDir:D:\ /Name:Drive-D
Dism /Apply-Image /ImageFile:d:\my-image.wim /index:1 /ApplyDir:c:\

What is native VHD boot?

Native VHD boot enables a physical computer to be booted directly from a virtual hard disk (VHD) with no requirement for virtualization software (such as Microsoft® Virtual PC or Hyper-V™). Native VHD boot is made possible with the addition of a mini-port driver that is responsible for all input/output (IO) operations to and from the disk. Earlier versions of Windows (such as Windows Vista®, Windows XP, and Windows 2000) do not support native VHD boot, and therefore, you cannot use them to implement the functionality described in this document.

http://technet.microsoft.com/en-us/library/gg318051%28v=ws.10%29.aspx

With the introduction of native VHD boot, it is possible to achieve a single image deployment strategy for both physical and virtual machines. As long as the operating system that resides on the VHD is generalized and hosts Windows 7 Enterprise, Windows 7 Ultimate, or Windows Server 2008 R2 (all editions), the VHD can be used in both environments.

To make a VHD available for use (either one you have just created or another existing VHD), on the Action menu, select Attach VHD, and then specify the location of the VHD, using a fully qualified path.

Option: **/Apply-Image** Arguments: **/ImageFile:** *<path_to_image_file>* [**/SWMFile:** *<pattern>*] **/ApplyDir:** *<target_directory>* {**/Index:** *< image_index>* | **/Name:** *<image_name>*} [**/CheckIntegrity**] [**/Verify**] [**/NoRpFix**] [**/ConfirmTrustedFile**]	Applies an image to a specified drive. This command-line option does not apply to virtual hard disk (VHD) files. **/CheckIntegrity** detects and tracks .wim file corruption when used with capture, unmount, export, and commit operations. **/CheckIntegrity** stops the operation if DISM detects that the .wim file is corrupted when used with apply and mount operations. **/Verify** checks for errors and file duplication. **/NoRpFix** disables the reparse point tag fix. A reparse point is a file that contains a link to another file on the file system. If **/NoRpFix** is not specified, reparse points that resolve to paths outside the value specified by **/ImageFile** will not be captured. **/SWMFile** enables you to reference split .wim files (SWMs). *pattern* is the naming pattern and location of split files. You can also specify wildcard characters. For example, "E:\image\install*.swm" will apply all of the split files in the E:\image directory named install1.swm, install2.swm, and so on. **/ConfirmTrustedFile** validates the image for Trusted Desktop on a Windows 8 or Windows 8.1 Preview. This option can only be run on a computer running at least Windows® Preinstallation Environment (Windows PE) 4.0. Example: **Dism /apply-image /imagefile:install.wim /index:1 /ApplyDir:D:** **Dism /apply-image /imagefile:install.swm /swmfile:install*.swm /index:1 /applydir:D:** **Dism /apply-image /imagefile:install.swm /swmfile:install*.sw**

http://technet.microsoft.com/en-us/library/hh824910.aspx
http://technet.microsoft.com/en-us/library/hh825258.aspx
http://technet.microsoft.com/en-us/library/dd851645.aspx

QUESTION 106
You have a server named Admin1 that runs Windows Server 2012.

On Admin1, 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) quota on the C:\Logs folder
B. A File Server Resource Manager (FSRM) file screen on the C:\Logs folder
C. A schedule for DCS1
D. The Data Manager settings of DCS1

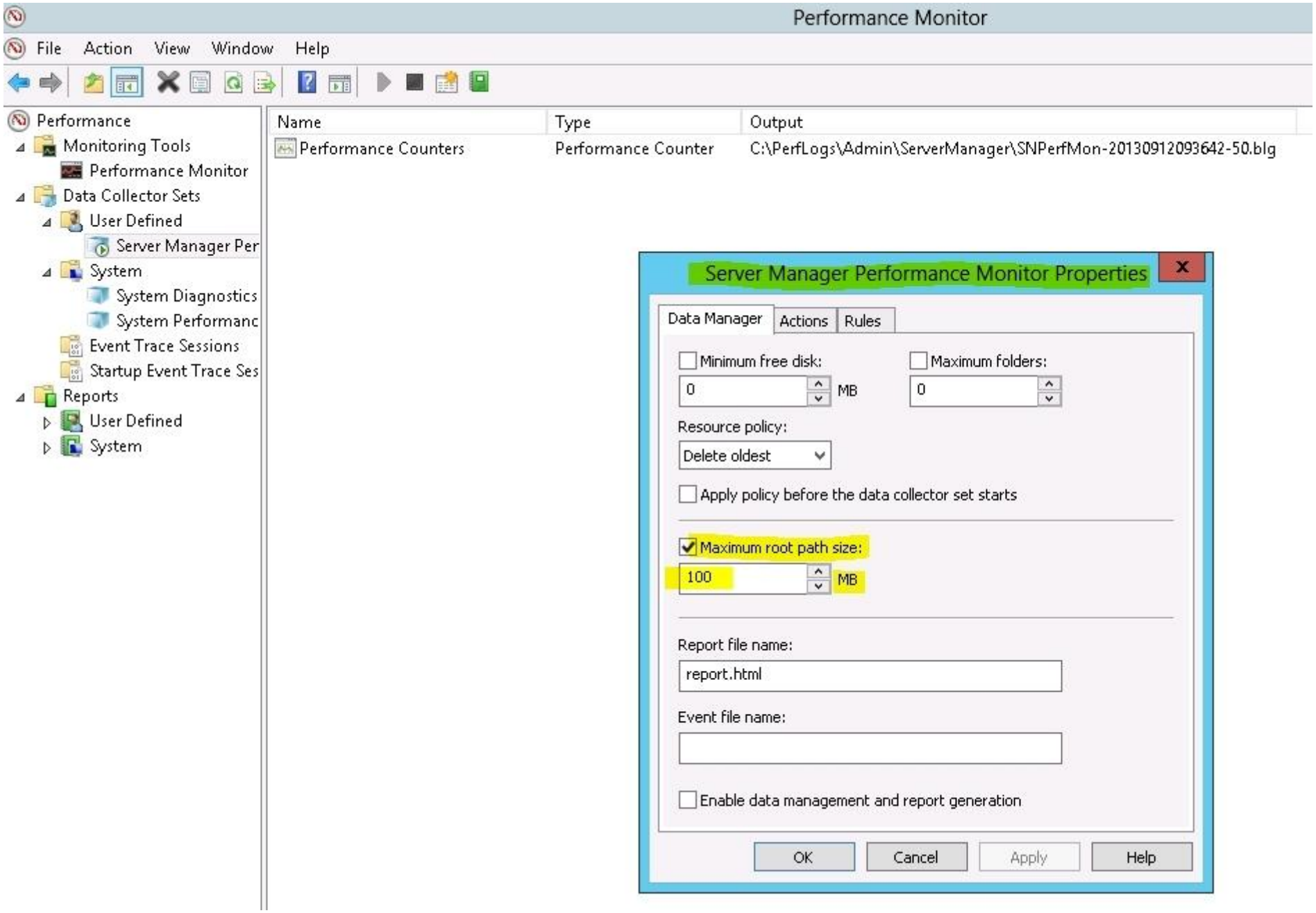
Correct Answer: D
Section: to review
Explanation

Explanation/Reference:
Data Collector Sets create a raw log data file, in addition to optional report files. With Data Management, you can configure how log data, reports, and compressed data are stored for each Data Collector Set. Membership in the local Performance Log Users or Administrators group, or equivalent, is the minimum required to complete this procedure.

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 Data Manager properties table for details on each option.
   - When the **Minimum free disk** or **Maximum folders** check box 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 the **Apply policy before the data collector set starts** check box is selected, previous data will be deleted according to your selections before the Data Collector Set creates its next log file.
   - When the **Maximum root path size** check box is selected, previous data will be deleted according to your selections when the root log folder size limit is reached.

http://technet.microsoft.com/en-us/library/dd744567%28v=ws.10%29.aspx


Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
Server Manager Per
System
System Diagnostics
System Performanc
Event Trace Sessions
Startup Event Trace Ses
Reports
User Defined
System
Name
Type
Output
Performance Counters
Performance Counter
C:\PerfLogs\Admin\ServerManager\SNPerfMon-20130912093642-50.blg
Server Manager Performance Monitor Properties
Data Manager
Actions
Rules
Minimum free disk:
0
MB
Maximum folders:
0
Resource policy:
Delete oldest
Apply policy before the data collector set starts
Maximum root path size:
100
MB
Report file name:
report.html
Event file name:
Enable data management and report generation
OK
Cancel
Apply
Help

http://technet.microsoft.com/en-us/library/cc765998.aspx
http://sourcedaddy.com/windows-7/using-data-manager-view-performance-data.html

QUESTION 107
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 and a server named Server2 that has the File Services server role installed.

You install the Windows Deployment Services server role on Server1.

You plan to use Server2 as a reference computer.

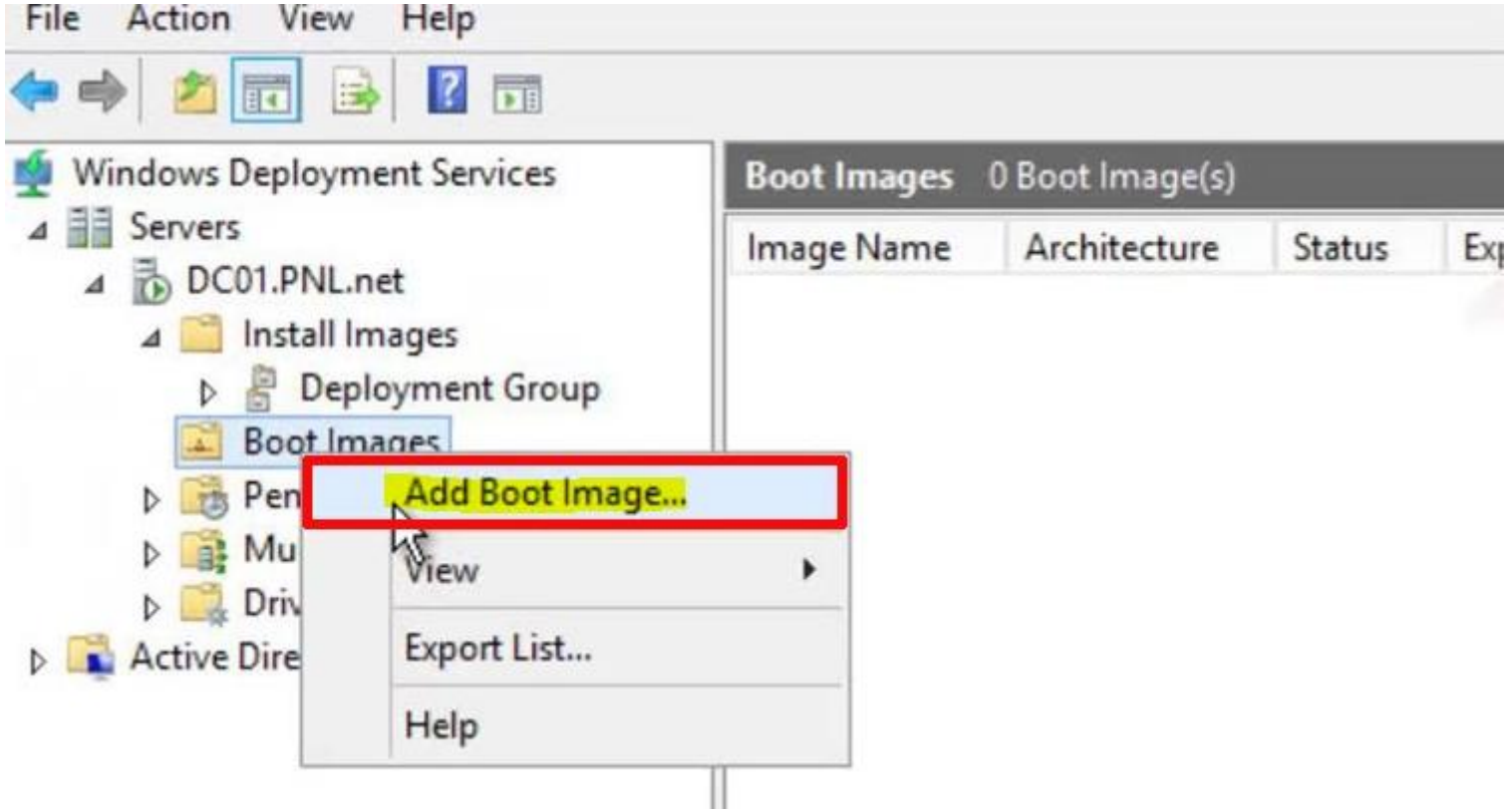
You need to create an image of Server2 by using Windows Deployment Services.

Which type of image should you add to Server1 first?

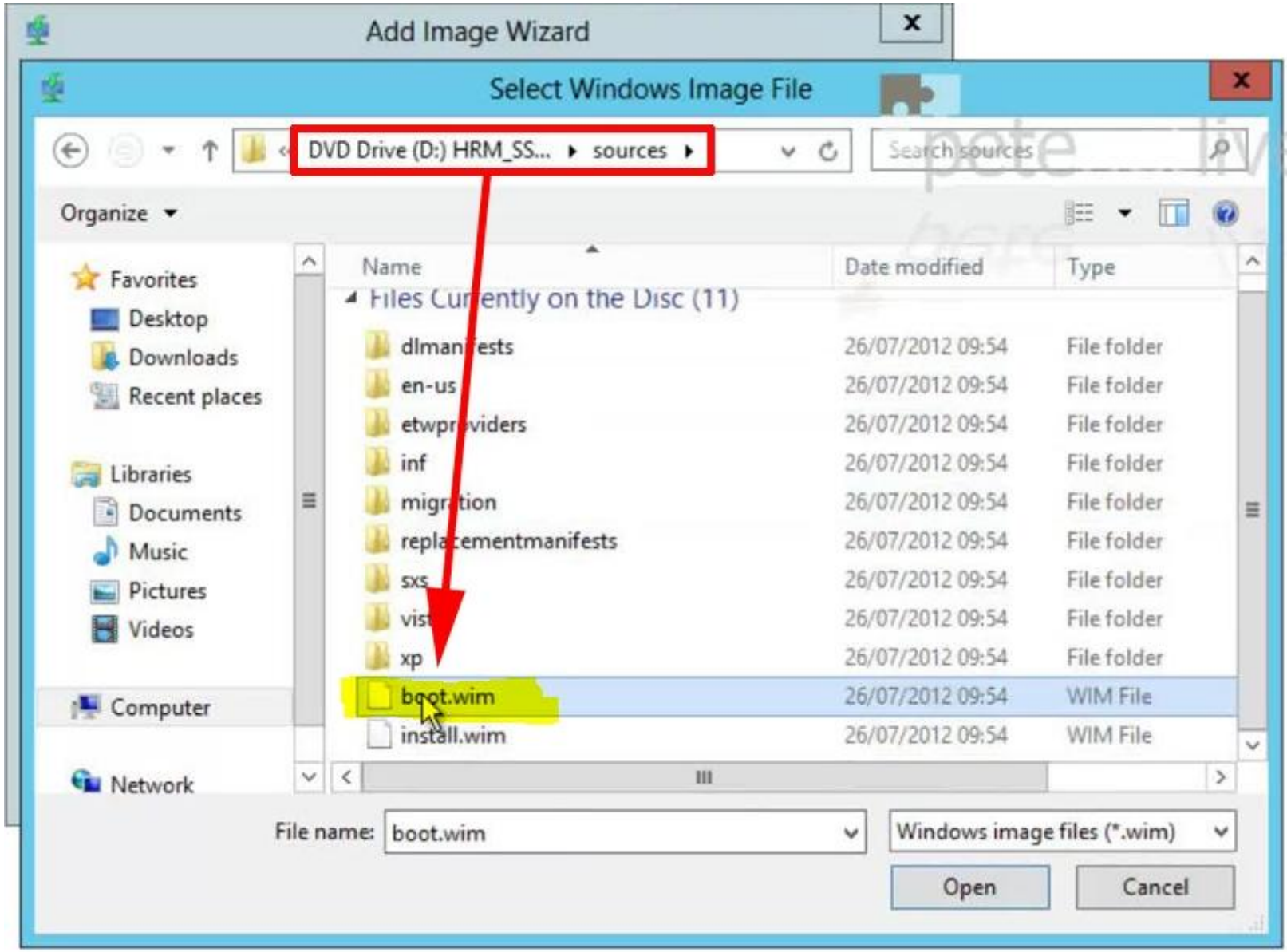
A. Install
B. Boot
C. Discovery
D. Capture

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
I need to add a boot image, so I can boot my remote clients form the WDS server and use this image to load WindowsPE on them, so they can be imaged. Right click Boot Images > Add Boot Image.



You can use either a Windows 8 DVD or a Windows Server 2012 DVD, you will need to navigate to the sources directory, and locate Boot.wim > Open.



http://www.petenetlive.com/KB/Article/0000735.htm
http://technet.microsoft.com/en-us/library/hh831764.aspx

http://technet.microsoft.com/en-us/library/dd637996(v=ws.10).aspx

QUESTION 108
You have a server named Server1 that runs Windows Server 2012. You create a Data Collector Set (DCS) named DCS1.

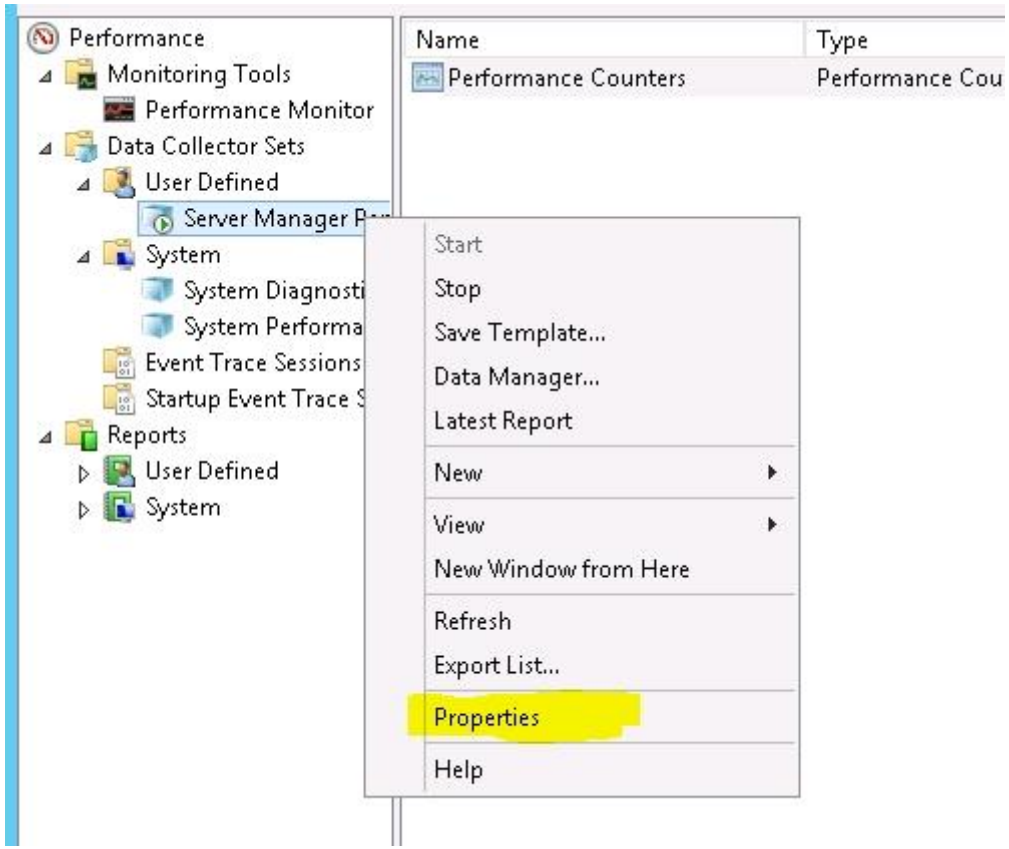
You need to configure DCS1 to log data to D:\logs.

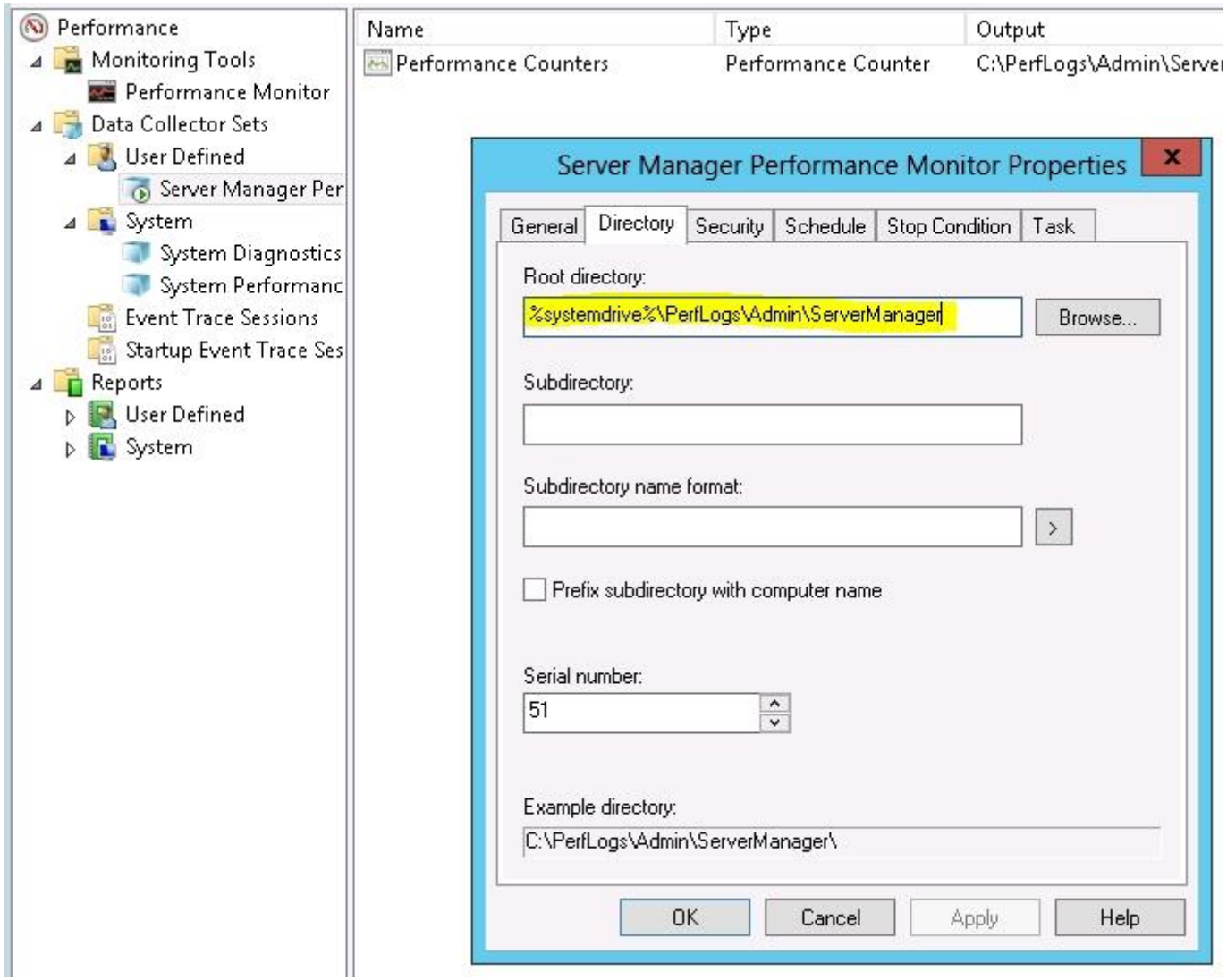
What should you do?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:


Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
Server Manager P
System
System Diagnosti
System Performa
Event Trace Sessions
Startup Event Trace S
Reports
User Defined
System
Name
Type
Performance Counters
Performance Cou
Start
Stop
Save Template...
Data Manager...
Latest Report
New
View
New Window from Here
Refresh
Export List...
Properties
Help



QUESTION 109

You have a server named WSUS1 that runs Windows Server 2012. 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 a command prompt, run wsusutil.exe and specify the movecontent parameter.
B. From the Update Services console, run the Windows Server Update Services Configuration Wizard.
C. From the Update Services console, configure the Update Files and Languages option.
D. From a command prompt, run wsusutil.exe and specify the export parameter.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.exe tool (with the **movecontent** command) to move the update files to the new disk. For this procedure, see Managing WSUS from the Command Line.

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

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/cc708480%28v=ws.10%29.aspx

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:

wsusutil movecontent *contentpath logfile* **-skipcopy** [**/?**]

The parameters are defined in the following table.

Parameter	Definition
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.

QUESTION 110

Your network contains an Active Directory domain named contoso.com. All client computers run Windows 8 Pro. You have a Group Policy object (GPO) named GP1.

GP1 is linked to the domain. GP1 contains the Windows Internet Explorer 10 and 11 Internet Settings.

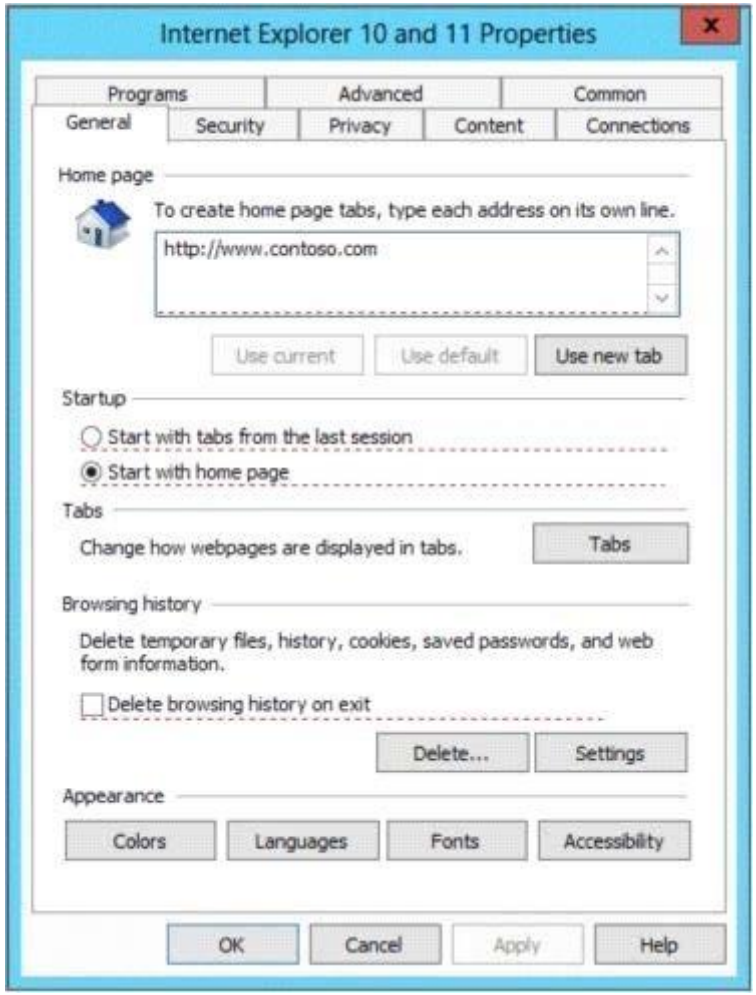
The settings are shown in the exhibit. (Click the Exhibit button.)

Users report that when they open Windows Internet Explorer, the home page is NOT set to http://www.contoso.com.

You need to ensure that the home page is set to http://www.contoso.com the next time users log on to the domain.

What should you do?

Exhibit:

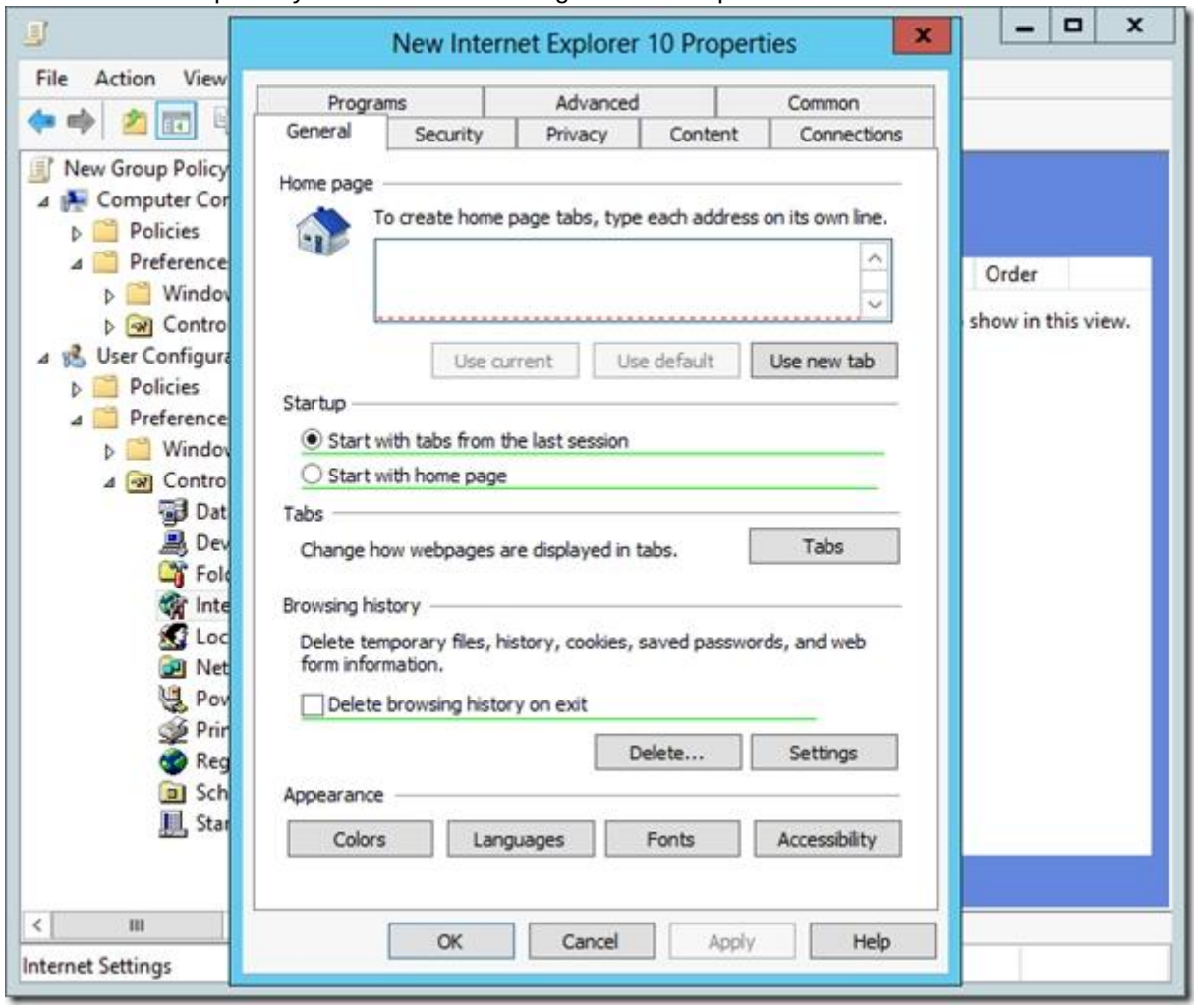


A. On each client computer, run gpupdate.exe.
B. Open the Internet Explorer 10 and 11 Internet Settings, and then press F5.
C. Open the Internet Explorer 10 and 11 Internet Settings, and then modify the Tabs settings.
D. On each client computer, run Invoke-GPupdate.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
You can use Group Policy Preferences to manage Internet Explorer 10.



Enabling and disabling settings with F5 – F8

As you can see, the tabs are exactly the same as in Internet Explorer, but with added green and dotted red lines underneath individual settings or red and green

circles in front of individual settings:

Settings with green lines underneath them or green circles in front of them get applied.
Settings with red lines underneath them or red circles in front of them do not get applied.

You can change theses statuses with the F5, F6, F7 and F8 buttons. **With F5 you can enable all settings on a tab**, while F6 only enables the specific setting you edited last. F8 disables all settings on a tab, while F7 only disables the specific setting you edited last. Press OK when done configuring settings.

http://4sysops.com/archives/internet-explorer-10-administration-part-3-group-policy-preferences/

QUESTION 111
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012. Server1 has the DHCP Server server role installed.

The network contains 400 client computers that run Windows 8. All of the client computers are joined to the domain and are configured DHCP clients.

You install a new server named Server2 that runs Windows Server 2012.

On Server2, you install the Network Policy Server role service and you configure Network Access Protection (NAP) to use the DHCP enforcement method.

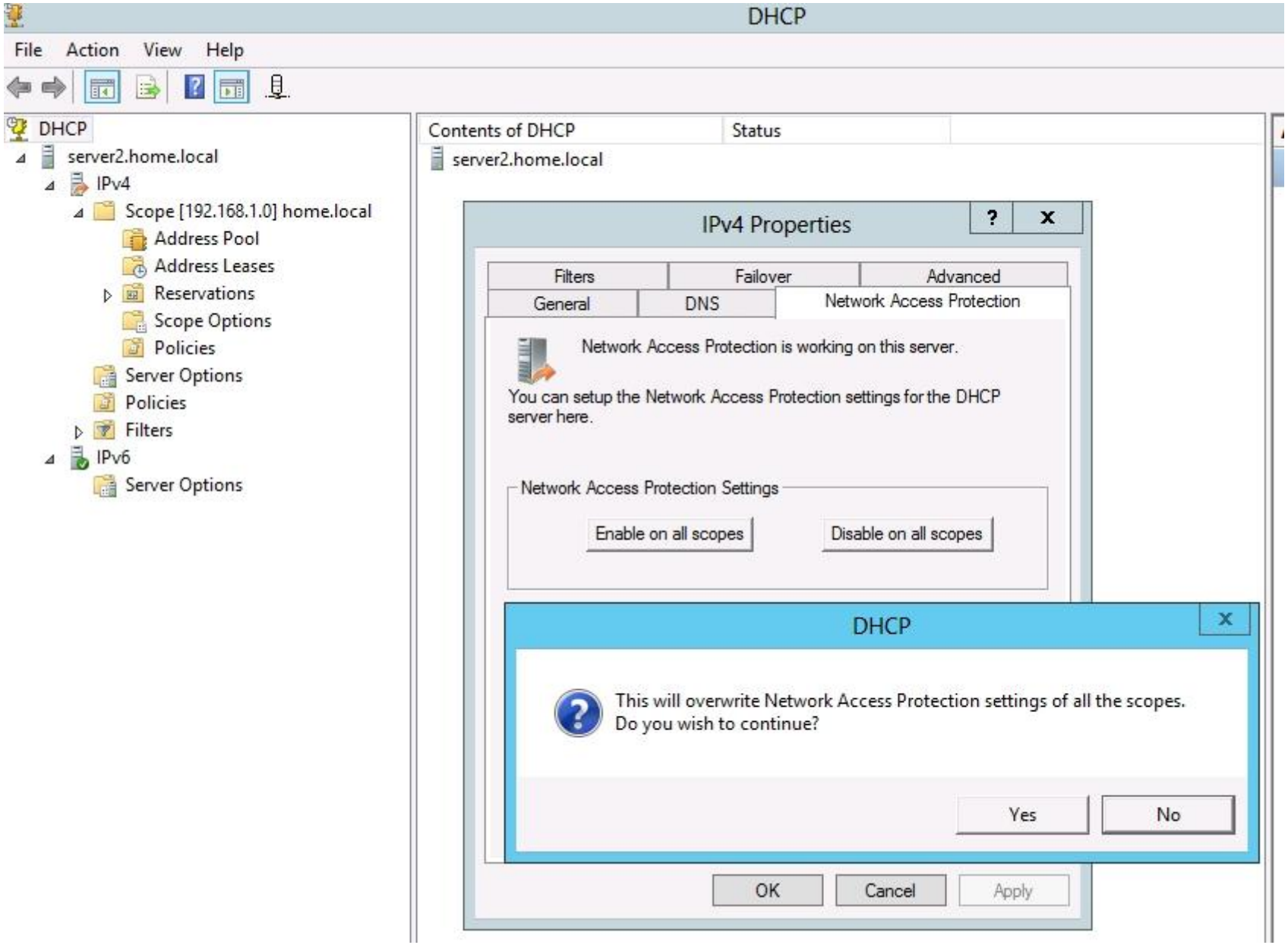
You need to ensure that Server1 only provides a valid default gateway to computers that pass the system health validation.

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

A. From the DHCP console, configure the 016 Swap Server option.
B. From the DHCP console, create a new policy.
C. From the NAP Client Configuration console, enable the DHCP Quarantine Enforcement Client.
D. From the DHCP console, enable NAP on all scopes.
E. From Server Manager, install the Network Policy Server role service.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:


DHCP
File Action View Help
DHCP
server2.home.local
IPv4
Scope [192.168.1.0] home.local
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
IPv6
Server Options
Contents of DHCP
Status
server2.home.local
IPv4 Properties
Filters
Failover
Advanced
General
DNS
Network Access Protection
Network Access Protection is working on this server.
You can setup the Network Access Protection settings for the DHCP server here.
Network Access Protection Settings
Enable on all scopes
Disable on all scopes
DHCP
This will overwrite Network Access Protection settings of all the scopes.
Do you wish to continue?
Yes
No
OK
Cancel
Apply

The administrator must define the following settings on the NAP DHCP server:
/ (D) NAP-enabled scopes: In order to use a DHCP scope with NAP, you must enable it specifically for NAP in scope properties under NAP settings.
/ Default NAP class: You must configure any required scope options for computers that are noncompliant with health requirements. A default gateway is not provided to noncompliant computers regardless of whether the 003 Router option is configured here. / Remote RADIUS server groups: If connection requests are forwarded from the DHCP server to a NAP health policy server on another computer, you must configure the NPS service on the NAP DHCP server to forward connection requests to the NAP health policy server. This setting is not required if the NAP DHCP server is also the NAP health policy server.
/ Default user class: You must configure any required scope options for computers that are compliant with health requirements.
The NAP DHCP server is a server running Windows Server 2008 or Windows Server 2008 R2 (or Windows 2012) with the DHCP server role installed and running. Additionally, if this server is not also the NAP health policy server, it must have the NPS role service installed (E), running, and configured to forward connection requests to the NAP health policy server. The NAP DHCP server restricts noncompliant client access by providing a limited IP address configuration to computers that do not meet health requirements. A limited access configuration has a subnet mask of 255.255.255.255 and no default gateway. Static host routes are provisioned to provide access to the DHCP server and any servers that have been added to remediation server groups on the NAP health policy server.

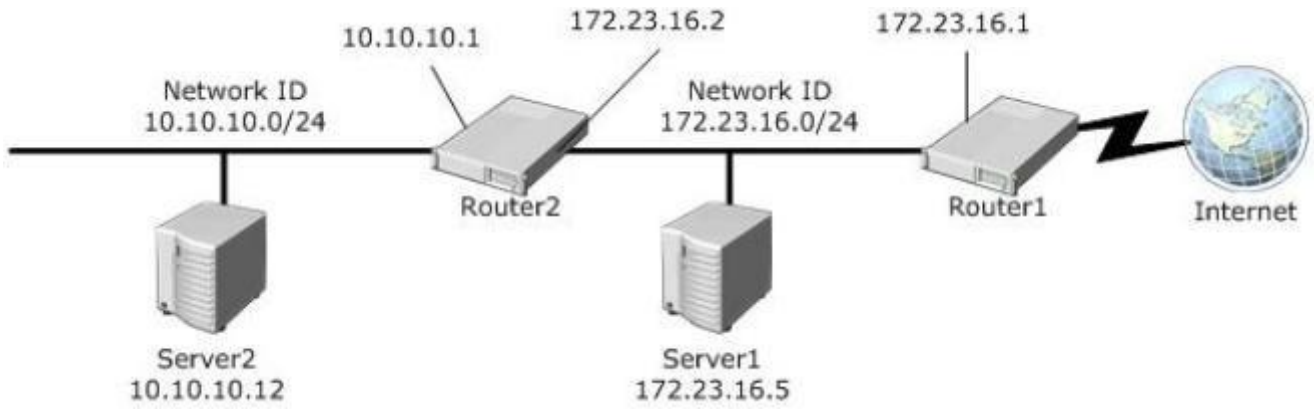
Network Policy and Access Services provides the following network connectivity solutions:

Solution	Description
Network Access Protection (NAP)	NAP is a client health policy creation, enforcement, and remediation technology. With NAP, system administrators can establish and automatically enforce health policies, which can include software requirements, security update requirements, and other settings. Client computers that are not in compliance with health policy can be provided restricted network access until their configuration is updated and brought into compliance with policy.
802.1X authenticated wired and wireless access	When you deploy 802.1X-capable wireless access points and Ethernet switches, you can use Network Policy Server (NPS) to deploy certificate-based authentication methods that are more secure than password-based authentication. Deploying 802.1X-capable hardware with NPS allows you to ensure that intranet users are authenticated before they can connect to the network or obtain an IP address from a DHCP server.
Central network policy management with RADIUS server and proxy	Rather than configuring network access policy at each network access server, you can create policies in a single location that specify all aspects of network connection requests, including who is allowed to connect, when they can connect, and the level of security they must use to connect to your network.

On the next screen, "Specify DHCP Scopes", we need only add scopes if we want this policy to apply to a specific set of scopes. If we do not specify any scopes it will apply to all NAP enabled scopes. Either add the name of all specific scopes to which this policy will apply or just click "*Next*" with the scopes empty to have it apply to all.

http://technet.microsoft.com/en-us/library/dd125379%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/network/bb545879.aspx
http://blogs.technet.com/b/teamdhcp/archive/2008/05/28/configuring-custom-nps-policies-per-dhcp-scope.aspx
http://blog.ittoby.com/2013/06/windows-2012-nap-nps-with-dhcp.html

QUESTION 112
Your network is configured as shown in the exhibit. (Click the Exhibit button.)



Server1 regularly accesses Server2.

You discover that all of the connections from Server1 to Server2 are routed through Router1.

You need to optimize the connection path from Server1 to Server2.

Which route command should you run on Server1?

A. Route add -p 10.10.10.0 MASK 255.255.255.0 10.10.10.1 METRIC 50
B. Route add -p 10.10.10.0 MASK 255.255.255.0 172.23.16.2 METRIC 100
C. Route add -p 10.10.10.12 MASK 255.255.255.0 10.10.10.1 METRIC 100
D. Route add -p 10.10.10.12 MASK 255.255.255.0 10.10.10.0 METRIC 50

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Static IP route entry	Definition
destination	Specifies either an IP address or host name for the network or host.
subnetmask	Specifies a subnet mask to be associated with this route entry. If *subnetmask* is not specified, 255.255.255.255 is used.
gateway	Specifies either an IP address or host name for the gateway or router to use when forwarding.
costmetric	Assigns an integer cost metric (ranging from 1 through 9,999) to be used in calculating the fastest, most reliable, and/or least expensive routes. If *costmetric* is not specified, 1 is used.
interface	Specifies the interface to be used for the route that uses the interface number. If an interface is not specified, the interface to be used for the route is determined from the gateway IP address.

http://support.microsoft.com/kb/299540/en-us
http://technet.microsoft.com/en-us/library/cc757323%28v=ws.10%29.aspx

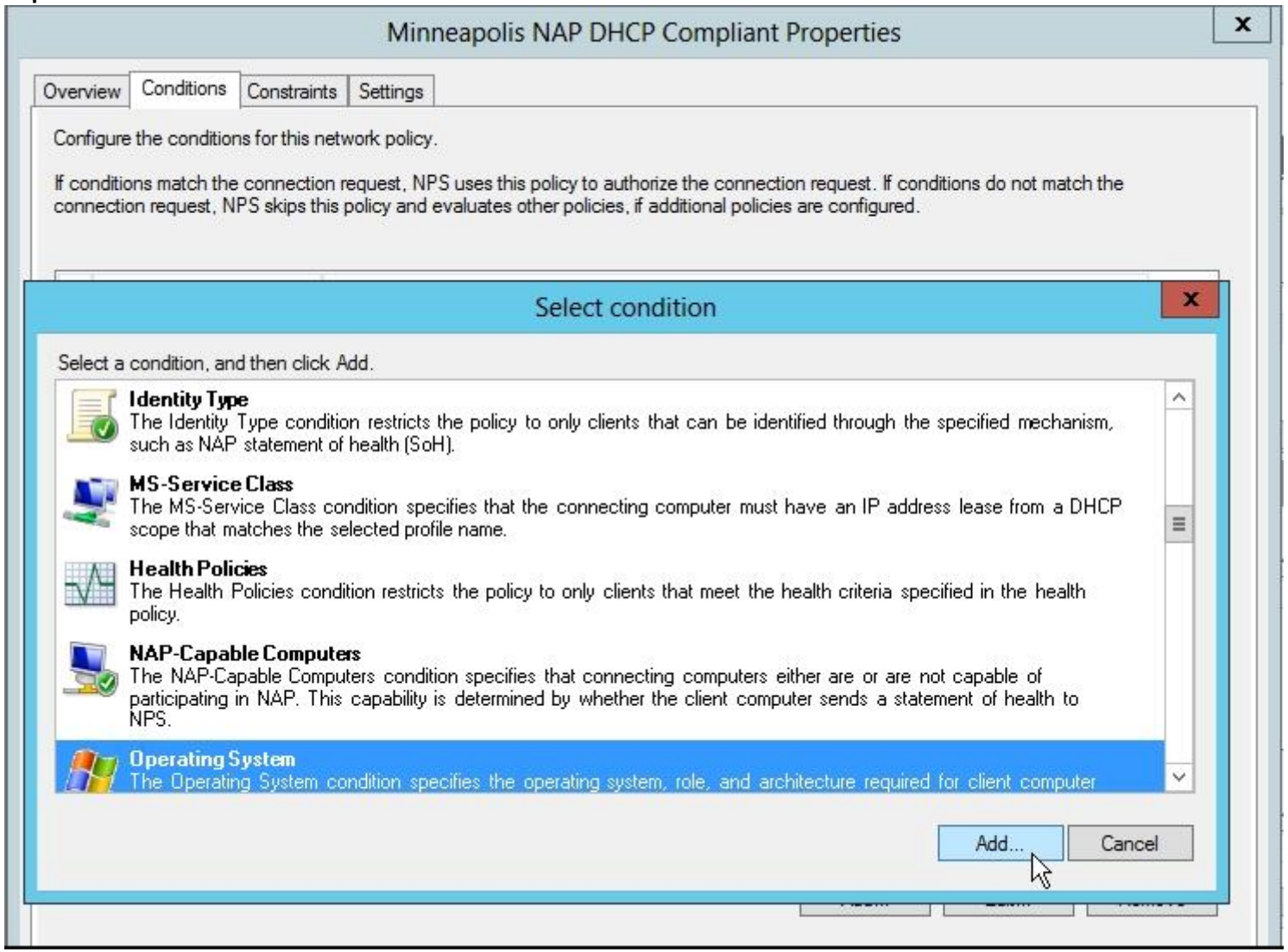
QUESTION 113
Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1 that runs Windows Server 2012. Server1 is configured as a Network Policy Server (NPS) server and as a DHCP server.
You need to ensure that only computers that send a statement of health are checked for Network Access Protection (NAP) health requirements.

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

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:



If you want to configure the Health Policies condition, click Health Policies, and then click Add. In Health Policies, choose an existing health policy, and then click OK. If you have not yet configured health policies, click New, and then configure a new health policy.
The Health Policies condition restricts the policy to clients that meet the health criteria in the policy that you specify.

If you want to configure the NAP-capable Computers condition, click NAP-capable Computers, and then click Add. In Specify the computers required to match this policy, click either Only computers that are NAP-capable or Only computers that are not NAP-capable, and then click OK.
The NAP-capable Computers condition restricts the policy to either clients that are capable of participating in NAP or clients that are not capable of participating in NAP. This capability is determined by whether the client sends a statement of health (SoH) to NPS.

http://technet.microsoft.com/en-us/library/cc731560.aspx
http://blog.ittoby.com/2013/06/windows-2012-nap-nps-with-dhcp.html

QUESTION 114
Your network contains two Active Directory forests named adatum.com and contoso.com. The network contains three servers. The servers are configured as shown in the following table.

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

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

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

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
A:
A connection request policy profile is a set of properties that are applied to an incoming RADIUS message. A connection request policy profile consists of the following groups of properties:
/ Authentication
You can set the following authentication options that are used for RADIUS Access-Request messages:
// Authenticate requests on this server.
// Forward requests to another RADIUS server in a remote RADIUS server group. // Accept the connection attempt without performing authentication or authorization.
/ Accounting
/ Attribute manipulation
/ Advanced

B:
A connection request policy is a named rule that consists of the following elements:
/ Conditions
/ Profile

* The User-Name RADIUS attribute is a character string that typically contains a user account location and a user account name. The user account location is also called the realm or realm name, and is synonymous with the concept of domain, including DNS domains, Active Directory domains, and Windows NT 4.0 domains

Note:
* NPS as a RADIUS proxy

The default connection request policy is deleted, and two new connection request policies are created to forward requests to two different domains. In this example, NPS is configured as a RADIUS proxy. NPS does not process any connection requests on the local server. Instead, it forwards connection requests to NPS or other RADIUS servers that are configured as members of remote RADIUS server groups.

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

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

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

QUESTION 115
You have installed Routing and Remote Access on Server1 what should you configure next to use it as a NAT server.

A. Add New Interface
B. Create Static Route
C. Configure the IPv4 DHCP Relay Agent
D. Configure the IPv6 DHCP Relay Agent

Correct Answer: A
Section: Configure a Network Policy infrastructure
Explanation

Explanation/Reference:
A. Network Address Translation allows you to share a connection to the public Internet through a single interface with a single public IP address.
The computers on the private network use private, non-routable addresses. NAT maps the private addresses to the public address.

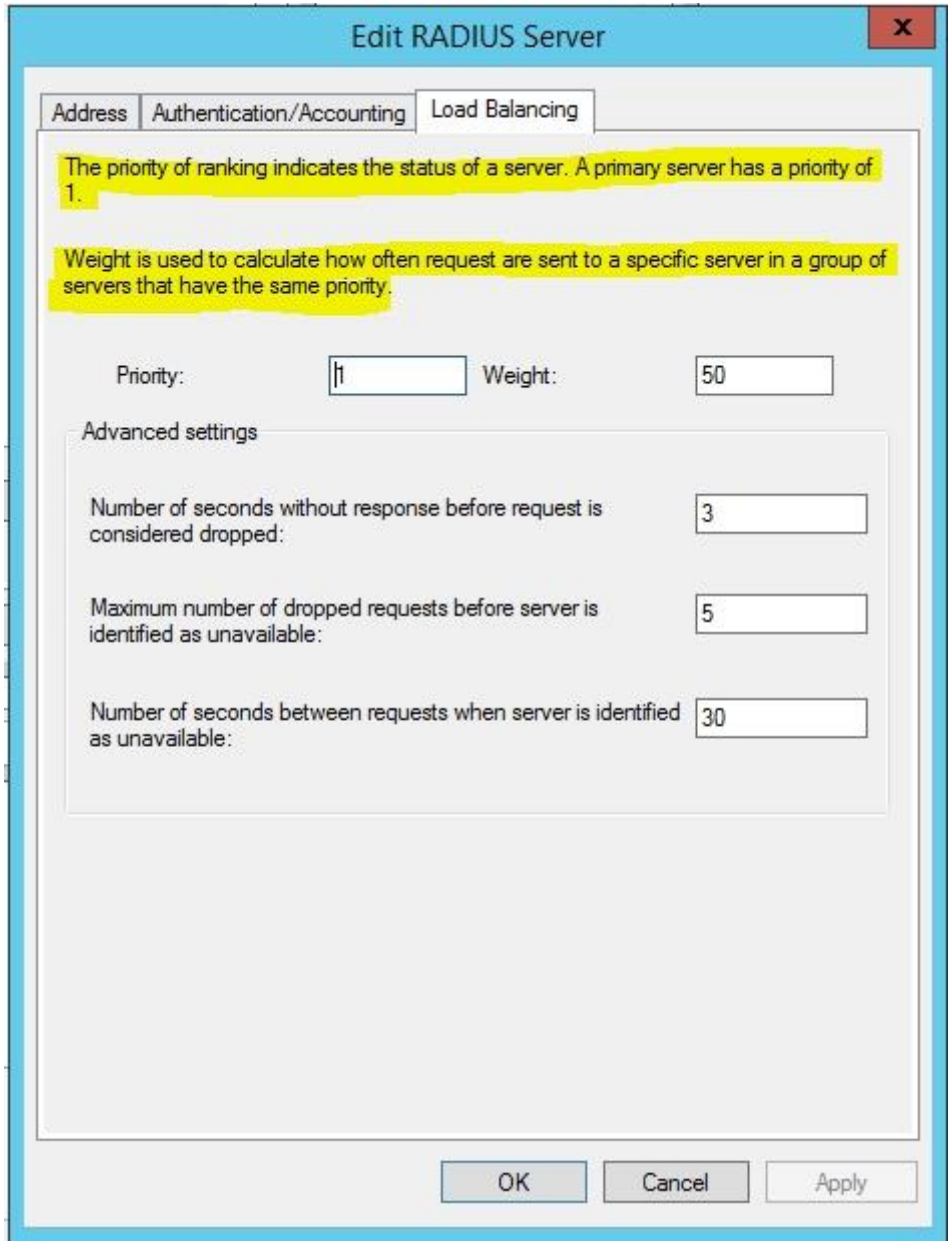
http://technet.microsoft.com/en-us/library/dd469812.aspx

QUESTION 116
Your network contains four Network Policy Server (NPS) servers named Server1, Server2, Server3, and Server4.
Server1 is configured as a RADIUS proxy that forwards connection request to a remote RADIUS server group named Group1.
You need to ensure that Server2 and Server3 receive connection requests. Server4 must only receive connection requests if both Server2 and Server3 are unavailable.
How should you configrure Group1?

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

Correct Answer: D
Section: Configure a Network Policy infrastructure
Explanation

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


Edit RADIUS Server
Address
Authentication/Accounting
Load Balancing
The priority of ranking indicates the status of a server. A primary server has a priority of 1.
Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority.
Priority:
1
Weight:
50
Advanced settings
Number of seconds without response before request is considered dropped:
3
Maximum number of dropped requests before server is identified as unavailable:
5
Number of seconds between requests when server is identified as unavailable:
30
OK
Cancel
Apply

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

Explanation:
During the NPS proxy configuration process, you can create remote RADIUS server groups and then add RADIUS servers to each group. To configure load balancing, you must have more than one RADIUS server per remote RADIUS server group. While adding group members, or after creating a RADIUS server as a group member, you can access the Add RADIUS server dialog box to configure the following items on the Load Balancing tab:

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

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

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

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

QUESTION 117
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012. 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 DC1, create a service location (SRV) record.
B. On Server2, configure the EnableDiscovery registry key.
C. On all of the client computers, configure the EnableDiscovery registry key.
D. In a GPO, modify the Request Policy setting for the NAP Client Configuration.
E. On Dc1, create an alias (CNAME) record.

Correct Answer: ACD
Section: Configure a Network Policy infrastructure
Explanation

Explanation/Reference:

Requirements for HRA automatic discovery

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

- Client computers must be running Windows Vista® with Service Pack 1 (SP1) or Windows XP with Service Pack 3 (SP3).
- The HRA server must be configured with a Secure Sockets Layer (SSL) certificate.
- The **EnableDiscovery** registry key must be configured on NAP client computers.
- DNS SRV records must be configured.
- The trusted server group configuration in either local policy or Group Policy must be cleared.

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

QUESTION 118
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012. Server1 has the Network Policy Server role service installed.
You plan to configure Server1 as a Network Access Protection (NAP) health policy server for VPN enforcement by using the Configure NAP wizard.
You need to ensure that you can configure the VPN enforcement method on Server1 successfully.

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

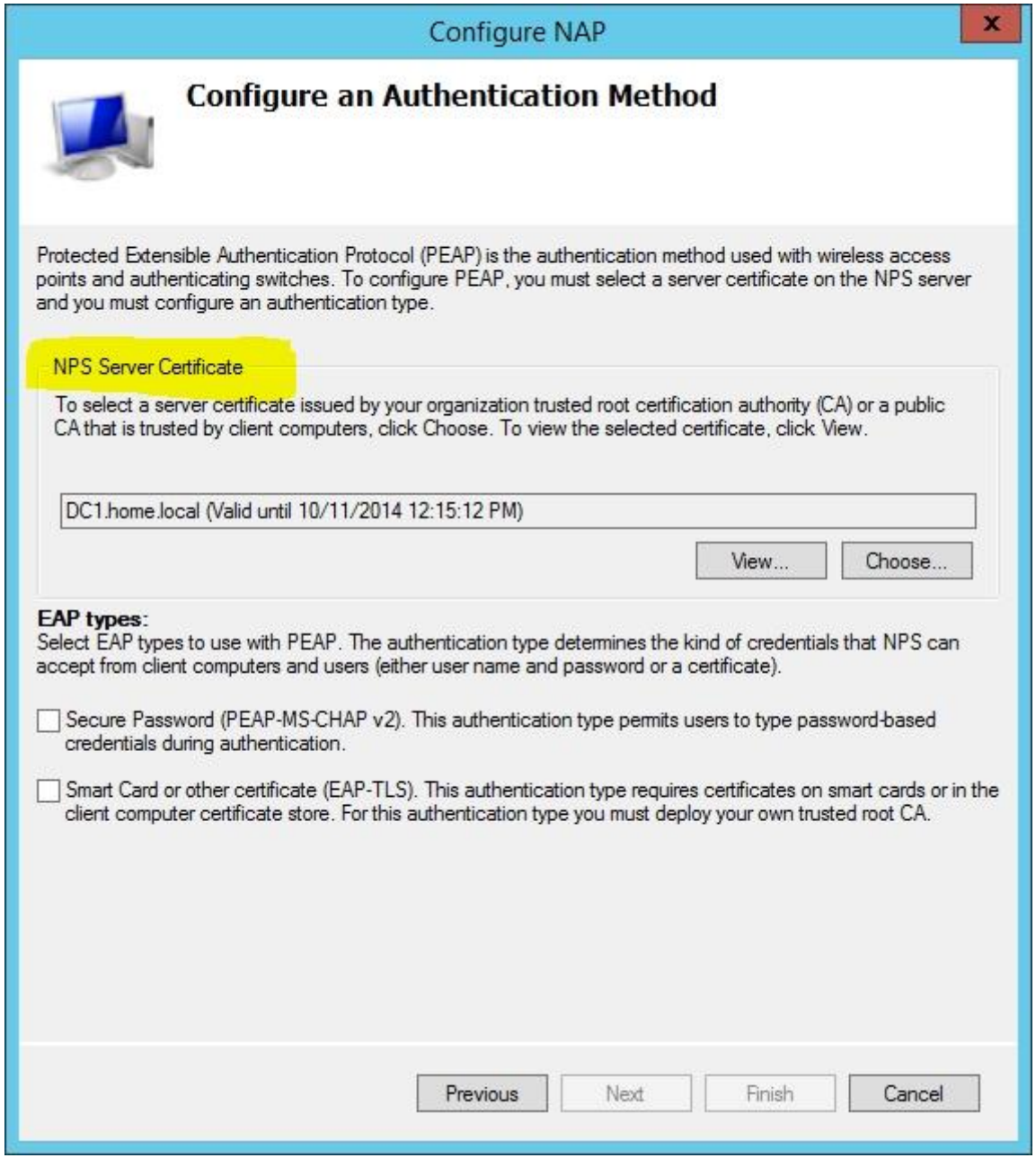
A. The Host Credential Authorization Protocol (HCAP)
B. A system health validator (SHV)
C. The Remote Access server role
D. A Computer certificate

Correct Answer: D
Section: Configure a Network Policy infrastructure
Explanation

Explanation/Reference:
http://technet.microsoft.com/en-us/library/dd125309%28v=ws.10%29.aspx
The NAP health policy server uses the NPS role service with configured network policies, 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 VPN server to provide full access to compliant NAP client computers, and to restrict access to noncompliant client computers when NAP is deployed using full enforcement mode.

VPN enforcement provides strong limited network access for all computers accessing the network through a VPN connection.
VPN enforcement is different from Network Access Quarantine Control, which is a feature in Windows Server 2003 and Internet Security and Acceleration (ISA) Server 2004.

For the most secure and effective NAP deployment on your network, deploy strong enforcement methods, such as the Internet Protocol security (IPsec), 802.1X, and virtual private network (VPN) enforcement methods. **Strong enforcement methods use certificate-based authentication methods and secure the channel between clients and servers** through which the statement of health (SoH) and statement of health response (SoHR) are sent.



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

NAP can be deployed in a variety of network environments, including networks with local wired or wireless access and remote access scenarios. **Network requirements vary, depending on the type of enforcement method you use**. However, all NAP enforcement methods require that the NAP client computer has TCP/IP network connectivity to the NAP enforcement point and that the enforcement point has connectivity to the NAP health policy server. SHAs can have their own network requirements. Consult your vendor documentation for any SHAs that you deploy to determine these requirements.

The 802.1X and VPN enforcement methods have the following AD DS requirements: The NAP health policy server requires connectivity to a domain controller to perform PEAP-based user or computer authentication of NAP client connection requests.
The 802.1X and VPN enforcement methods have the following AD DS requirements: The NAP health policy server requires a computer certificate to perform PEAP-based user or computer authentication. After this certificate is acquired, a connection to AD CS is not required for as long as the certificate is valid.

The NAP health policy server requires a computer certificate to perform PEAP-based user or computer authentication. After this certificate is acquired, a connection to AD CS is not required for as long as the certificate is valid.

http://technet.microsoft.com/en-us/library/dd125382%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc770422%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc731363%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc732681.aspx
http://technet.microsoft.com/en-us/library/dd125396(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/hh831416.aspx
http://technet.microsoft.com/en-us/library/dd125301(v=ws.10).aspx

QUESTION 119
You deploy two servers named Server1 and Server2. You install Network Policy Server (NPS) on both servers.
On Server1, you configure the following NPS settings:
· RADIUS Clients
· Network Policies
· Connection Request Policies
· SQL Server Logging Properties
You export the NPS configurations to a file and import the file to Server2.
You need to ensure that the NPS configurations on Server2 are the same as the NPS configurations on Server1.

Which settings should you manually configure on Server2?

A. SQL Server Logging Properties
B. Connection Request Policies
C. RADIUS Clients
D. Network Policies

Correct Answer: A
Section: Configure a Network Policy infrastructure

Explanation

Explanation/Reference:
If SQL Server logging is configured on the source NPS server, SQL Server logging settings are not exported to the XML file. After you import the file on another NPS server, you must manually configure SQL Server logging.

By default, NPS does not log any data until you configure it to do so. When you configure SQL Server logging, all required attributes, accounting, and authentication data that is normally logged in either IAS format or database-compatible format is logged to the SQL Server database.

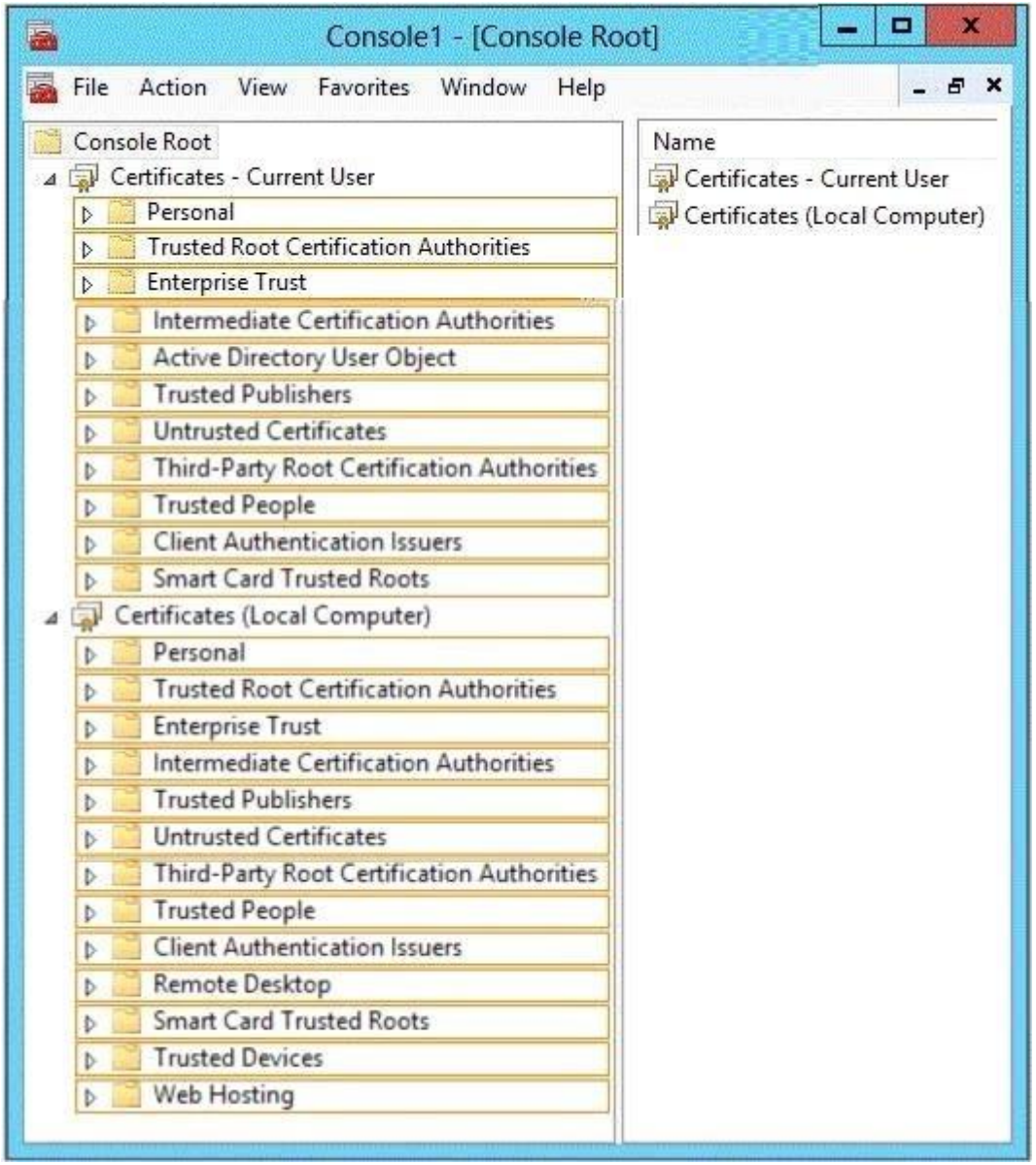
Initially, it is recommended that you enable the logging of accounting and user authentication requests. You can refine your logging settings after you determine your required data.

http://technet.microsoft.com/en-us/library/dd197595%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc754123.aspx
http://technet.microsoft.com/pt-pt/library/cc732059%28v=ws.10%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/bb960723%28v=vs.85%29.aspx

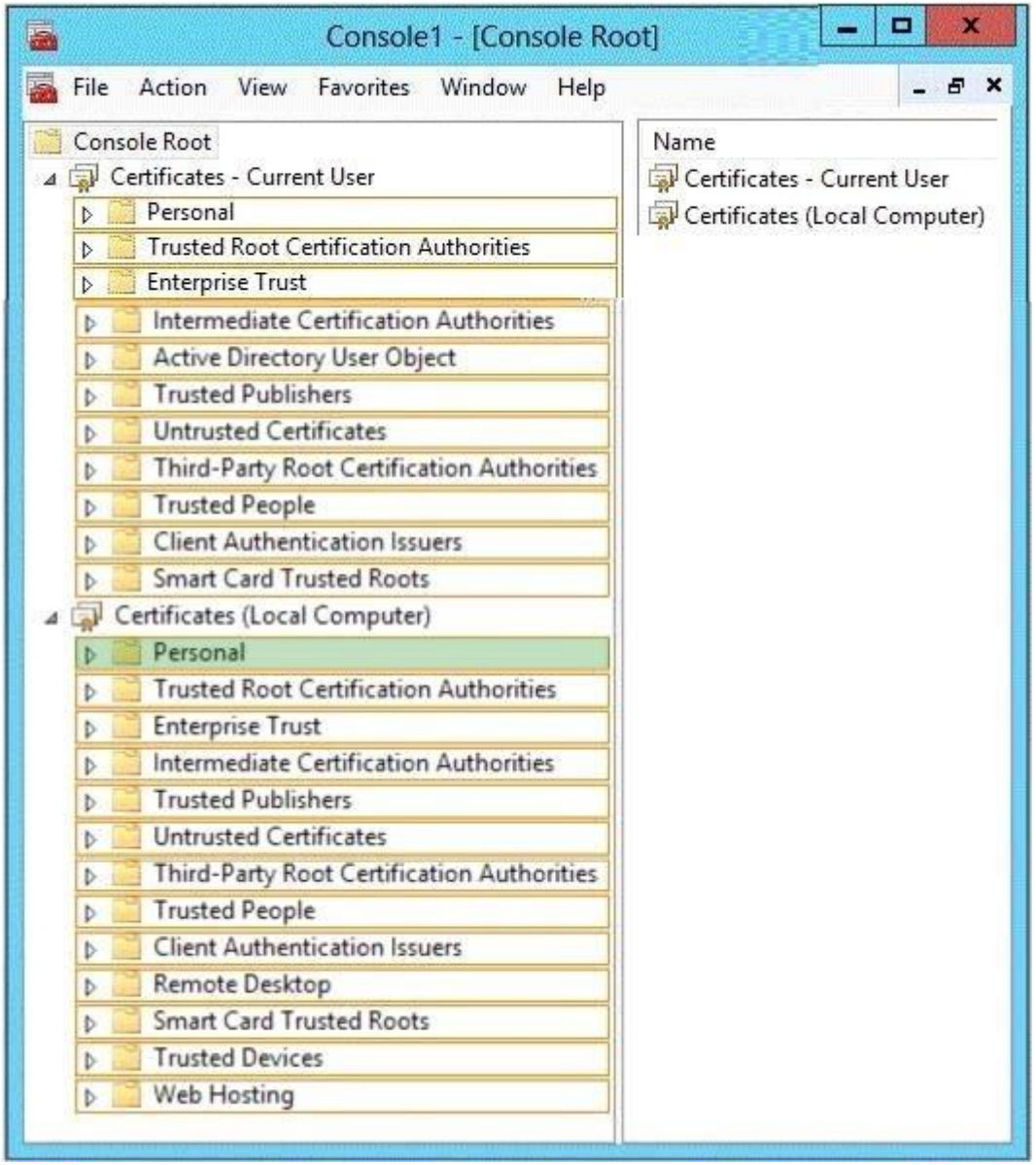
QUESTION 120
You have a server named Server1 that has the Network Policy and Access Services server role installed.
You plan to configure Network Policy Server (NPS) on Server1 to use certificate-based authentication for VPN connections. You obtain a certificate for NPS.
You need to ensure that NPS can perform certificate-based authentication.

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

Hot Area:



Correct Answer:



Section: Configure a Network Policy infrastructure

Explanation

Explanation/Reference:

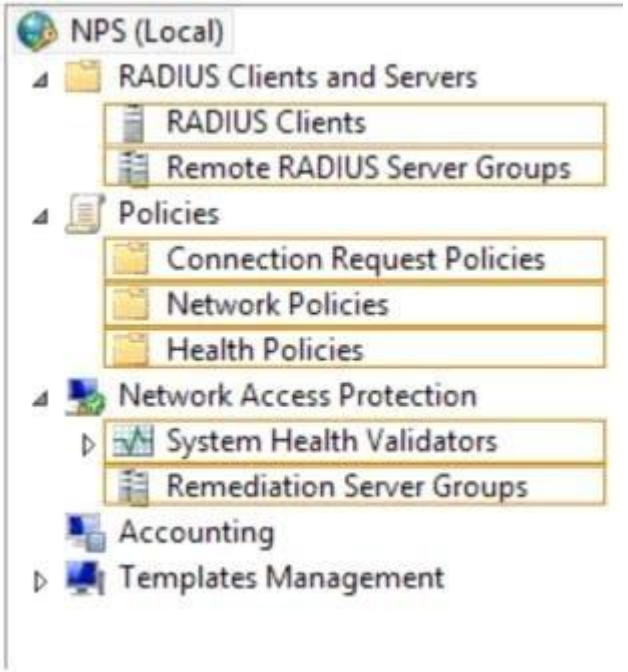
http://technet.microsoft.com/en-us/library/cc730811.aspx
http://technet.microsoft.com/en-us/library/cc772401%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/ee407543%28v=ws.10%29.aspx

QUESTION 121
Your network contains a RADIUS server named Server1. You install a new server named Server2 that runs Windows Server 2012 and has Network Policy Server (NPS) installed.
You need to ensure that all accounting requests for Server2 are forwarded to Server1.
On Server2, you create a new remote RADIUS server group named Group1 that contains Server1.

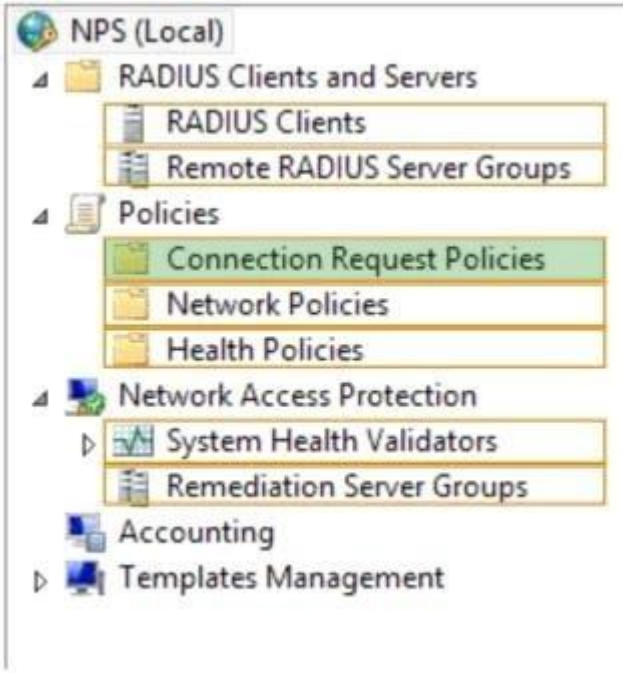
What should you configure next on Server2?

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

Hot Area:



Correct Answer:



Section: Configure a Network Policy infrastructure
Explanation

Explanation/Reference:

QUESTION 122
Your network contains an Active Directory domain named contoso.com. The domain contains a RADIUS server named Server1 that runs Windows Server 2012.
You add a VPN server named Server2 to the network.
On Server1, you create several network policies.
You need to configure Server1 to accept authentication requests from Server2.

Which tool should you use on Server1?

A. Connection Manager Administration Kit (CMAK).

B. Routing and Remote Access
C. Network Policy Server (NPS)
D. Set-RemoteAccessRadius

Correct Answer: C
Section: Configure a Network Policy infrastructure
Explanation

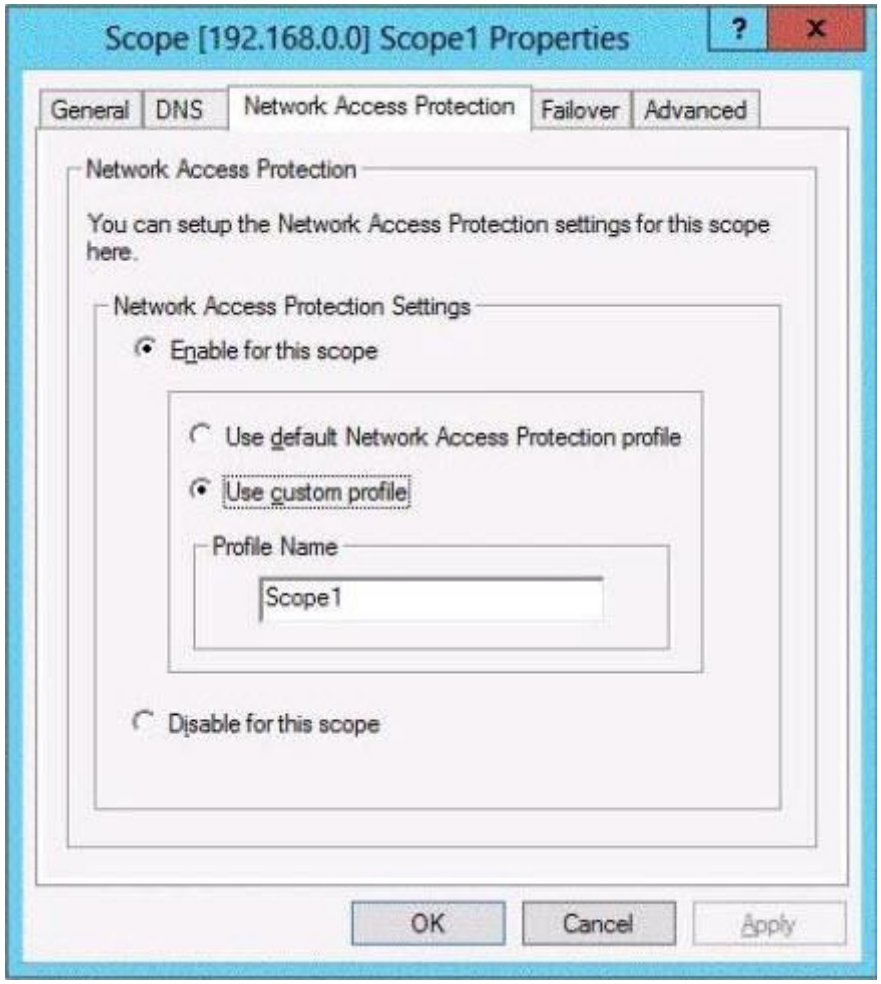
Explanation/Reference:
Forward requests to the following remote RADIUS server group . By using this setting, NPS forwards connection requests to the remote RADIUS server group that you specify.
If the NPS server receives a valid Access-Accept message that corresponds to the Access- Request message, the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

http://technet.microsoft.com/en-us/library/cc753603.aspx
http://www.youtube.com/watch?v=0_1GOBTL4FE

QUESTION 123
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1.
Server1 has the DHCP Server server role and the Network Policy Server role service installed.
Server1 contains three non-overlapping scopes named Scope1, Scope2, and Scope3.
Server1 currently provides the same Network Access Protection (NAP) settings to the three scopes.
You modify the settings of Scope1 as shown in the exhibit. (Click the Exhibit button.)
You need to configure Server1 to provide unique NAP enforcement settings to the NAP non- compliant DHCP clients from Scope1.

What should you create?

Exhibit:



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

Correct Answer: A
Section: Configure a Network Policy infrastructure

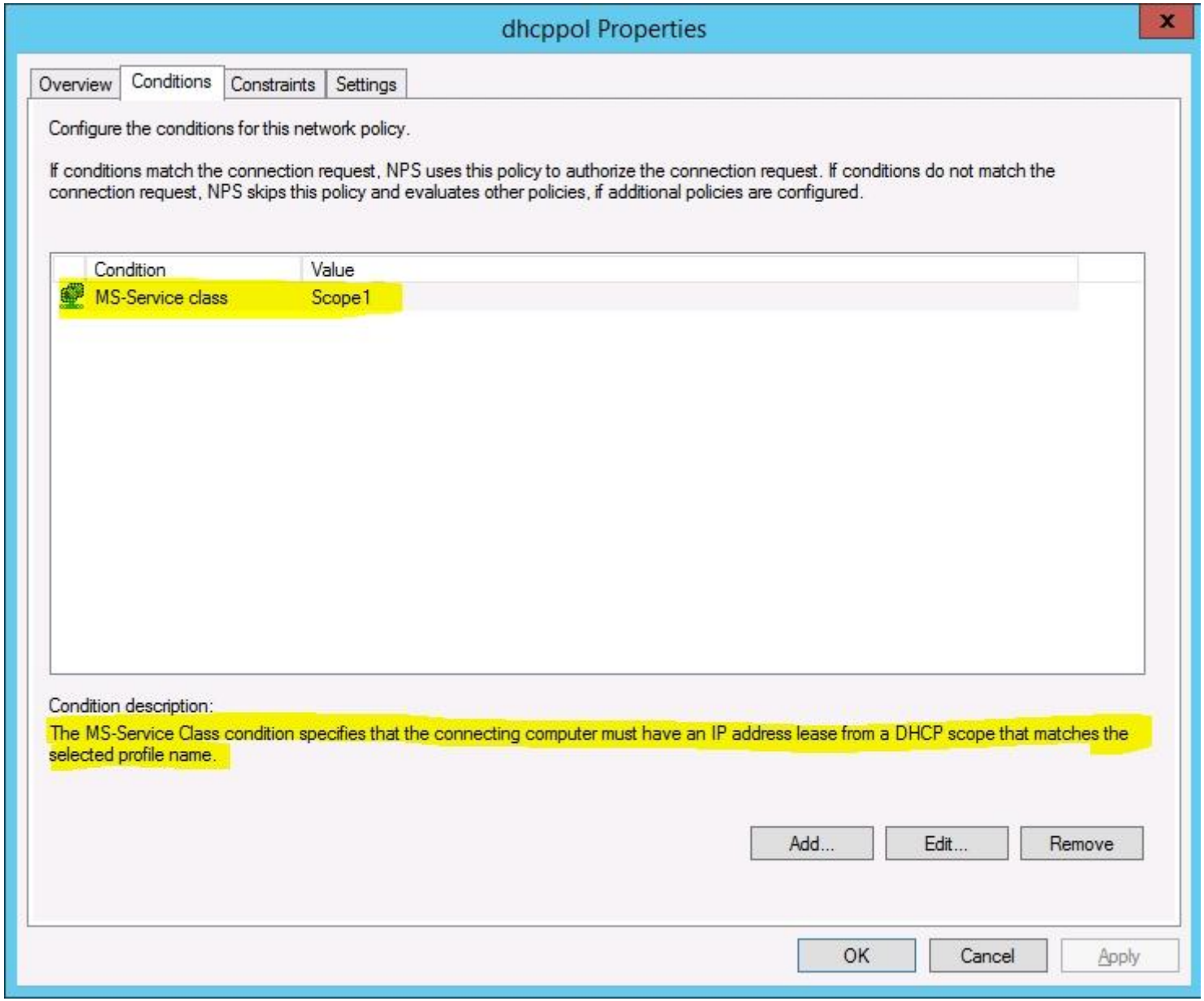
Explanation

Explanation/Reference:
http://technet.microsoft.com/en-us/library/cc731560(v=ws.10).aspx

Open the NPS console, double-click **Policies**, click **Network Policies**, and then double-click the policy you want to configure.
In policy **Properties**, click the **Conditions tab**, and then click **Add**. In **Select condition**, scroll to the **Network Access Protection group of conditions.**
If **you want to configure the Identity Type condition, click Identity Type, and then click Add.** In Specify the method in which clients are identified in this policy, select the items appropriate for your deployment, and then click OK.

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

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



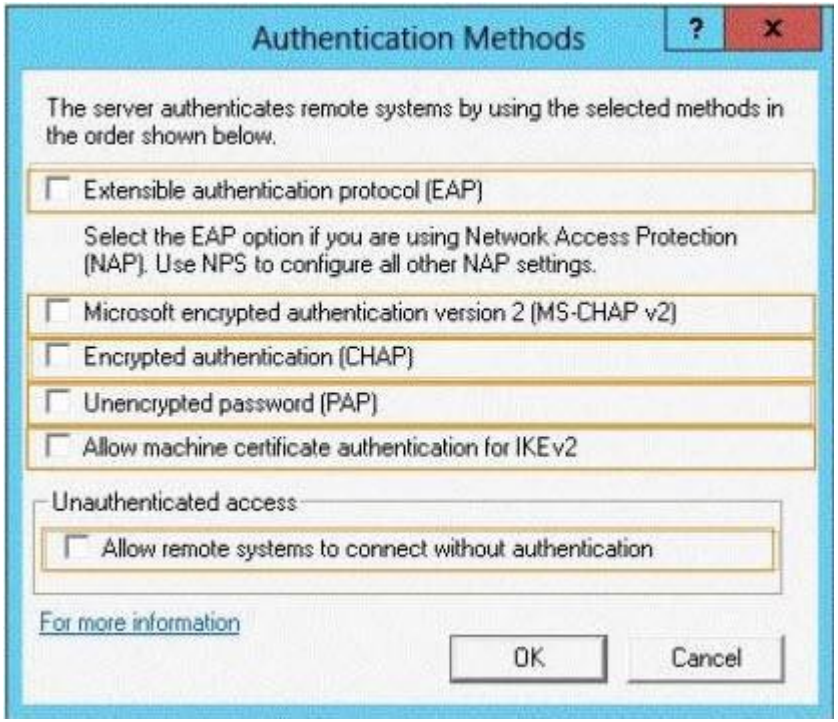
The MS-Service Class condition restricts the policy to clients that have received an IP address from a DHCP scope that matches the specified DHCP profile name.

This condition is used only when you are deploying NAP with the DHCP enforcement method.
http://technet.microsoft.com/en-us/library/cc731220(v=ws.10).aspx

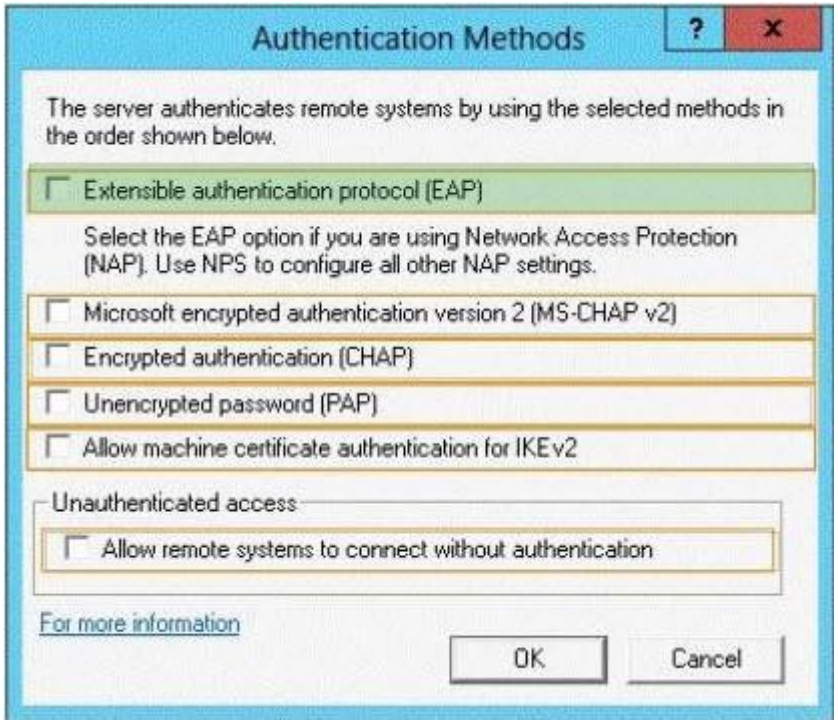
QUESTION 124
You have a server named Server1 that runs Windows Server 2012. Server1 has the Remote Access server role installed.
You have a client named Client1 that is configured as an 802.1X supplicant. You need to configure Server1 to handle authentication requests from Client1.
The solution must minimize the number of authentication methods enabled on Server1.

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

Hot Area:



Correct Answer:

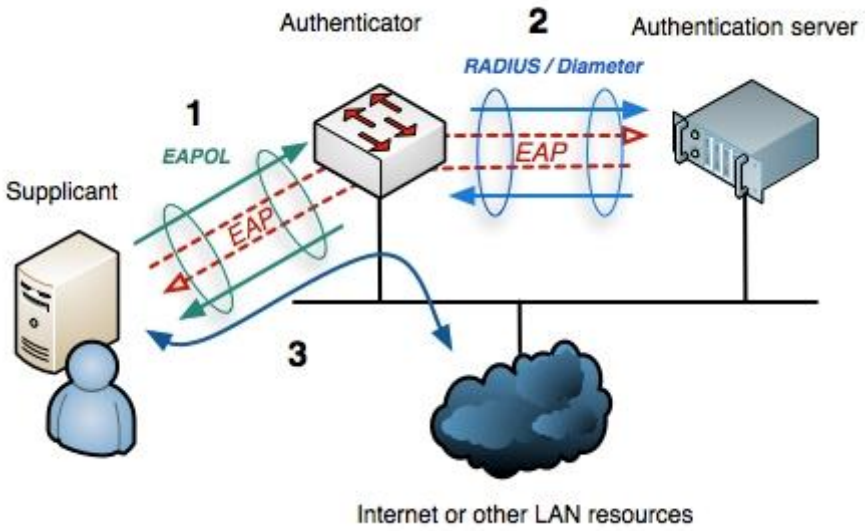


Section: Configure a Network Policy infrastructure
Explanation

Explanation/Reference:
IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized.



EAP data is first encapsulated in EAPOL frames between the Supplicant and Authenticator, then re-encapsulated between the Authenticator and the Authentication server using RADIUS or Diameter.

http://en.wikipedia.org/wiki/IEEE_802.1X

QUESTION 125
DRAG DROP

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

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

Which three actions should you perform in sequence?

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

Select and Place:

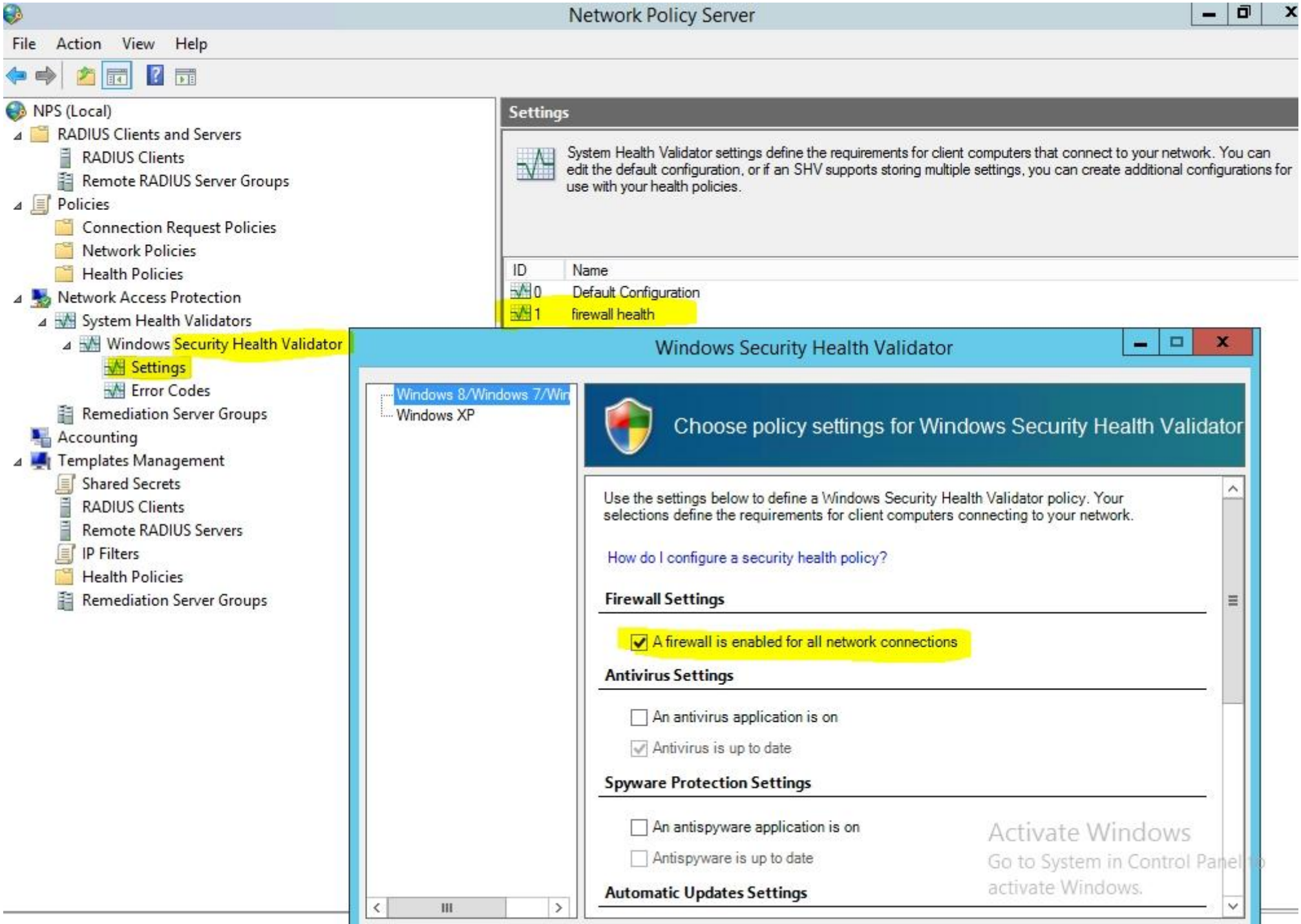
Actions	Answer Area
Create a connection request policy.	
Create a network policy.	
Create a remediation server group.	
Create a Windows Security Health Validator (WSHV) configuration.	
Create a health policy.	

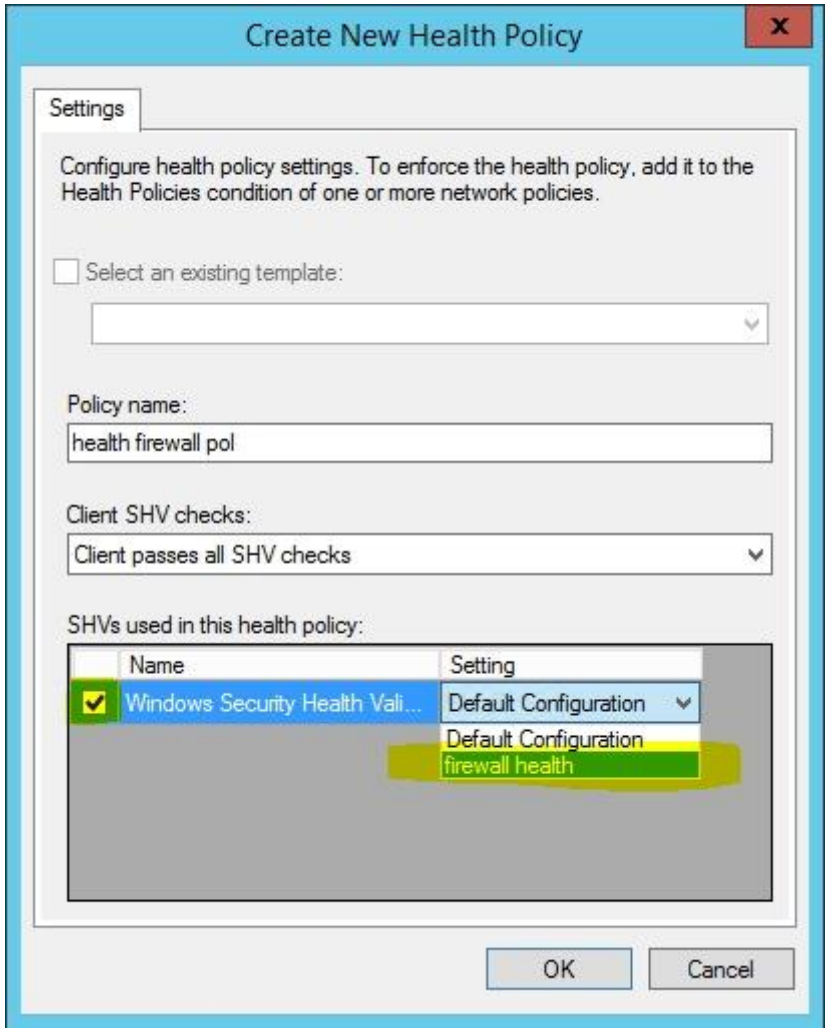
Correct Answer:

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

Section: Configure a Network Policy infrastructure
Explanation

Explanation/Reference:


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
System Health Validators
Windows Security Health Validator
Settings
Error Codes
Remediation Server Groups
Accounting
Templates Management
Shared Secrets
RADIUS Clients
Remote RADIUS Servers
IP Filters
Health Policies
Remediation Server Groups
Settings
System Health Validator settings define the requirements for client computers that connect to your network. You can edit the default configuration, or if an SHV supports storing multiple settings, you can create additional configurations for use with your health policies.
ID
Name
0
Default Configuration
1
firewall health
Windows Security Health Validator
Windows 8/Windows 7/Win
Windows XP
Choose policy settings for Windows Security Health Validator
Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.
How do I configure a security health policy?
Firewall Settings
A firewall is enabled for all network connections
Antivirus Settings
An antivirus application is on
Antivirus is up to date
Spyware Protection Settings
An antispyware application is on
Antispyware is up to date
Automatic Updates Settings
Activate Windows
Go to System in Control Panel to activate Windows.


Create New Health Policy
Settings
Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.
Select an existing template:
Policy name:
health firewall pol
Client SHV checks:
Client passes all SHV checks
SHVs used in this health policy:
Name
Setting
Windows Security Health Vali...
Default Configuration
Default Configuration
firewall health
OK
Cancel

Network Policy Server

File Action View Help

- NPS (Local)
  - RADIUS Clients and Servers
  - Policies
    - Connection Request Po
    - Network Policies
    - Health Policies
  - Network Access Protection
    - System Health Validato
      - Windows Security H
        - Settings
        - Error Codes
    - Remediation Server Gro
  - Accounting
  - Templates Management

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
firewall net pol	Enabled	1	Grant Acce...	DHCP Server

firewall net pol

Conditions - If the following conditions are met:

Condition	Value
Health Policy	health firewall pol

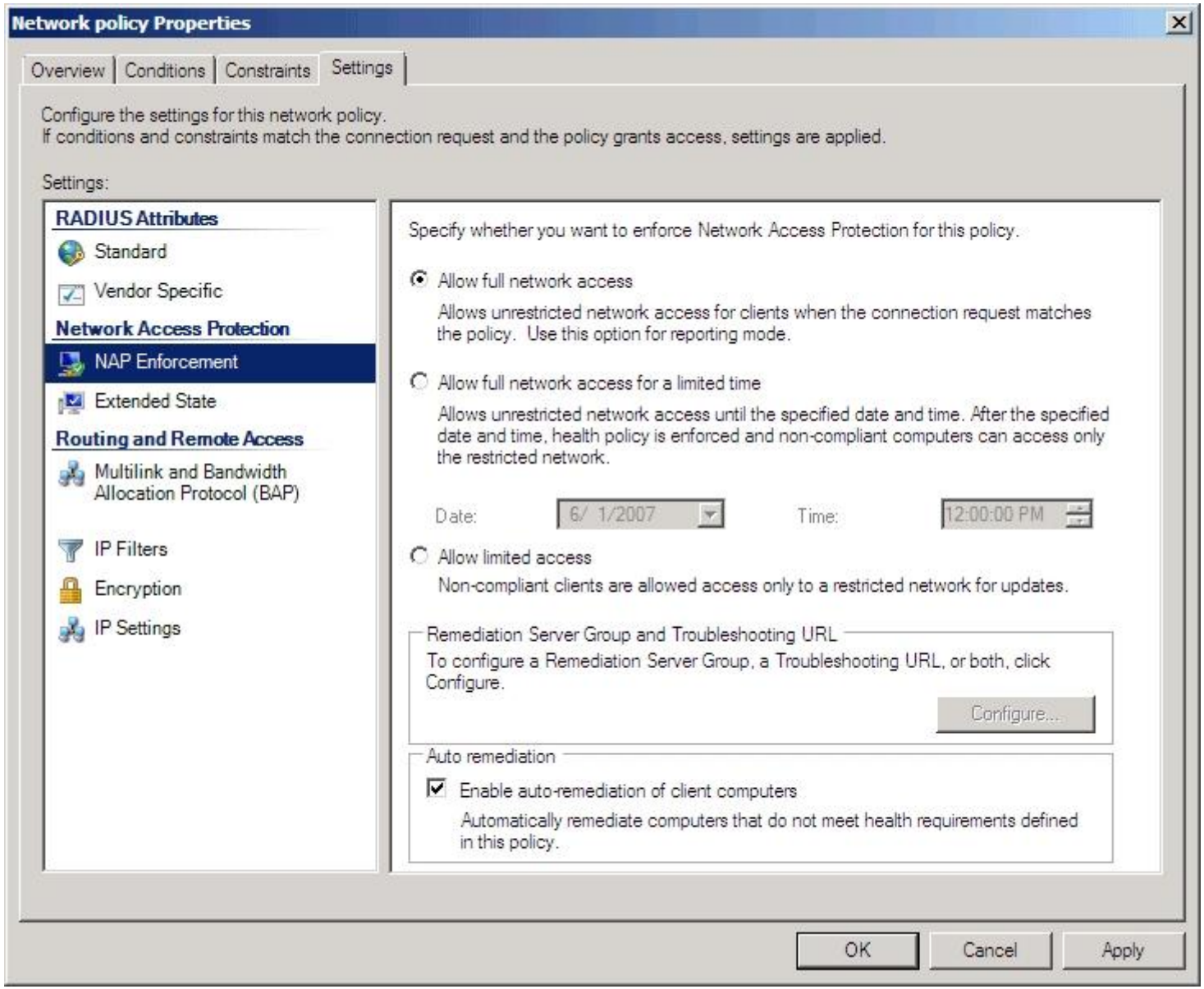
Settings - Then the following settings are applied:

Setting	Value
Authentication Method	Perform Machine Health Check Only
Access Permission	Grant Access
Update Noncompliant Clients	False
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed
Extended State	<Blank>
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

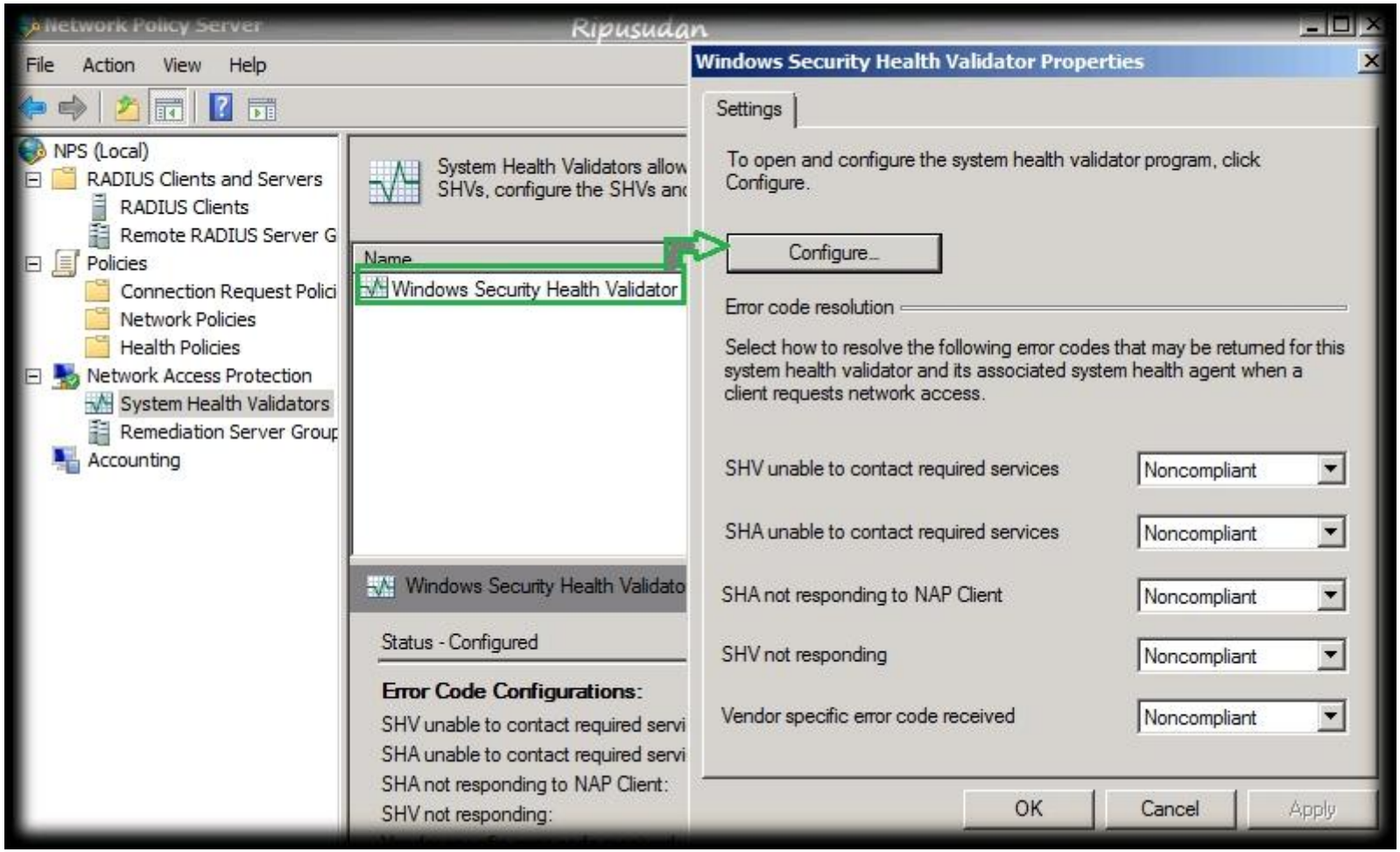
Activate Windows
Go to System in Control Pane
activate Windows.

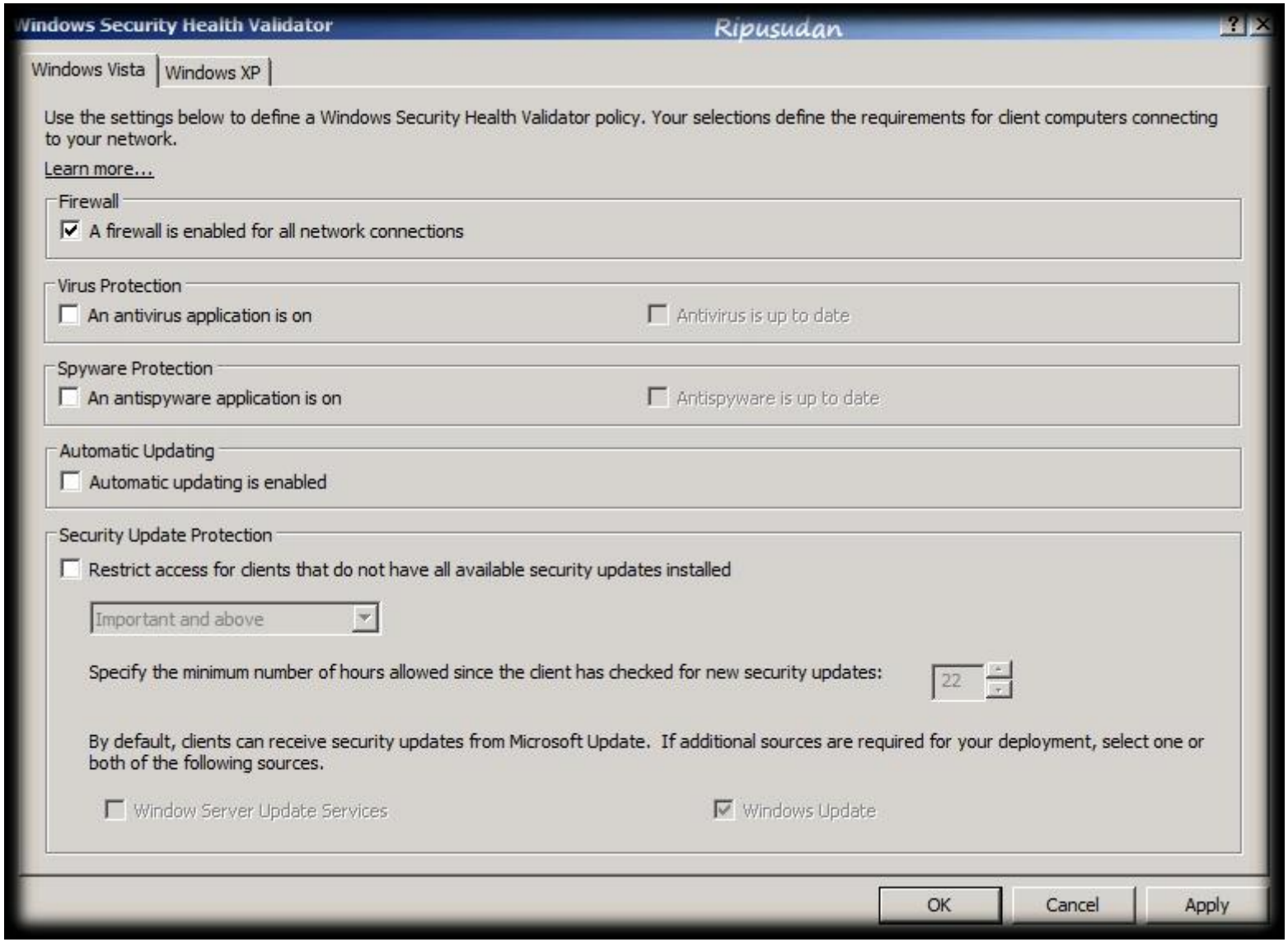
you don´t need create a Remediation server because you only need enabling NAP in reporting mode only

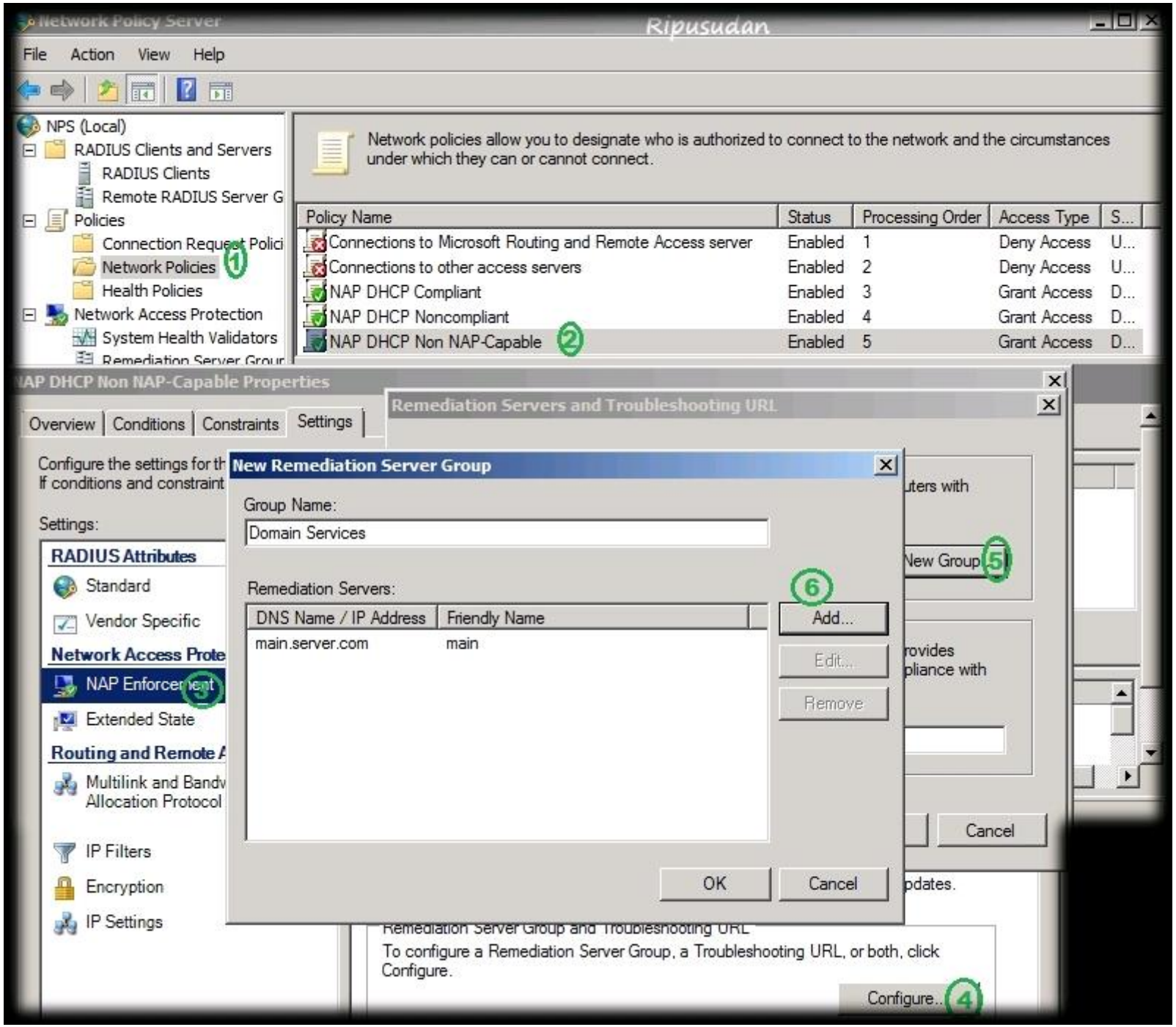
http://technet.microsoft.com/en/library/dd314198%28v=ws.10%29.aspx
http://technet.microsoft.com/en/magazine/2009.05.goat.aspx
http://technet.microsoft.com/en/library/dd314173%28v=ws.10%29.aspx
http://ripusudan.wordpress.com/2013/03/19/how-to-configure-nap-enforcement-for-dhcp/
http://technet.microsoft.com/es-es/magazine/2009.05.goat.aspx
http://technet.microsoft.com/en-us/library/dd125379%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc772356%28v=ws.10%29.aspx



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


Network Policy Server
Ripusudan
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server G
Policies
Connection Request Polici
Network Policies
Health Policies
Network Access Protection
System Health Validators
Remediation Server Group
Accounting
System Health Validators allow
SHVs, configure the SHVs anc
Name
Windows Security Health Validator
Windows Security Health Validato
Status - Configured
Error Code Configurations:
SHV unable to contact required servi
SHA unable to contact required servi
SHA not responding to NAP Client:
SHV not responding:
Windows Security Health Validator Properties
Settings
To open and configure the system health validator program, click Configure.
Configure...
Error code resolution
Select how to resolve the following error codes that may be returned for this system health validator and its associated system health agent when a client requests network access.
SHV unable to contact required services
Noncompliant
SHA unable to contact required services
Noncompliant
SHA not responding to NAP Client
Noncompliant
SHV not responding
Noncompliant
Vendor specific error code received
Noncompliant
OK
Cancel
Apply


Windows Security Health Validator
Ripusudan
Windows Vista
Windows XP
Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.
Learn more...
Firewall
A firewall is enabled for all network connections
Virus Protection
An antivirus application is on
Antivirus is up to date
Spyware Protection
An antispyware application is on
Antispyware is up to date
Automatic Updating
Automatic updating is enabled
Security Update Protection
Restrict access for clients that do not have all available security updates installed
Important and above
Specify the minimum number of hours allowed since the client has checked for new security updates:
22
By default, clients can receive security updates from Microsoft Update. If additional sources are required for your deployment, select one or both of the following sources.
Window Server Update Services
Windows Update
OK
Cancel
Apply


Network Policy Server
Ripusudan
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server G
Policies
Connection Request Polici
Network Policies
Health Policies
Network Access Protection
System Health Validators
Remediation Server Group
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name | Status | Processing Order | Access Type
Connections to Microsoft Routing and Remote Access server | Enabled | 1 | Deny Access
Connections to other access servers | Enabled | 2 | Deny Access
NAP DHCP Compliant | Enabled | 3 | Grant Access
NAP DHCP Noncompliant | Enabled | 4 | Grant Access
NAP DHCP Non NAP-Capable | Enabled | 5 | Grant Access
NAP DHCP Non NAP-Capable Properties
Overview Conditions Constraints Settings
Remediation Servers and Troubleshooting URL
New Remediation Server Group
Group Name:
Domain Services
Remediation Servers:
DNS Name / IP Address | Friendly Name
main.server.com | main
Add...
Edit...
Remove
OK
Cancel
New Group...
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Prote
NAP Enforcement
Extended State
Routing and Remote A
Multilink and Bandw Allocation Protocol
IP Filters
Encryption
IP Settings
To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.
Configure...
1
2
3
4
5
6

QUESTION 126
HOTSPOT

You have a server named Server1 that runs Windows Server 2012. Server1 has the Remote Access server role installed. Server1 is located in the perimeter network.

The IPv4 routing table on Server1 is configured as shown in the following exhibit. (Click the Exhibit button.)

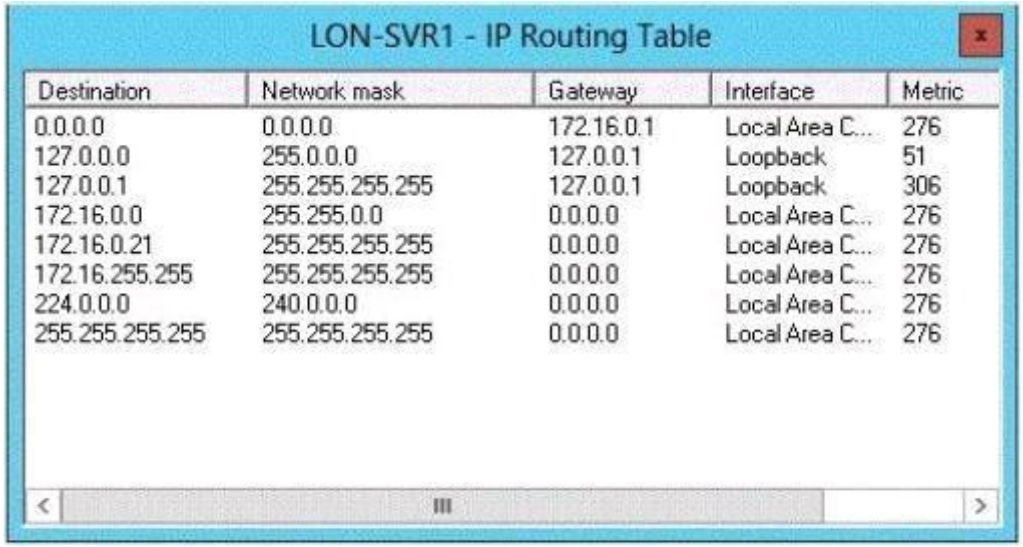
Your company purchases an additional router named Router1. Router1 has an interface that connects to the perimeter network and an interface that connects to the Internet. The IP address of the interface that connects to the perimeter network is 172.16.0.2.

You need to ensure that Server1 will route traffic to the Internet by using Router1 if the current default gateway is unavailable.

How should you configure the static route on Server1?

To answer, select the appropriate static route in the answer area.

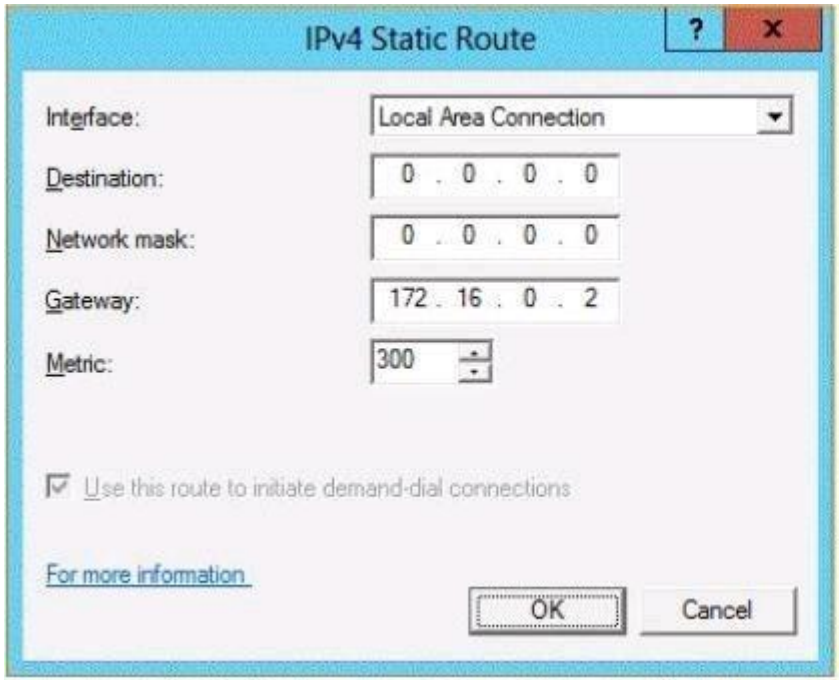
Exhibit:

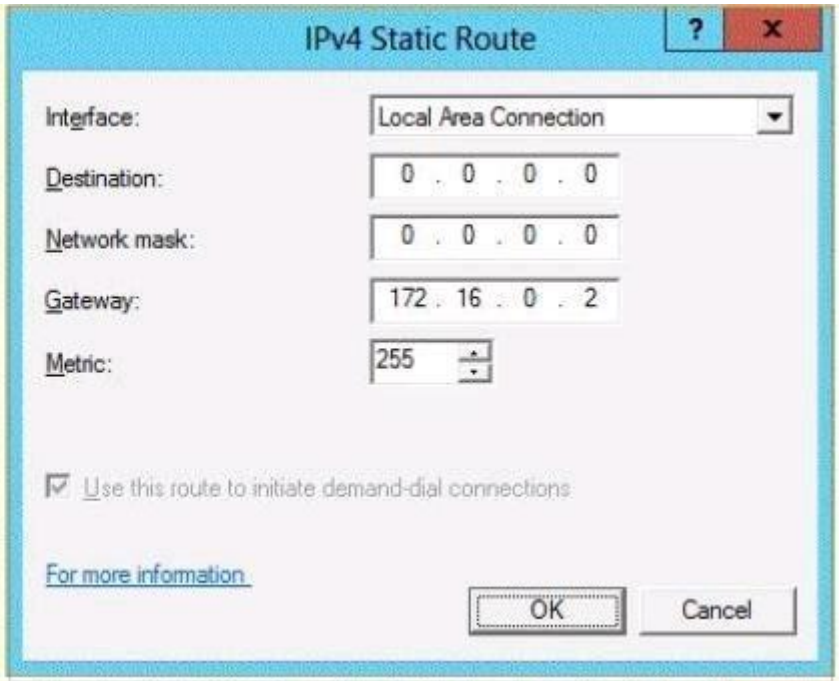


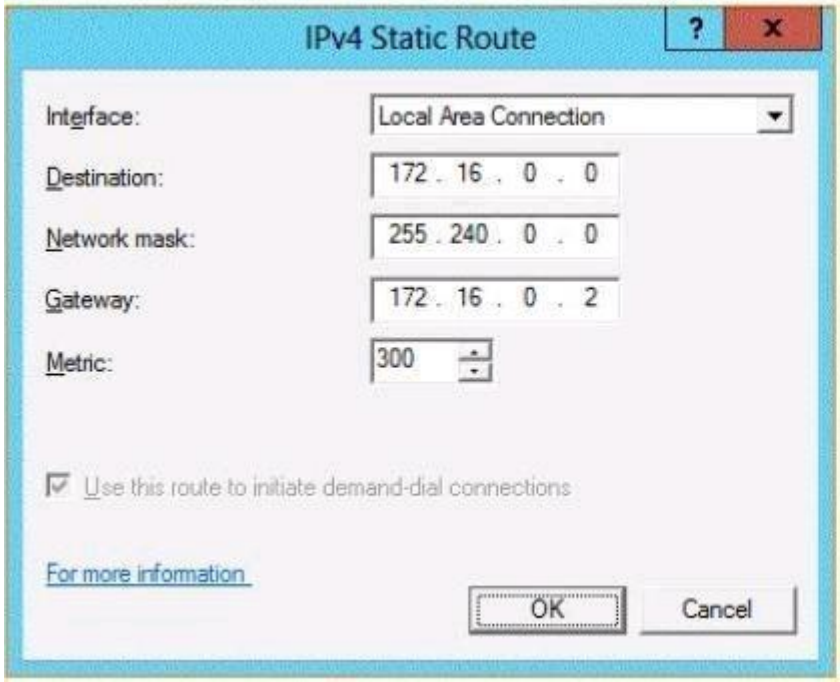
LON-SVR1 - IP Routing Table

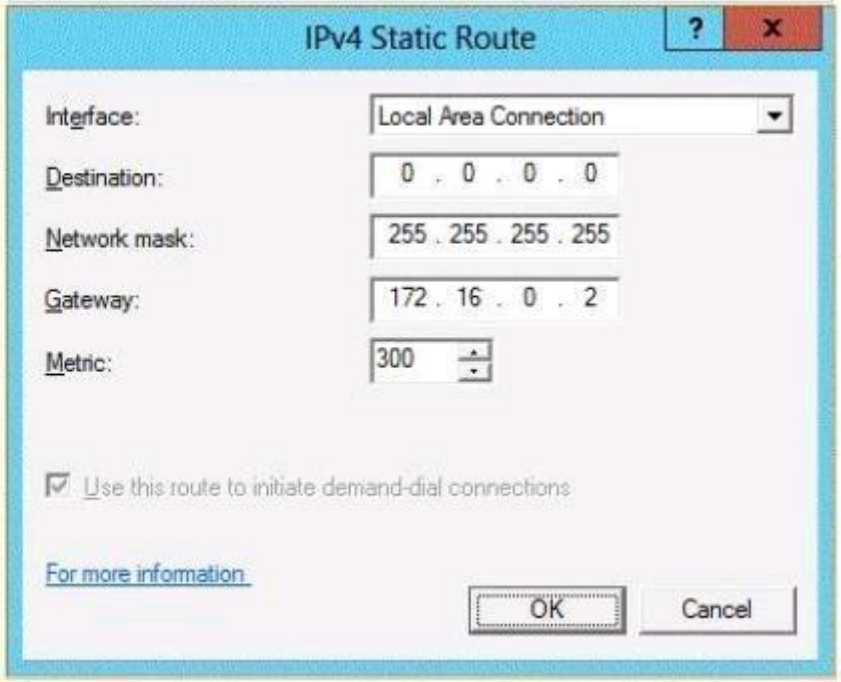
Destination	Network mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.16.0.1	Local Area C...	276
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	51
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	306
172.16.0.0	255.255.0.0	0.0.0.0	Local Area C...	276
172.16.0.21	255.255.255.255	0.0.0.0	Local Area C...	276
172.16.255.255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

Hot Area:


IPv4 Static Route
Interface:
Local Area Connection
Destination:
0 . 0 . 0 . 0
Network mask:
0 . 0 . 0 . 0
Gateway:
172 . 16 . 0 . 2
Metric:
300
Use this route to initiate demand-dial connections
For more information
OK
Cancel

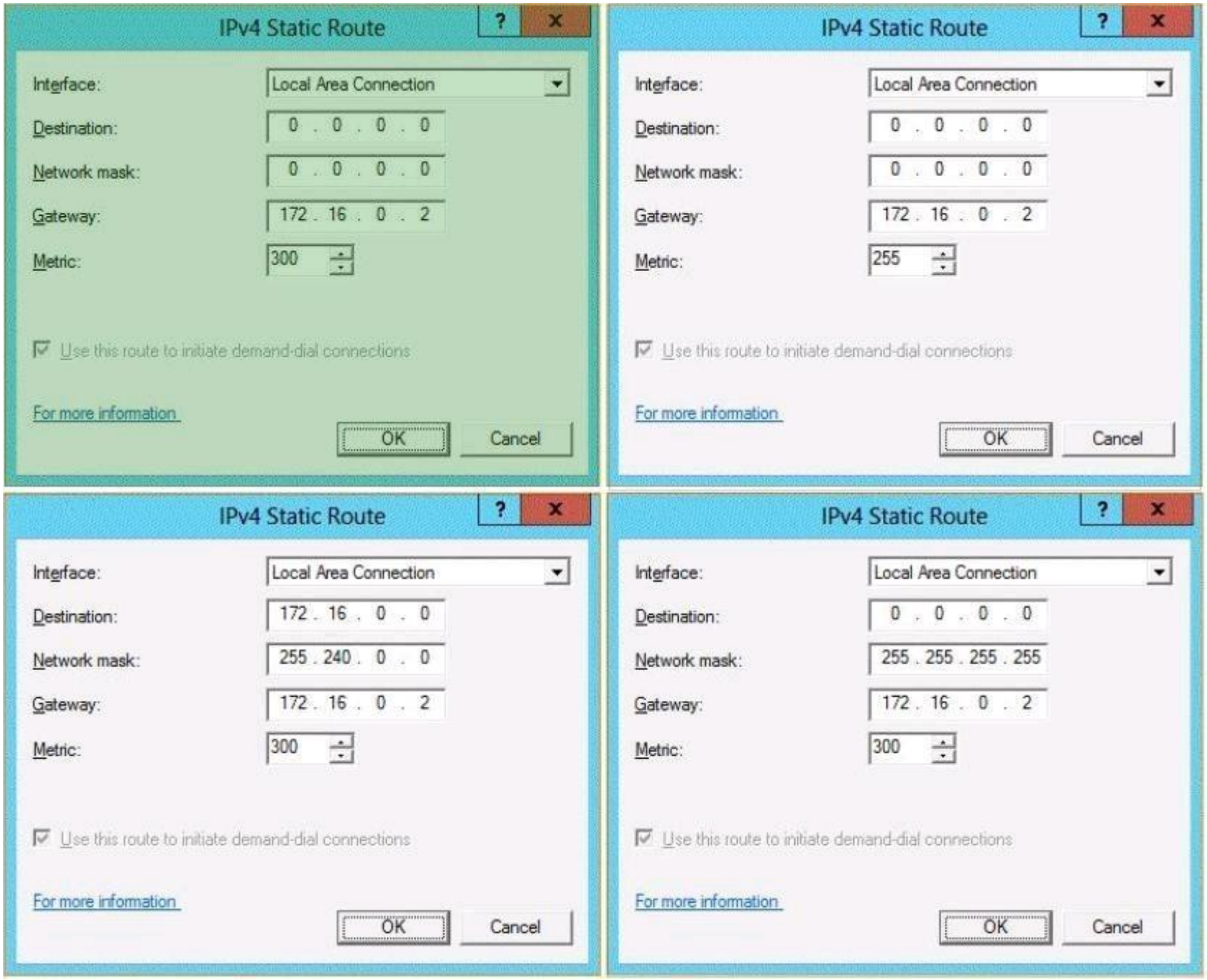

IPv4 Static Route
Interface:
Local Area Connection
Destination:
0 . 0 . 0 . 0
Network mask:
0 . 0 . 0 . 0
Gateway:
172 . 16 . 0 . 2
Metric:
255
Use this route to initiate demand-dial connections
For more information
OK
Cancel


IPv4 Static Route
Interface:
Local Area Connection
Destination:
172 . 16 . 0 . 0
Network mask:
255 . 240 . 0 . 0
Gateway:
172 . 16 . 0 . 2
Metric:
300
Use this route to initiate demand-dial connections
For more information
OK
Cancel


IPv4 Static Route
Interface:
Local Area Connection
Destination:
0 . 0 . 0 . 0
Network mask:
255 . 255 . 255 . 255
Gateway:
172 . 16 . 0 . 2
Metric:
300
Use this route to initiate demand-dial connections
For more information
OK
Cancel

Correct Answer:

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


IPv4 Static Route
Interface: Local Area Connection
Destination: 0 . 0 . 0 . 0
Network mask: 0 . 0 . 0 . 0
Gateway: 172 . 16 . 0 . 2
Metric: 300
Use this route to initiate demand-dial connections
For more information
OK
Cancel
IPv4 Static Route
Interface: Local Area Connection
Destination: 0 . 0 . 0 . 0
Network mask: 0 . 0 . 0 . 0
Gateway: 172 . 16 . 0 . 2
Metric: 255
Use this route to initiate demand-dial connections
For more information
OK
Cancel
IPv4 Static Route
Interface: Local Area Connection
Destination: 172 . 16 . 0 . 0
Network mask: 255 . 240 . 0 . 0
Gateway: 172 . 16 . 0 . 2
Metric: 300
Use this route to initiate demand-dial connections
For more information
OK
Cancel
IPv4 Static Route
Interface: Local Area Connection
Destination: 0 . 0 . 0 . 0
Network mask: 255 . 255 . 255 . 255
Gateway: 172 . 16 . 0 . 2
Metric: 300
Use this route to initiate demand-dial connections
For more information
OK
Cancel

Section: Configure a Network Policy infrastructure
Explanation

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

A metric is a value that is assigned to an IP route for a particular network interface that identifies the cost that is associated with using that route.
The metric that is assigned to specific default gateways can be configured independently for each gateway. This setup enables a further level of control over the metric that is used for the local routes.

QUESTION 127
Force an authoritative and non-authoritative synchronization for FRS-Replicated SYSVOL

A. dfsgui.msc
B. ultrasound
C. rplmon
D. frsutil

Correct Answer: D
Section: to review
Explanation

Explanation/Reference:
Active Directory (AD) uses Distributed File System Replication (DFSR) to replicate the disk-based portion of AD (SYSVOL) in Windows Server 2008 and later mode domains, replacing the old File Replication Service (FRS). DFSR has many advantages over FRS, including being far more efficient in the data it replicates.
One of the best ways to check the health of the SYSVOL replication using DFSR is to install the Distributed File System management tools on a machine. You can do this through Server Manager.

Select one or more roles to install on the selected server.

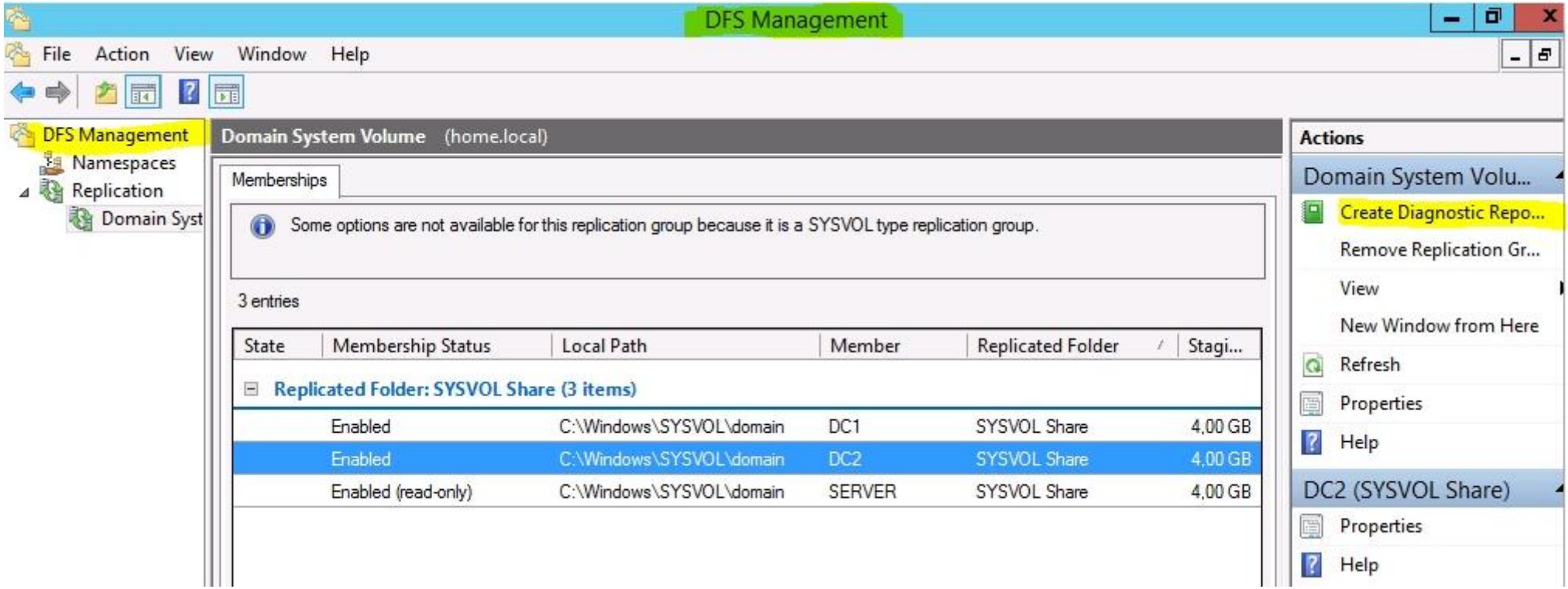
Roles

- [x] DNS Server (Installed)
- [ ] Fax Server
- [ ] File and Storage Services (2 of 12 installed)
  - [ ] File and iSCSI Services (1 of 11 installed)
    - [x] File Server (Installed)
    - [ ] BranchCache for Network Files
    - [ ] Data Deduplication
    - [ ] DFS Namespaces
    - [x] DFS Replication
    - [ ] File Server Resource Manager
    - [ ] File Server VSS Agent Service
    - [ ] iSCSI Target Server
    - [ ] iSCSI Target Storage Provider (VDS and VSS
    - [ ] Server for NFS

Description

DFS Replication is a multimaster replication engine that enables you to synchronize folders on multiple servers across local or wide area network (WAN) network connections. It uses the Remote Differential Compression (RDC) protocol to update only the portions of files that have changed since the last replication. DFS Replication can be used in conjunction with DFS Namespaces, or by itself.

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



http://msdn.microsoft.com/en-us/library/windows/desktop/cc507518%28v=vs.85%29.aspx#determining_whether_a_domain_controller_s_sysvol_folder_is_replicated_by_dfsr_or_frs

Determining Whether a Domain Controller's SYSVOL Folder is Replicated by DFSR or FRS

The following table summarizes how to determine whether a domain controller's SYSVOL folder is being replicated by DFSR or FRS.

If the domain controller is running	SYSVOL is replicated by
Windows Server 2008 + domain functional level of Windows Server 2008 + SYSVOL migration completed	DFSR
Windows Server 2008 + domain functional level below Windows Server 2008	FRS
Windows Server 2003	FRS

http://www.polymerit.co.uk/blog/2012/05/troubleshooting-sysvol-and-file-replication-service-issues/
http://support.microsoft.com/kb/2218556
http://windowsitpro.com/windows-server-2012/fixing-broken-sysvol-replication

QUESTION 128
I am using a Domain Admins account to run the console and the service is running under local system.I try approve Requests from Pending devices, then I got notice Access Denied, (Windows Server 2003 R2). And why Architecture x64, clients are x86 ? Is that the reason and how to fix it?

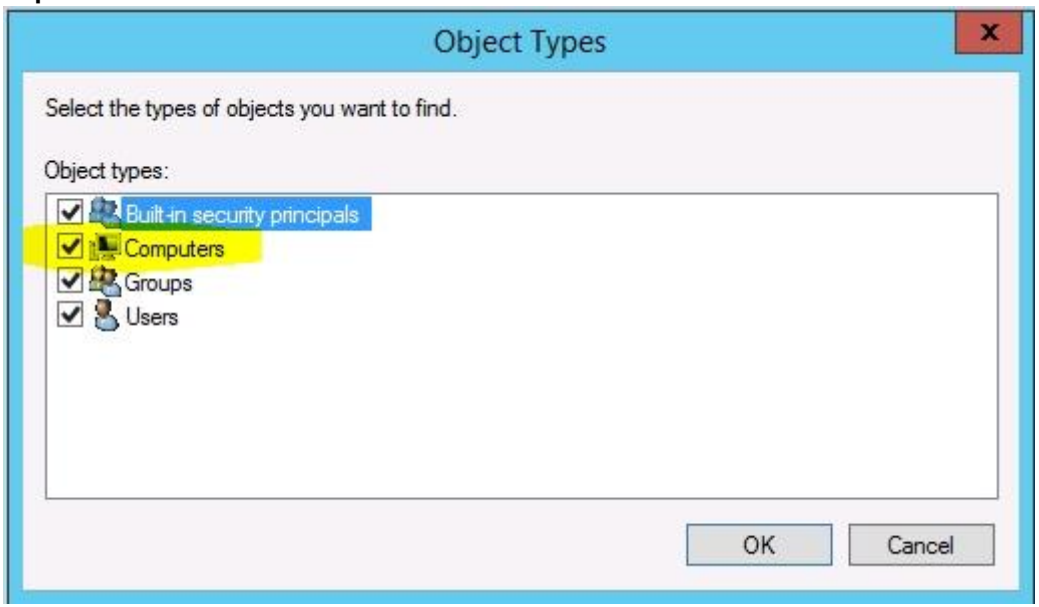
A. Open WDS and right click on the server and select properties. Then click on the tab "PXE Response settings" and select respond to all (known and unknown) client. And also select the little checkbox below.
B. You need to grant permissions on the OU in which you want to create machine accounts for the WDS Server Machine Account.
C. **To grant permissions to approve a pending computer**
Open **Active Directory Users and Computers**.
Right-click the OU where you are creating prestaged computer accounts, and then select **Delegate Control**.
On the first screen of the wizard, click **Next**.
Change the object type to include computers.
Add the computer object of the Windows Deployment Services server, and then click **Next**.

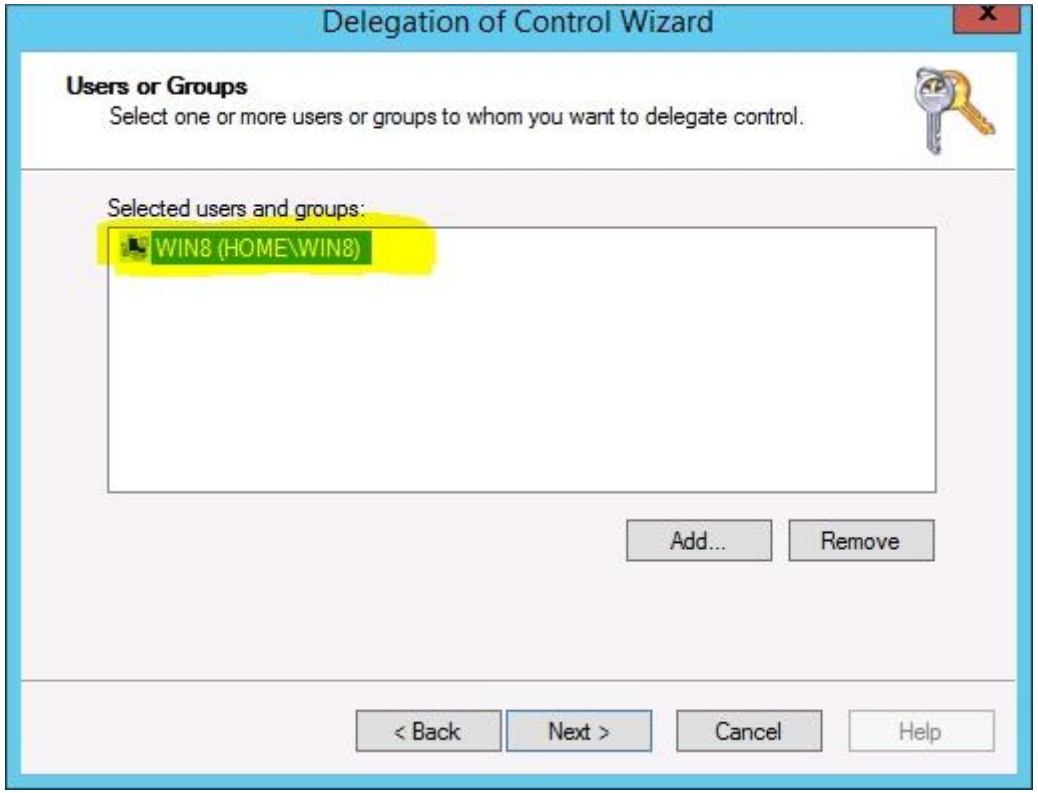
Select **Create a Custom task to delegate**.
Select **Only the following objects in the folder**. Then select the **Computer Objects** check box, select **Create selected objects in this folder**, and click **Next**.
In the Permissions box, select the **Write all Properties** check box, and click **Finish**.

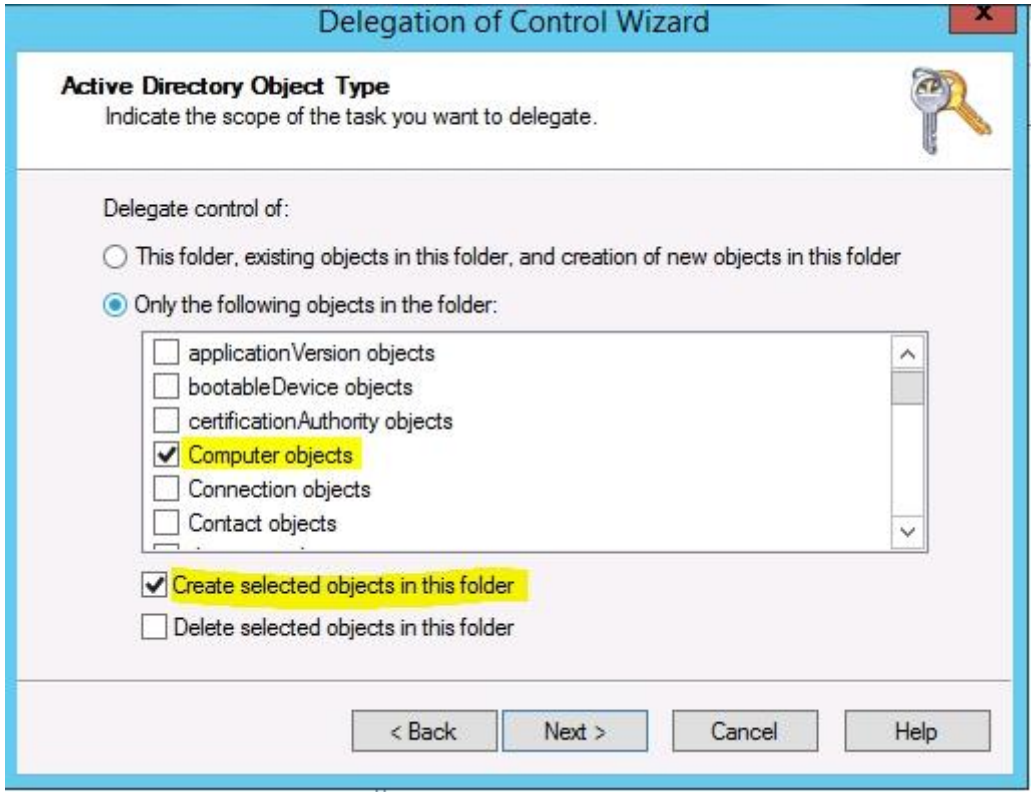
D. 1. Define the OU path to add systems in WDS
2. Delegate Computer object create or gretaer rights to the WDS server for the OU
3. Delegate computer object create rights to your account or simply use a domain admin account to logon

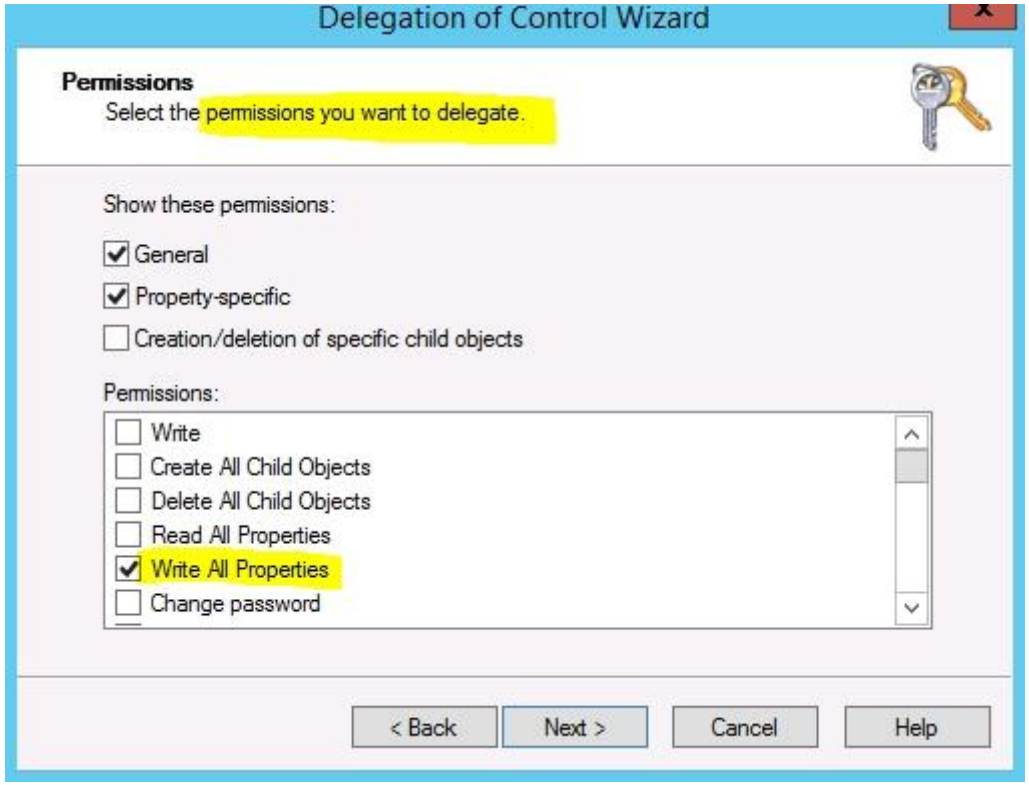
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:




Delegation of Control Wizard
Users or Groups
Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
WIN8 (HOME\WIN8)
Add...
Remove
< Back
Next >
Cancel
Help


Delegation of Control Wizard
Active Directory Object Type
Indicate the scope of the task you want to delegate.
Delegate control of:
This folder, existing objects in this folder, and creation of new objects in this folder
Only the following objects in the folder:
applicationVersion objects
bootableDevice objects
certificationAuthority objects
Computer objects
Connection objects
Contact objects
Create selected objects in this folder
Delete selected objects in this folder
< Back
Next >
Cancel
Help



http://technet.microsoft.com/en-us/library/cc754005(WS.10).aspx
http://technet.microsoft.com/en-us/library/cc766320(v=WS.10).aspx#BKMK_CreatingDiscover

QUESTION 129
force an authoritative and non-authoritative synchronization for DFSR-replicated SYSVOL

A. ldp
B. dfsgui.msc
C. ultrasound
D. rplmon

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
ldp: modify the distinguished name (DN) value and attribute on each of the domain controllers that you want to make synchronization (igualmente adsiedit)
http://support.microsoft.com/kb/2218556

Para lanzar la replicación se usa
DFSRDIAG POLLAD

dfsgui.msc: allows administrators to create DFS namespaces, add and remove targets, set the Time to Live for targets, enable and disable referrals, enable replication for DFS root or link targets, create custom replication schedules and topologies, and so forth. **SYSVOL is intentionally protected from any editing through its management interfaces to prevent accidents**.

ultrasound: is a monitoring and troubleshooting tool for the File Replication Service (FRS). FRS is a legacy technology that replicates files and folders that are stored in Distributed File System (DFS) folders or in the System Volume (SYSVOL) folder on domain controllers.

rplmon: Replication monitoring tool

http://slvirtualguy.com/2011/03/31/sysvol-and-netlogon-shared-folders-missing-after-a-non-authoritative-restore/

QUESTION 130
how to give the minimum required permission to a user who wants to promote a RODC.

A. member of the Domain Admins group
B. allowed to attach the server to the RODC computer account
C. Local admin
D. organization admin

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
http://technet.microsoft.com/en-us/library/jj574152.aspx

The **Delegation of RODC Installation and Administration** dialog enables you to configure a user or group containing users who are allowed to attach the server to the RODC computer account.
The user or group specified in this dialog gains local administrative permissions to the RODC. The specified user or members of the specified group can perform operations on the RODC with privileges equivalent to the computer's Administrators group. They are ***not*** members of the Domain Admins or domain built-in Administrators groups.

http://technet.microsoft.com/es-es/library/cc770627(v=ws.10).aspx

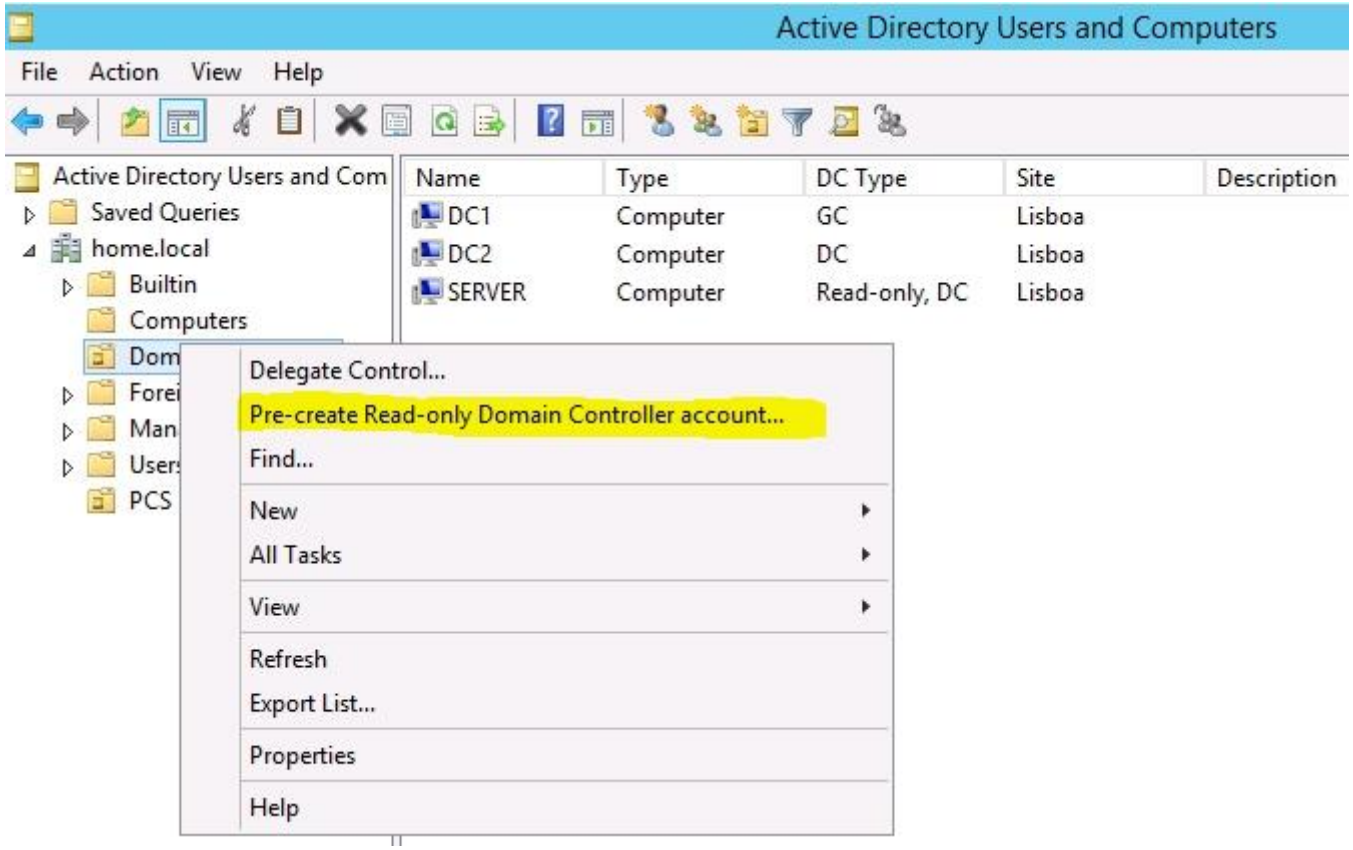
You can perform an installation of a read-only domain controller (RODC) in which the installation is completed in two stages by different individuals. The first stage of the installation, which requires Domain Admin credentials, creates an account for the RODC in Active Directory Domain Services (AD DS). The second stage of the installation attaches the actual server that will be the RODC in a remote location, such as a branch office, to the account that was previously created for it. **You can delegate the ability to attach the server to a nonadministrative group or user**.

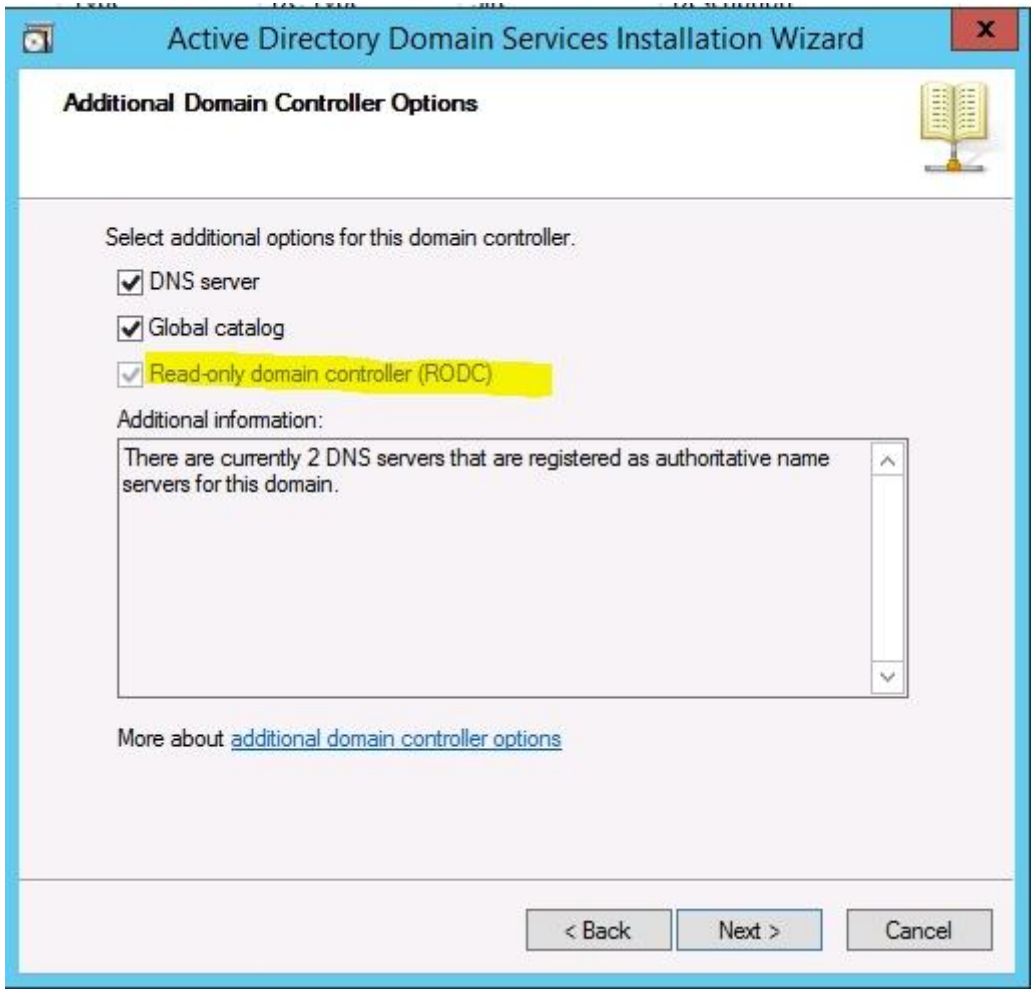
During this first stage, the Active Directory Domain Services Installation Wizard records all data about the RODC that will be stored in the distributed Active Directory database, such as its domain controller account name and the site in which it will be placed. This stage must be performed by a member of the Domain Admins group.

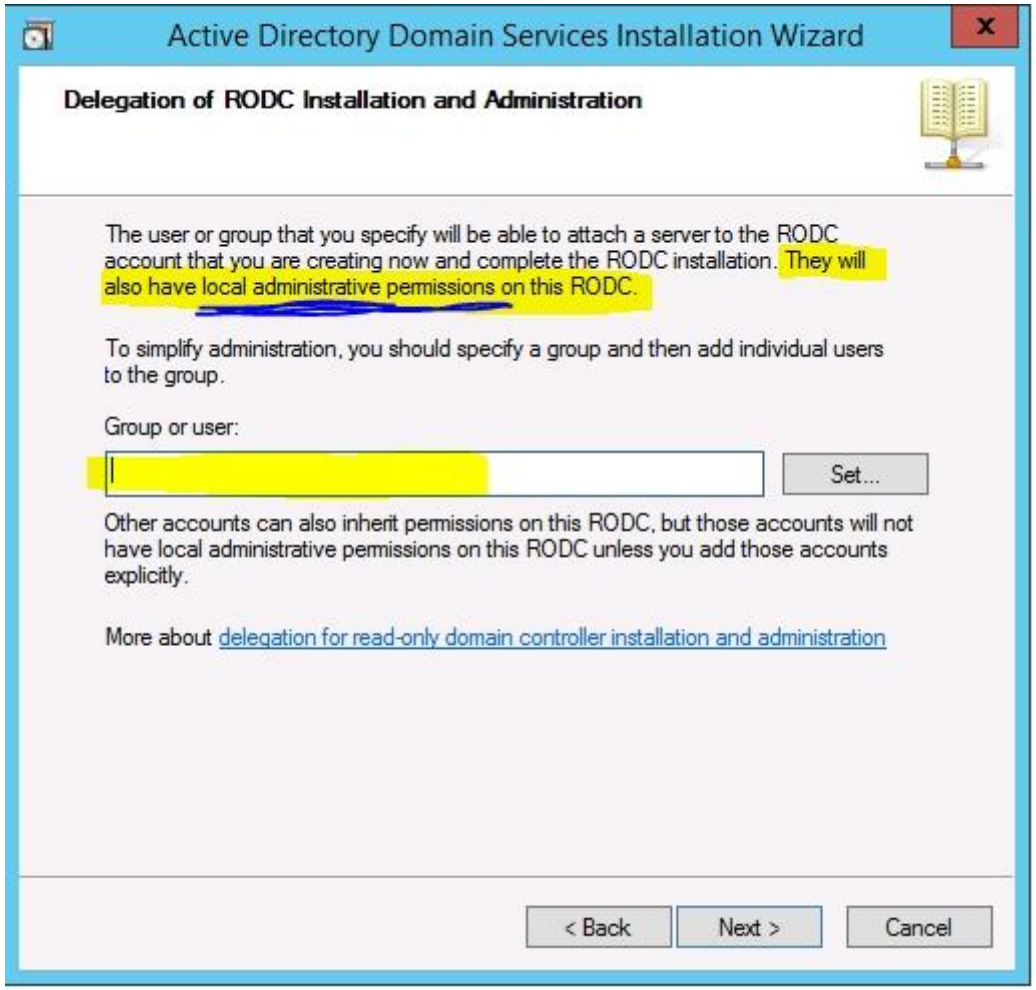
The administrator who creates the RODC account can also specify at that time which users or groups can complete the next stage of the installation. The next stage of the installation can be performed in the branch office by any user or group who was delegated the right to complete the installation when the account was created. This stage does not require any membership in built-in groups, such as the Domain Admins group. If the user who creates the RODC account does not specify any delegate to complete the installation (and administer the RODC), only a member of the Domain Admins or Enterprise Admins groups can complete the installation.

During the second stage, the wizard installs AD DS on the server that will become the RODC and it attaches the server to the domain account that was previously created for it. This stage typically occurs in the branch office where the RODC is deployed. During this stage, all Active Directory data that resides locally, such as the database, log files, and so on, is created on the RODC itself. The installation source files can be replicated to the RODC from another domain controller over the network, or you can use the install from media (IFM) feature. To use IFM, use Ntdsutil.exe to create the installation media.

The server that will become the RODC must not be joined to the domain before you try to attach it to the RODC account. As part of the installation, the wizard automatically detects whether the name of the server matches the names of any RODC accounts that have been created in advance for the domain. When the wizard finds a matching account name, it prompts the user to use that account to complete the RODC installation.


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
home.local
Builtin
Computers
Dom
Forei
Man
Users
PCS
Name
Type
DC Type
Site
Description
DC1
Computer
GC
Lisboa
DC2
Computer
DC
Lisboa
SERVER
Computer
Read-only, DC
Lisboa
Delegate Control...
Pre-create Read-only Domain Controller account...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help


Active Directory Domain Services Installation Wizard
Additional Domain Controller Options
Select additional options for this domain controller.
DNS server
Global catalog
Read-only domain controller (RODC)
Additional information:
There are currently 2 DNS servers that are registered as authoritative name servers for this domain.
More about additional domain controller options
< Back
Next >
Cancel



QUESTION 131
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.
A domain controller named DC1 has the ADMX Migrator tool installed. You have a custom Administrative Template file on DC1 named Template1.adm.
You need to add a custom registry entry to Template1.adm by using the ADMX Migrator tool.

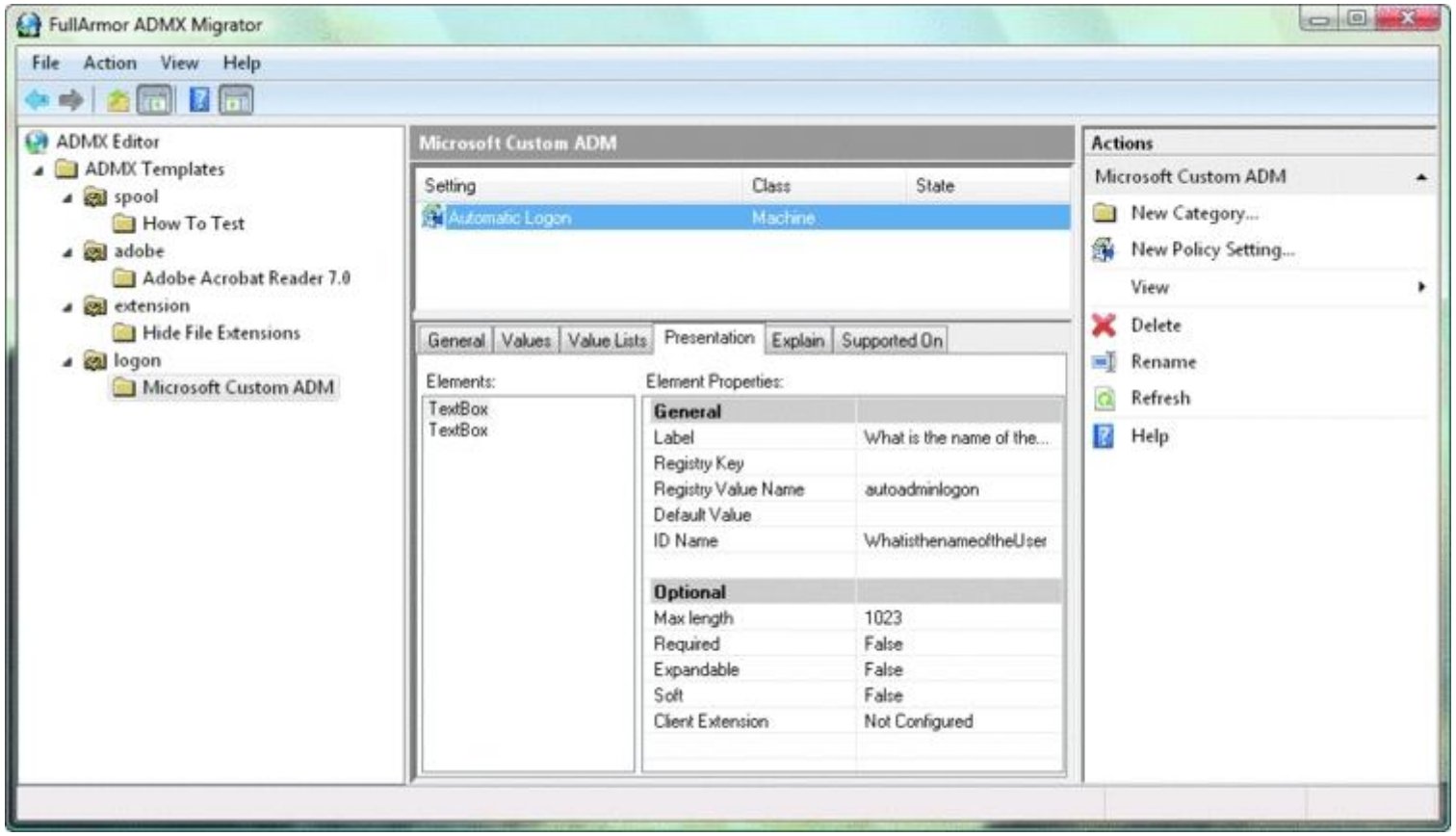
Which action should you run first?

A. New Category

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

Correct Answer: D
Section: (none)
Explanation

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



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

QUESTION 132
Your network contains an Active Directory domain named contoso.com.
You need to audit access to removable storage devices.

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

Hot Area:

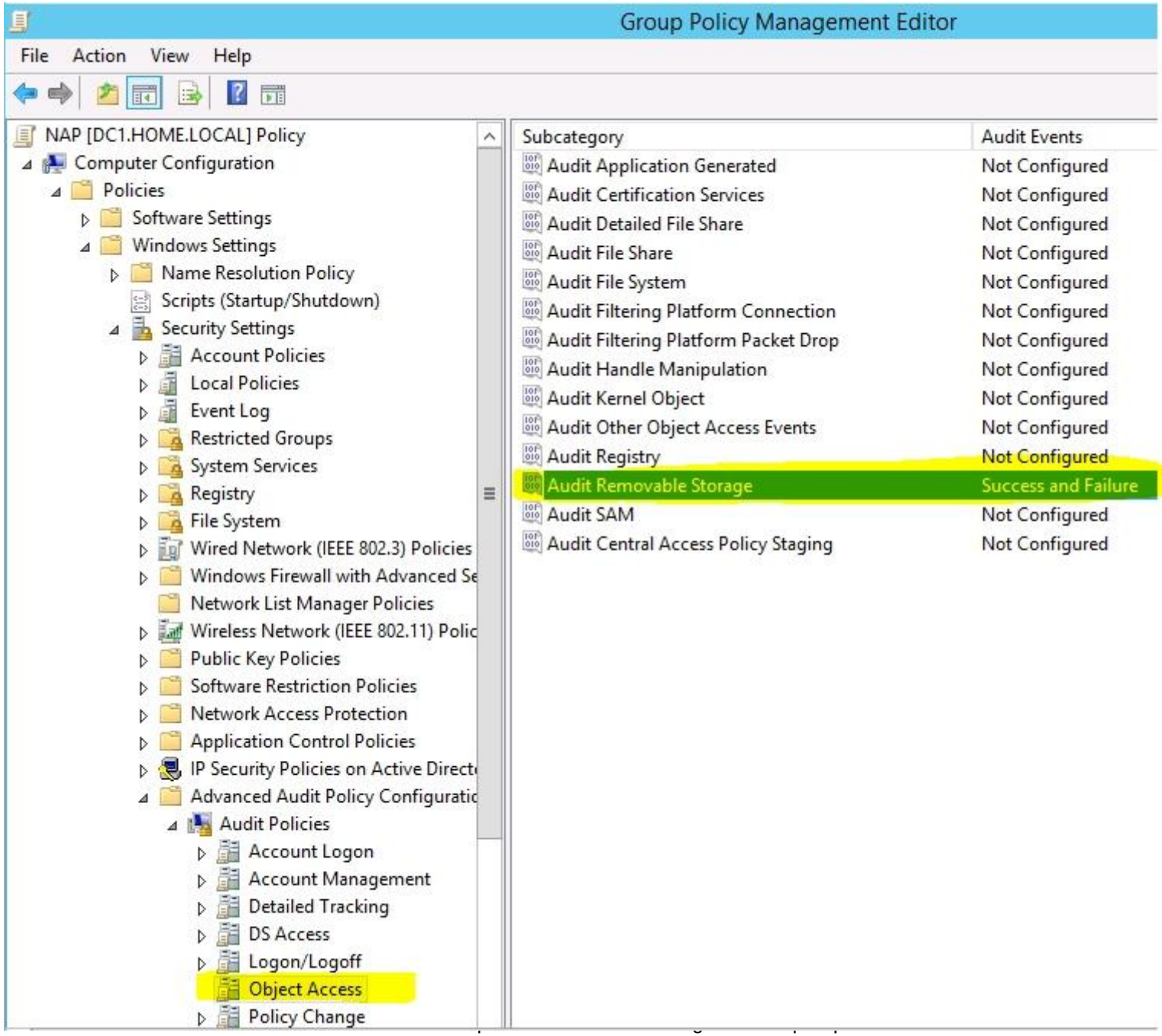
Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Correct Answer:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Section: (none)
Explanation

Explanation/Reference:
If you configure this policy setting, an audit event is generated each time a user attempts to copy, move, or save a resource to a removable storage device.


Group Policy Management Editor
File
Action
View
Help
NAP [DC1.HOME.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Direct
Advanced Audit Policy Configuratic
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Subcategory
Audit Events
Audit Application Generated
Not Configured
Audit Certification Services
Not Configured
Audit Detailed File Share
Not Configured
Audit File Share
Not Configured
Audit File System
Not Configured
Audit Filtering Platform Connection
Not Configured
Audit Filtering Platform Packet Drop
Not Configured
Audit Handle Manipulation
Not Configured
Audit Kernel Object
Not Configured
Audit Other Object Access Events
Not Configured
Audit Registry
Not Configured
Audit Removable Storage
Success and Failure
Audit SAM
Not Configured
Audit Central Access Policy Staging
Not Configured

To configure settings to monitor removable storage devices

1. Sign in to your domain controller by using domain administrator credentials.
2. In Server Manager, point to **Tools**, and then click **Group Policy Management**.
3. In the console tree, right-click the flexible access Group Policy Object on the domain controller, and then click **Edit**.
4. Double-click **Computer Configuration**, double-click **Security Settings**, double-click **Advanced Audit Policy Configuration**, double-click **Object Access**, and then double-click **Audit Removable Storage**.
5. Select the **Configure the following audit events** check box, select the **Success** check box (and the **Failure** check box, if desired), and then click **OK**.
6. If you selected the **Failure** check box, double-click **Audit Handle Manipulation**, select the **Configure the following audit events check box**, and then select **Failure**.
7. Click **OK**, and then close the Group Policy Management Editor.

http://technet.microsoft.com/en-us/library/jj574128.aspx

QUESTION 133
Your network contains an Active Directory domain named adatum.com.
You need to audit changes to the files in the SYSVOL shares on all of the domain controllers.
The solution must minimize the amount of SYSVOL replication traffic caused by the audit.

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

A. Audit Policy\Audit system events
B. Advanced Audit Policy Configuration\DS Access
C. Advanced Audit Policy Configuration\Global Object Access Auditing
D. Audit Policy\Audit object access
E. Audit Policy\Audit directory service access
F. Advanced Audit Policy Configuration\Object Access

Correct Answer: DF
Section: (none)

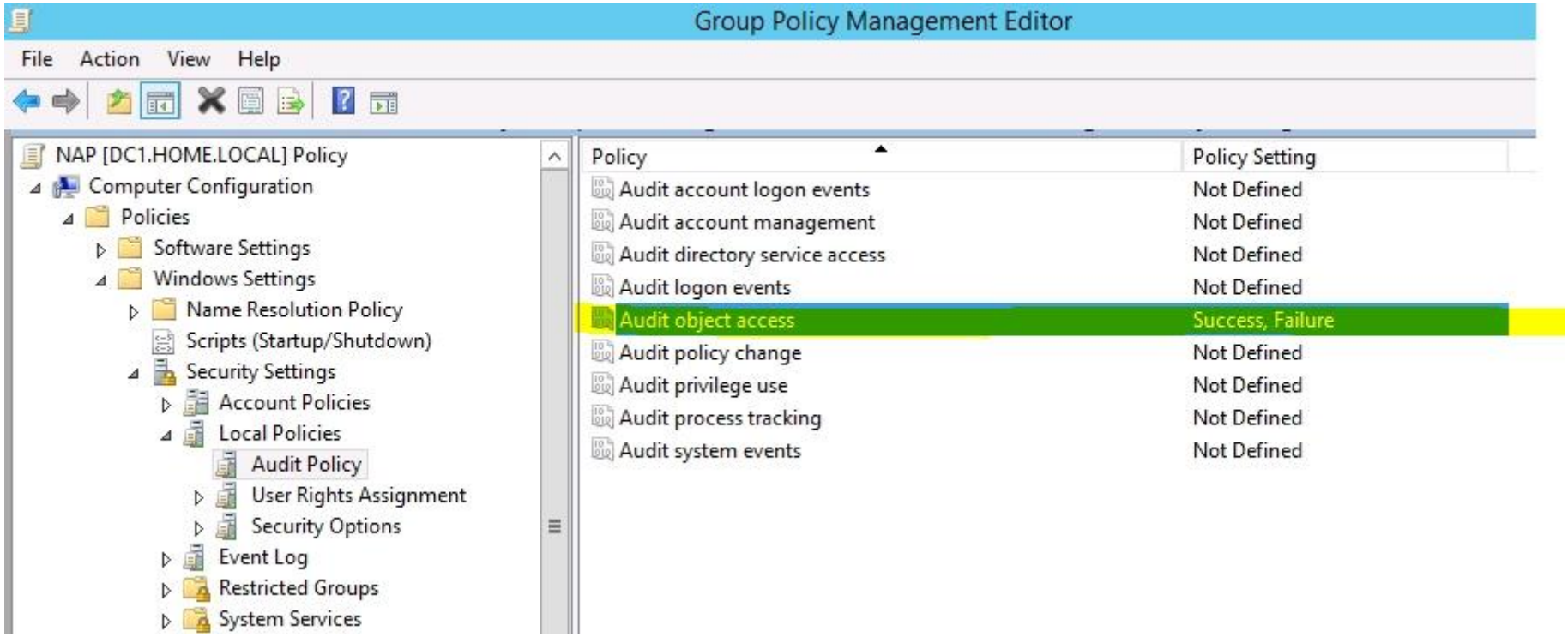
Explanation

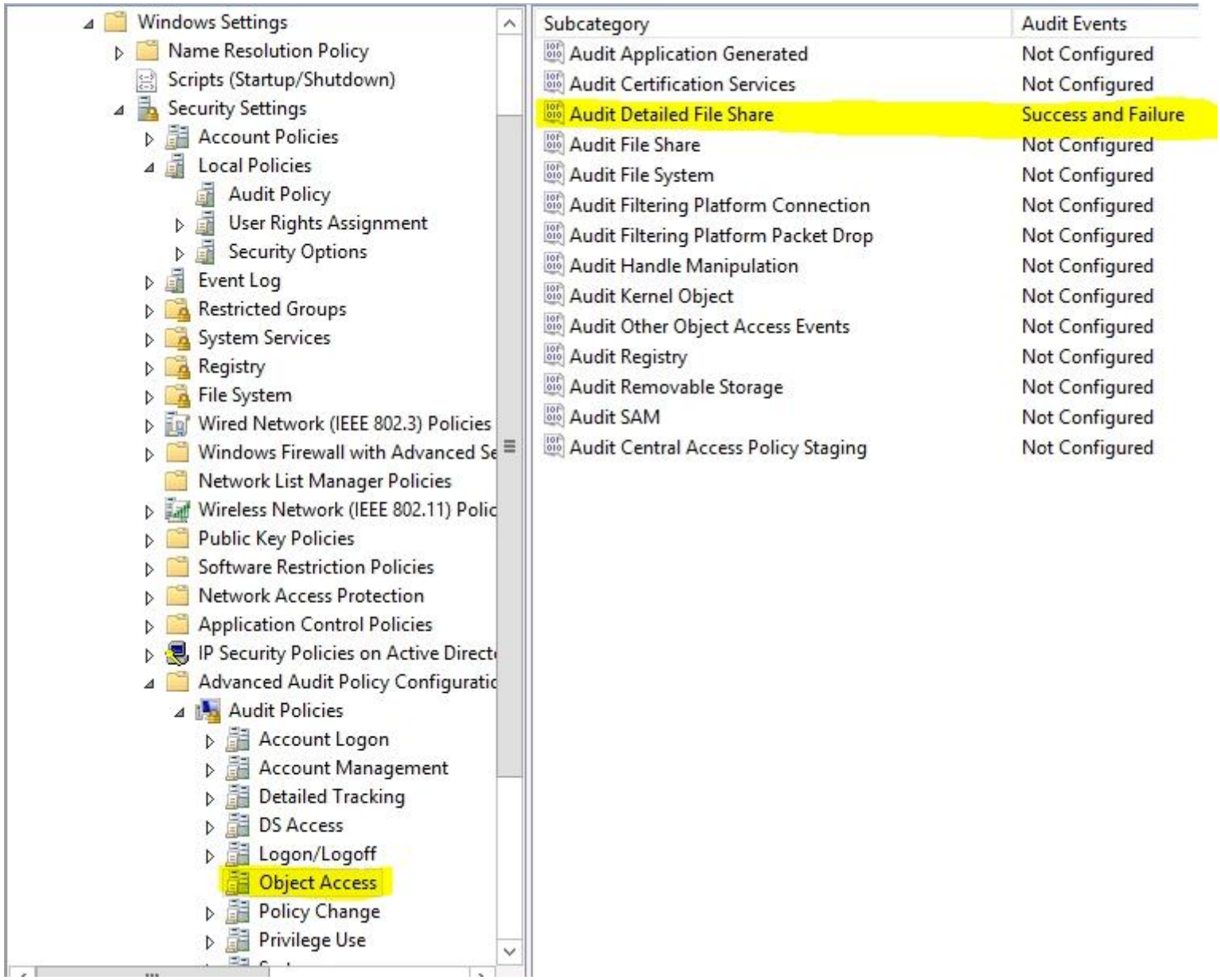
Explanation/Reference:
http://technet.microsoft.com/en-us/library/dd772690(v=ws.10).aspx

There are no system access control lists (SACLs) for shares; therefore, once this setting is enabled, access to all shares on the system will be audited.

The answer to that question should be

Audit Policy\Audit object access
Advanced Audit Policy Configuration\Object Access
In that there is a security setting "Access File Share" and "Access Detailed file share".




Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Direct
Advanced Audit Policy Configuratic
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
Subcategory
Audit Events
Audit Application Generated
Not Configured
Audit Certification Services
Not Configured
Audit Detailed File Share
Success and Failure
Audit File Share
Not Configured
Audit File System
Not Configured
Audit Filtering Platform Connection
Not Configured
Audit Filtering Platform Packet Drop
Not Configured
Audit Handle Manipulation
Not Configured
Audit Kernel Object
Not Configured
Audit Other Object Access Events
Not Configured
Audit Registry
Not Configured
Audit Removable Storage
Not Configured
Audit SAM
Not Configured
Audit Central Access Policy Staging
Not Configured

QUESTION 134
Your network contains an Active Directory domain named contoso.com. You have several Windows PowerShell scripts that execute when client computers start.
When a client computer starts, you discover that it takes a long time before users are prompted to log on.
You need to reduce the amount of time it takes for the client computers to start.
The solution must not prevent scripts from completing successfully.

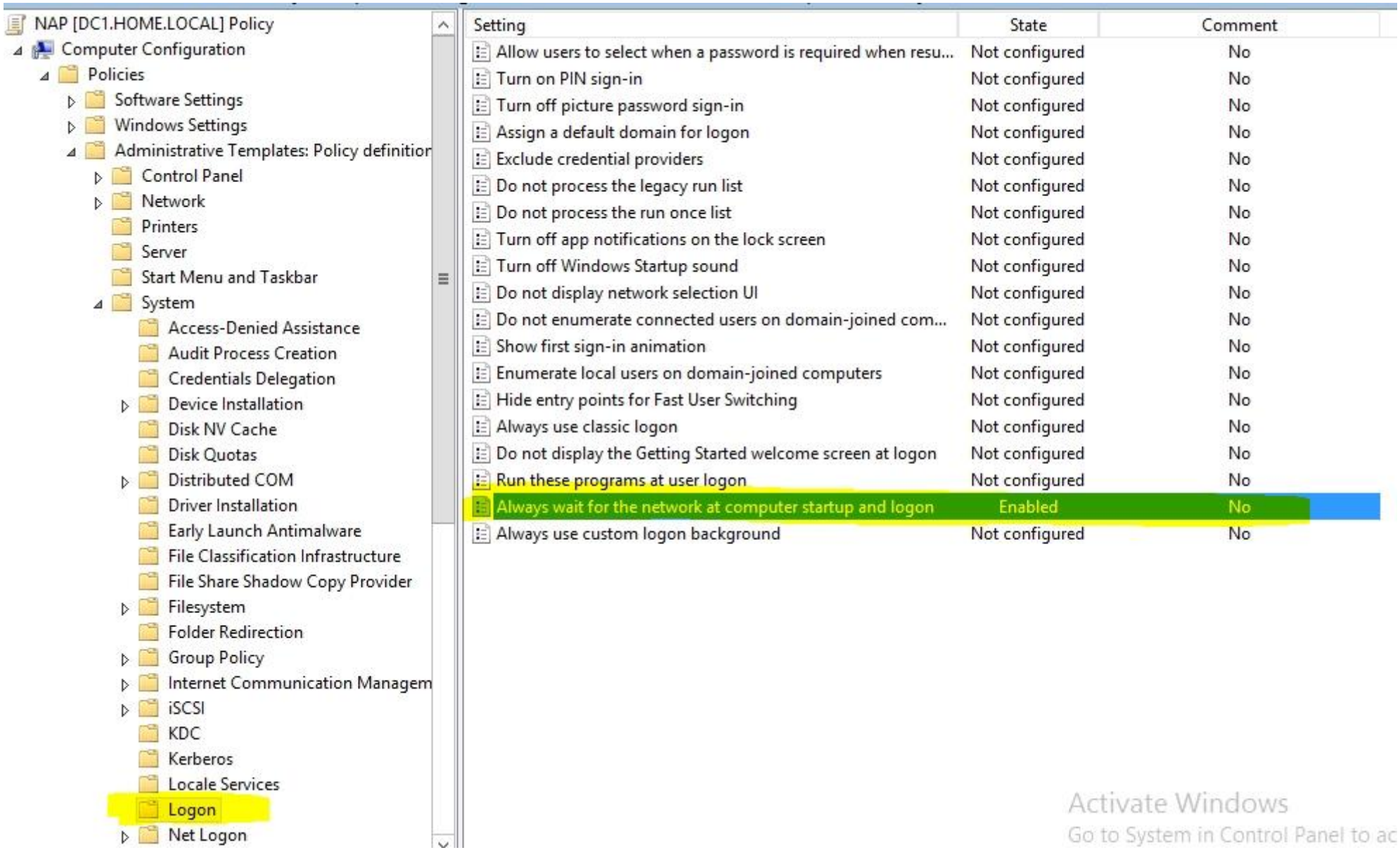
Which setting should you configure? To answer, select the appropriate setting in the answer area.

Hot Area:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:



http://technet.microsoft.com/en-us/magazine/gg486839.aspx

---

http://technet.microsoft.com/en-us/library/cc958585.aspx

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

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

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

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

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

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

QUESTION 135
You are a network administrator of an Active Directory domain named contoso.com. You have a server named Server1 that runs Windows Server 2012.
Server1 has the Web Server (IIS) server role installed. Server1 will host a web site at URL https://secure.contoso.com.
The application pool identity account of the web site will be set to a domain user account named AppPool1.
You need to identify the setspn.exe command that you must run to configure the appropriate Service Principal Name (SPN) for the web site.

What should you run? To answer, drag the appropriate objects to the correct location. Each object may be used once, more than once, or not at all.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
ATT: with Windows 2008 option is -a but with Windows 2012 it started to show -s

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

Adding SPNs

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

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

For example, the command may resemble the following command:

setspn –S HTTP/iis6server1.mydomain.com mydomain\appPool1

http://support.microsoft.com/kb/929650/en-us
http://technet.microsoft.com/en-us/library/cc731241%28v=ws.10%29.aspx

QUESTION 136
Your network contains an Active Directory domain named contoso.com. You deploy a web-based application named App1 to a server named Server1.
App1 uses an application pool named AppPool1. AppPool1 uses a domain user account named User1 as its identity.
You need to configure Kerberos constrained delegation for User1.

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

Select and Place:

Actions	Answer Area
Run **setspn.exe** and specify the *–l* parameter.	
From the properties of User1, open the **Delegation** tab, and add the **HOST** service.	
From the properties of User1, open the Delegation tab, and select Trust this user for delegation to any service (Kerberos only).	
From the properties of User1, open the Delegation tab, and select Trust this user for delegation to specified services only.	
Run **setspn.exe** and specify the *–s* parameter.	

Correct Answer:

Actions	Answer Area
Run **setspn.exe** and specify the *-l* parameter.	Run **setspn.exe** and specify the *-l* parameter.
From the properties of User1, open the **Delegation** tab, and add the **HOST** service.	Run **setspn.exe** and specify the *-s* parameter.
From the properties of User1, open the Delegation tab, and select Trust this user for delegation to any service (Kerberos only).	From the properties of User1, open the Delegation tab, and select Trust this user for delegation to specified services only.
From the properties of User1, open the Delegation tab, and select Trust this user for delegation to specified services only.	
Run **setspn.exe** and specify the *-s* parameter.	

Section: (none)
Explanation

Explanation/Reference:
first answer should be "setspn -L" - to check for SPNs of User1. After that we should add HTTP SPN for User1 "setspn -s" so delegation tab appears and we can select "Trust this user for delegation to specified services only"

http://support.microsoft.com/kb/929650/en-us
http://technet.microsoft.com/pt-pt/library/cc755413%28v=ws.10%29.aspx

List currently registered SPNs

```
setspn -l daserver1
Registered ServicePrincipalNames for CN=DASERVER1,CN=Computers,DC=reskit,DC=microsoft,DC=com:
HOST/daserver1
HOST/daserver1.reskit.microsoft.com
```

QUESTION 137
Your network contains an Active Directory domain called contoso.com. The domain contains a domain controller named DC1 that runs Windows server 2012.
The domain contains some test client computers that run either Windows XP, Windows Vista, Windows 7, or Windows 8.
The computer accounts for the test computers are located in an organizational unit (OU) named OU1.
You have a Group Policy object (GPO) named GPO1 linked to OU1. GPO1 is used to assign several applications to the test computers.
You need to ensure that when the test computers in OU1 restart, you can see which application installation is running currently.

Which setting should you modify in GPO1? To answer, select the appropriate setting in the answer area.

Hot Area:

Group Policy Management Editor

File Action View Help

Setting

- Download missing COM components
- Allow Distributed Link Tracking clients to use domain resources
- Do not automatically encrypt files moved to encrypted folders
- Do not turn off system power after a Windows system shutdown has occurred.
- Enable Persistent Time Stamp
- Activate Shutdown Event Tracker System State Data feature
- Display Shutdown Event Tracker
- Do not display Manage Your Server page at logon
- Specify settings for optional component installation and component repair
- Turn off Data Execution Prevention for HTML Help Executible
- Restrict potentially unsafe HTML Help functions to specified folders
- Restrict these programs from being launched from Help
- Remove Boot / Shutdown / Logon / Logoff status messages
- Display highly detailed status messages

Correct Answer:

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

Group Policy Management Editor

File Action View Help

Setting

- Download missing COM components
- Allow Distributed Link Tracking clients to use domain resources
- Do not automatically encrypt files moved to encrypted folders
- Do not turn off system power after a Windows system shutdown has occurred.
- Enable Persistent Time Stamp
- Activate Shutdown Event Tracker System State Data feature
- Display Shutdown Event Tracker
- Do not display Manage Your Server page at logon
- Specify settings for optional component installation and component repair
- Turn off Data Execution Prevention for HTML Help Executible
- Restrict potentially unsafe HTML Help functions to specified folders
- Restrict these programs from being launched from Help
- Remove Boot / Shutdown / Logon / Logoff status messages
- Display highly detailed status messages

Section: (none)
Explanation

Explanation/Reference:
Display highly detailed status messages
If verbose logging is not enabled, you will still receive normal status messages such as "Applying your personal settings..." or "Applying computer settings..." when you start up, shut down, log on, or log off the computer. However, if verbose logging is enabled, you will receive additional information, such as "RPCSS is starting" or "Waiting for machine group policies to finish...."

http://support.microsoft.com/kb/325376/en-us
http://msdn.microsoft.com/en-us/library/ms813386.aspx

Verbose vs normal status messages

This topic has not yet been rated

Computer Configuration\Administrative Templates\System

Description

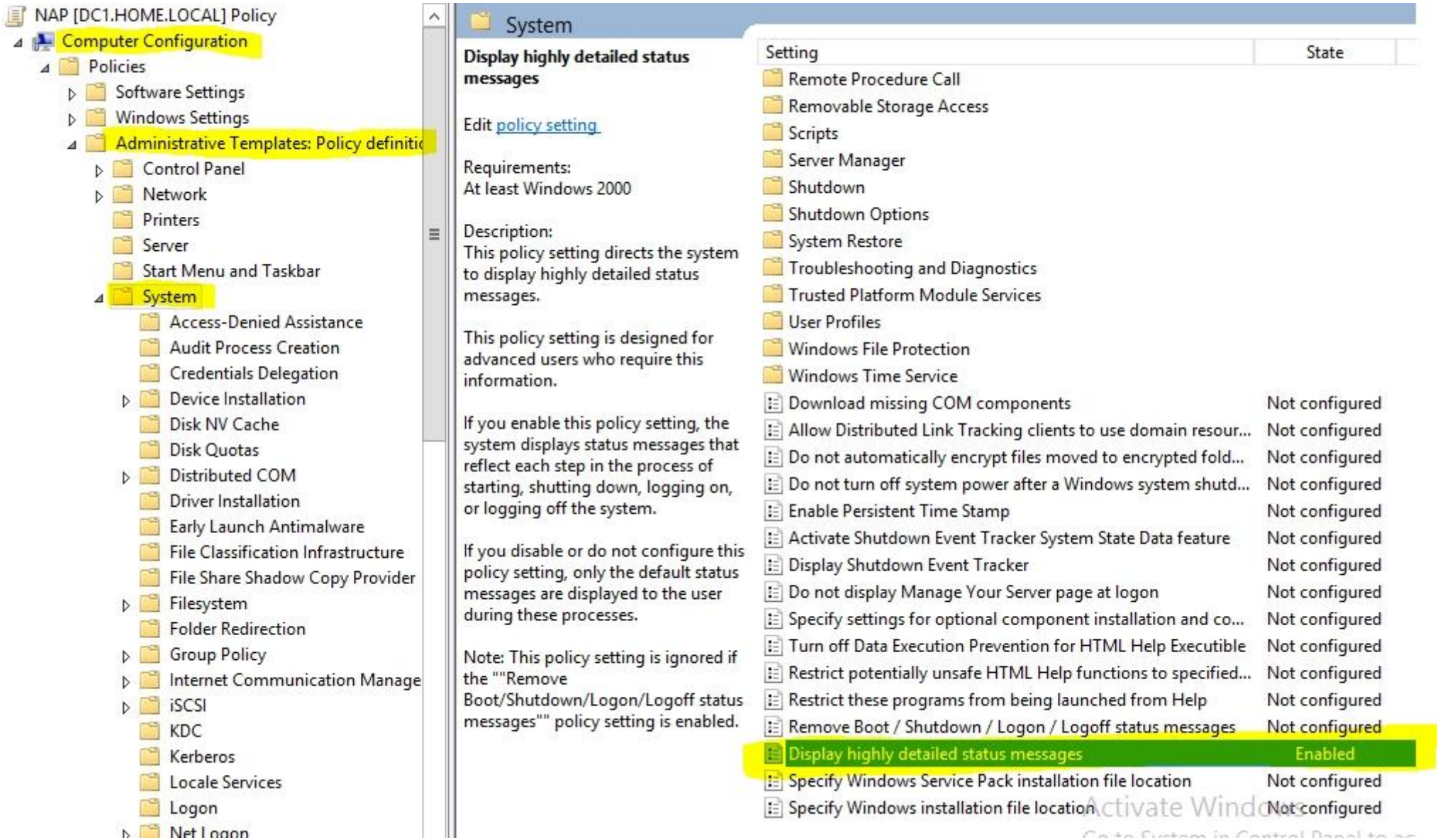
Directs the system to display highly detailed status messages.

If you enable this policy, the system displays status message that reflect each step in the process of starting, shutting down, logging on, or logging off the system.

Important

This policy is ignored if the Disable Boot / Shutdown / Logon / Logoff status messages policy is enabled.

http://msdn.microsoft.com/en-us/library/ms813386.aspx



QUESTION 138

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

You create an Active Directory snapshot of DC1 each day.

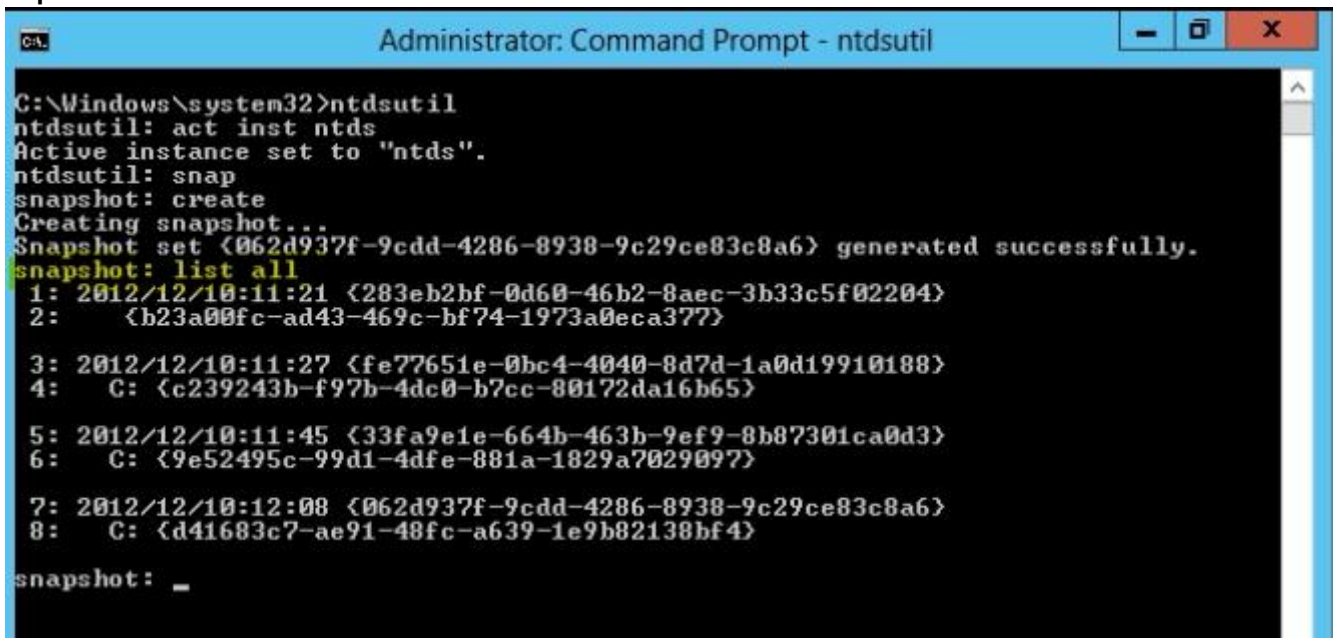
You need to view the contents of an Active Directory snapshot from two days ago.

What should you do first?

A. Run the dsamain.exe command.
B. Stop the Active Directory Domain Services (AD DS) service.
C. Run the ntdsutil.exe command.
D. Start the Volume Shadow Copy Service (VSS).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:



Explanation:

Mounting an Active Directory snapshot

Before connecting to the snapshot we need to mount it. By looking at the results of the List All command in step #8 above, identify the snapshot that you wish to mount, and note the number next to it.
In order to mount an Active Directory snapshot follow these steps:
Log on as a member of the Domain Admins group to one of your Windows Server 2008 Domain Controllers.
Open a Command Prompt window by clicking on the CMD shortcut in the Start menu, or by typing CMD and pressing Enter in the Run or Quick Search parts of the Start menu.

Note: You must run NTDSUTIL from an elevated command prompt. To open an elevated command prompt, click Start, right-click Command Prompt, and then click Run as administrator.
In the CMD window, type the following command:
ntdsutil

In the CMD window, type the following command:
snapshot

To view all available snapshots, in the CMD window, type the following command:
list all

The result should look like this:
snapshot: List All
1: 2008/10/25:03:14 {ec53ad62-8312-426f-8ad4-d47768351c9a}
2: C: {15c6f880-cc5c-483b-86cf-8dc2d3449348}

In this example we only have one snapshot available, one from 2008/10/25 at 03:14AM (yes, I write articles at this time…). We'll mount this one.

In the CMD window, type the following command:
mount 2

The result should look like this:
snapshot: mount 2
Snapshot {15c6f880-cc5c-483b-86cf-8dc2d3449348} mounted as C:'$SNAP_200810250314_VOLUMEC$'

Next, you can leave the NTDSUTIL running, or you can quit by typing quit 2 times.

Note: Like the above command, the mounting process can also be run in one line. However, note that ***NTDSUTIL requires that the "list all" command be run in the same session that you mount the snapshot***. So in order to mount the snapshot with a one-liner, you will need to run "list all" first.

ntdsutil snapshot "list all" "mount 2" quit quit

Note: You do not need to quit from the NTDSUTIL command, you can keep it open assuming that you'll probably want to unmount the snapshot right after working with it.

QUESTION 139
Your network contains an Active Directory domain named adatum.com. All domain controllers run Windows Server 2012. The domain contains a virtual machine named DC2.

On DC2, you run Get-ADDCCloningExcludedApplicationList and receive the output shown in the following table.

Name	Type
App1	Service

You need to ensure that you can clone DC2.

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

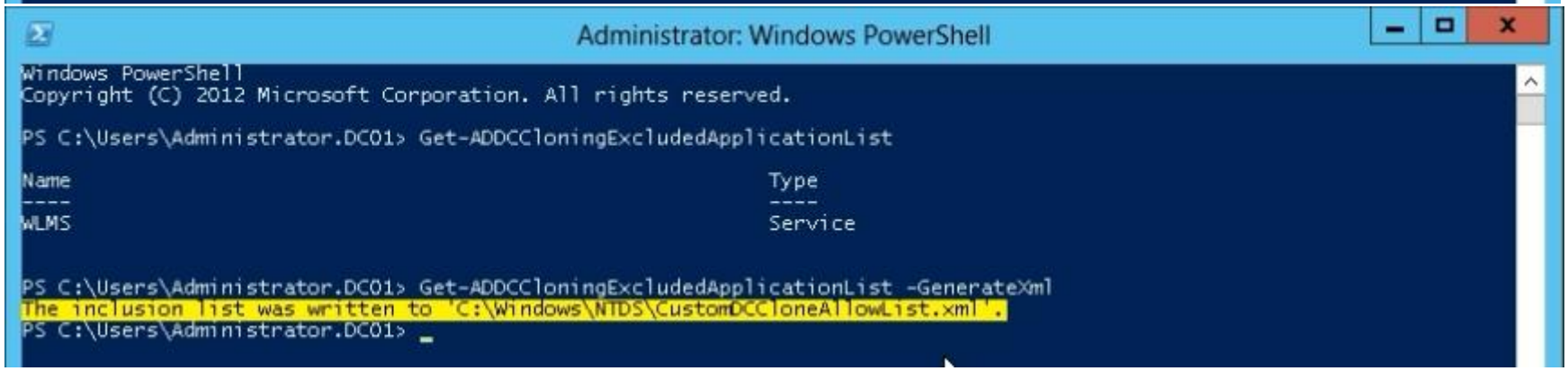
A. Create an empty file named CustomDCClonesAllowList.xml
B. Add the following information to the DCCloneConfigSchema.xsd
```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```
C. Create a filename DCCloneConfig.xml that contains the following information
```
<AllowList>
  <Allow>
    <Name>App1</Name>
    <Type>Service</Type>
  </Allow>
</AllowList>
```
D. Create a filename CustomDCCloneAllowList.xml that contains the following information
```
<AllowList>
  <Allow>
    <Name>App1</Name>
```

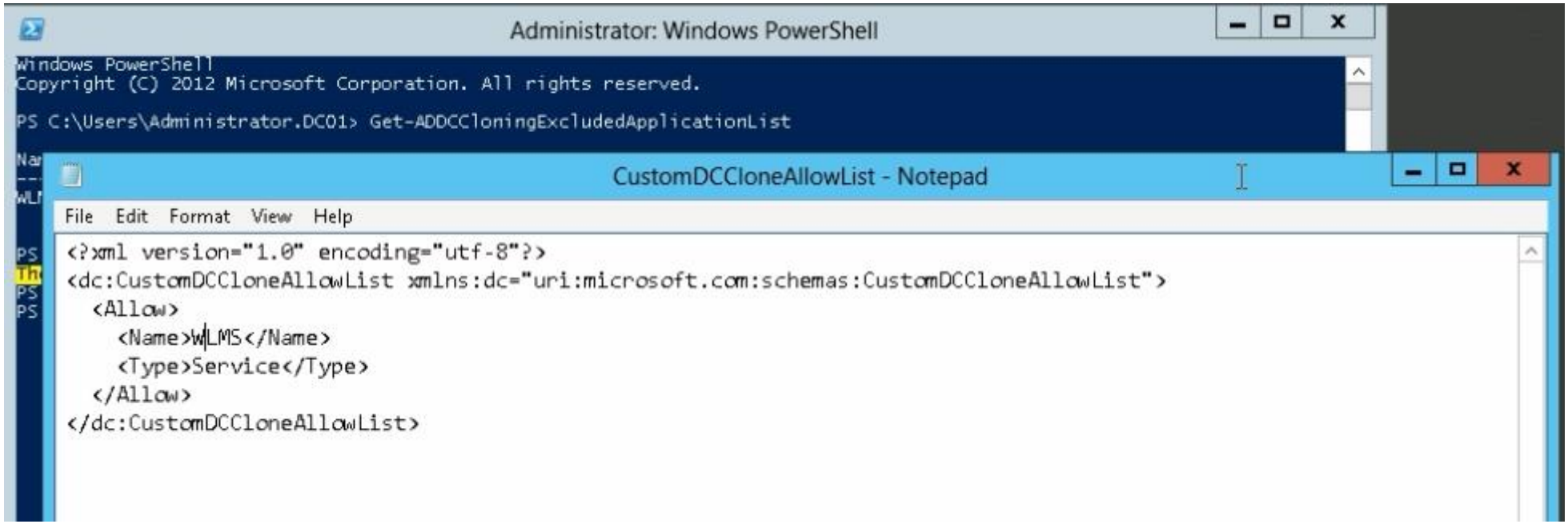
```
    <Type>Service</Type>
  </Allow>
</AllowList>
```

E. Create an empty file named DCCloneConfig.xml

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:





You can populate the XML file.....doesn't need to be empty.....

Administrator: Windows PowerShell

```
PS C:\Users\Administrator.DC01> New-ADDCCloneConfigFile -Static -IPv4Address 10.10.10.202 -IPv4DefaultGateway 10.10.10.1
 -IPv4SubnetMask 255.255.255.0 -IPv4DNSResolver 10.10.10.73,10.10.10.202 -CloneComputerName DC02 -SiteName Default-First
-Site-Name
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or late
r...
Passed: The domain controller hosting the PDC FSMO role (DC01.accusource.local) was located and running Windows Server 2
012 or later.

Verifying authorization: Checking if this domain controller is a member of the 'Cloneable Domain Controllers' group...
Located the local domain controller: (DC01.accusource.local).
Querying the 'Cloneable Domain Controllers' group...
Pass: The local domain controller is a member of the 'Cloneable Domain Controllers' group.

Starting test: Validating the cloning allow list.
NOTE: C:\Windows\NTDS\CustomDCCloneAllowList.xml is being used as the defined inclusion list.
No excluded applications were detected.
Pass: No excluded applications were detected.

No valid clone configuration files were found at any of the supported locations.

All preliminary validation checks passed.

Starting creation of the clone configuration file...
Finding the path to the Directory Service database...
The clone configuration file was generated at:
C:\Windows\NTDS\DCCloneConfig.xml
Generating the clone configuration file content...
The clone configuration file has been created.

PS C:\Users\Administrator.DC01>
```

DCCloneConfig - Notepad

File Edit Format View Help

```
<?xml version="1.0"?>
<d3c:DCCloneConfig xmlns:d3c="uri:microsoft.com:schemas:DCCloneConfig">
  <ComputerName>DC02</ComputerName>
  <SiteName>Default-First-Site-Name</SiteName>
  <IPSettings>
    <IPv4Settings>
      <StaticSettings>
        <Address>10.10.10.202</Address>
        <SubnetMask>255.255.255.0</SubnetMask>
        <DefaultGateway>10.10.10.1</DefaultGateway>
        <DNSResolver>10.10.10.73</DNSResolver>
        <DNSResolver>10.10.10.202</DNSResolver>
      </StaticSettings>
    </IPv4Settings>
  </IPSettings>
</d3c:DCCloneConfig>
```

Explanation:

D: Run Get-ADDCCloningExcludedApplicationList cmdlet In this procedure, run the Get-ADDCCloningExcludedApplicationList cmdlet on the source virtualized domain controller to identify any programs or services that are not evaluated for cloning. You need to run the Get-ADDCCloningExcludedApplicationList cmdlet before the New- ADDCCloneConfigFile cmdlet because if the New-ADDCCloneConfigFile cmdlet detects an excluded application, it will not create a DCCloneConfig.xml file. To identify applications or services that run on a source domain controller which have not been evaluated for cloning
Get-ADDCCloningExcludedApplicationList
Get-ADDCCloningExcludedApplicationList -GenerateXml

E: The clone domain controller will be located in the same site as the source domain controller unless a different site is specified in the DCCloneConfig.xml file.

Note:
* The Get-ADDCCloningExcludedApplicationList cmdlet searches the local domain controller for programs and services in the installed programs database, the services control manager that are not specified in the default and user defined inclusion list. The applications in the resulting list can be added to the user defined exclusion list if they are determined to support cloning. If the applications are not cloneable, they should be removed from the source domain controller before the

clone media is created. Any application that appears in cmdlet output and is not included in the user defined inclusion list will force cloning to fail.
* The Get-ADDCCloningExcludedApplicationList cmdlet needs to be run before the New- ADDCCloneConfigFile cmdlet is used because if the New-ADDCCloneConfigFile cmdlet detects an excluded application, it will not create a DCCloneConfig.xml file.
* DCCloneConfig.xml is an XML configuration file that contains all of the settings the cloned DC will take when it boots. This includes network settings, DNS, WINS, AD site name, new DC name and more. This file can be generated in a few different ways.

The New-ADDCCloneConfig cmdlet in PowerShell
By hand with an XML editor
By editing an existing config file, again with an XML editor (Notepad is not an XML editor.)

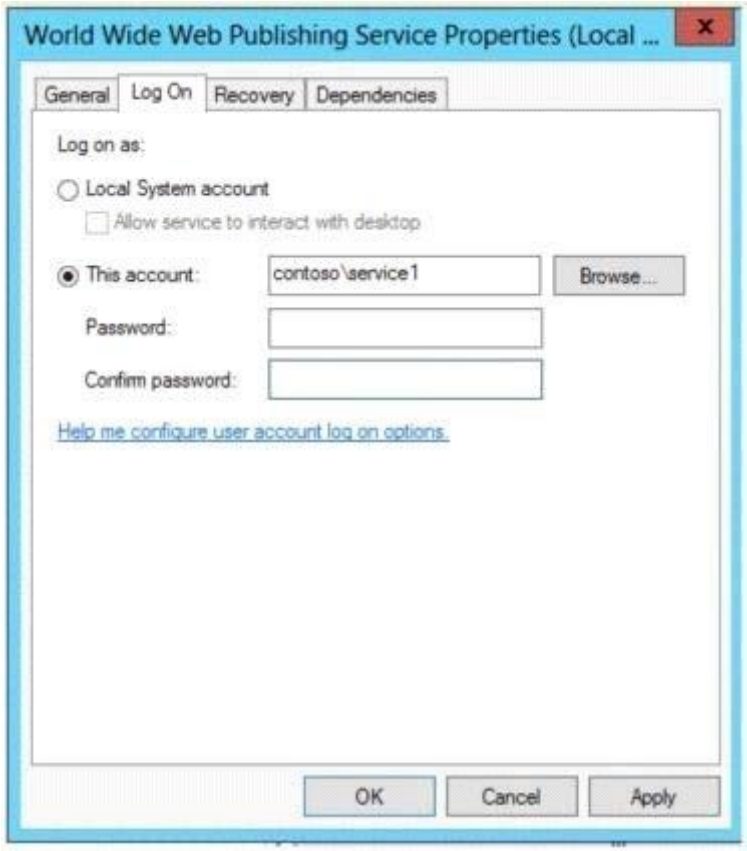
Reference: Introduction to Active Directory Domain Services (AD DS) Virtualization (Level 100)

See
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

QUESTION 140
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1.
Server1 has the Web Server (IIS) server role installed. On Server1, you install a managed service account named Service1.
You attempt to configure the World Wide Web Publishing Service as shown in the exhibit. (Click the Exhibit button.)
You receive the following error message: "The account name is invalid or does not exist, or the password is invalid for the account name specified."
You need to ensure that the World Wide Web Publishing Service can log on by using the managed service account.

What should you do?

Exhibit:



A. Specify contoso\service1$ as the account name.
B. Specify service1@contoso.com as the account name.
C. Reset the password for the account.
D. Enter and confirm the password for the account.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
On the Log On tab, set “This Account” to the domain\name$ of your MSA.

So if your MSA was called “**AskDS**” in the “contoso.com” domain, it would be: contoso**AskDS$**

http://blogs.technet.com/b/askds/archive/2009/09/10/managed-service-accounts-understanding-implementing-best-practices-and-troubleshooting.aspx

QUESTION 141
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.
You pre-create a read-only domain controller (RODC) account named RODC1.
You export the settings of RODC1 to a file named File1.txt. You need to promote RODC1 by using File1.txt.

Which tool should you use?

A. The Dcpromo command
B. The Install-WindowsFeature cmdlet
C. The Install-ADDSDomainController cmdlet
D. The Add-WindowsFeature cmdlet
E. The Dism command

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
http://technet.microsoft.com/en-us/library/dd378860%28v=ws.10%29.aspx

dcp - Notepad

File Edit Format View Help

```
; DCPROMO unattend file (automatically generated by dcpromo)
; Usage:
;   dcpromo.exe /CreateDCAccount /ReplicaDomainDNSName:home.local /unattend:C:\Users\Administrator\Desktop\dcp.txt
;
[DCInstall]
; Read-Only Replica DC promotion (stage 1)
DCAccountName=TESTE
; RODC Password Replication Policy
PasswordReplicationDenied="BUILTIN\Administrators"
PasswordReplicationDenied="BUILTIN\Server Operators"
PasswordReplicationDenied="BUILTIN\Backup Operators"
PasswordReplicationDenied="BUILTIN\Account Operators"
PasswordReplicationDenied="HOME\Denied RODC Password Replication Group"
PasswordReplicationAllowed="HOME\Allowed RODC Password Replication Group"
DelegatedAdmin="HOME\user1"
SiteName=Lisboa
InstallDNS=No
ConfirmGc=No
ReplicationSourceDC=DC1.home.local
```

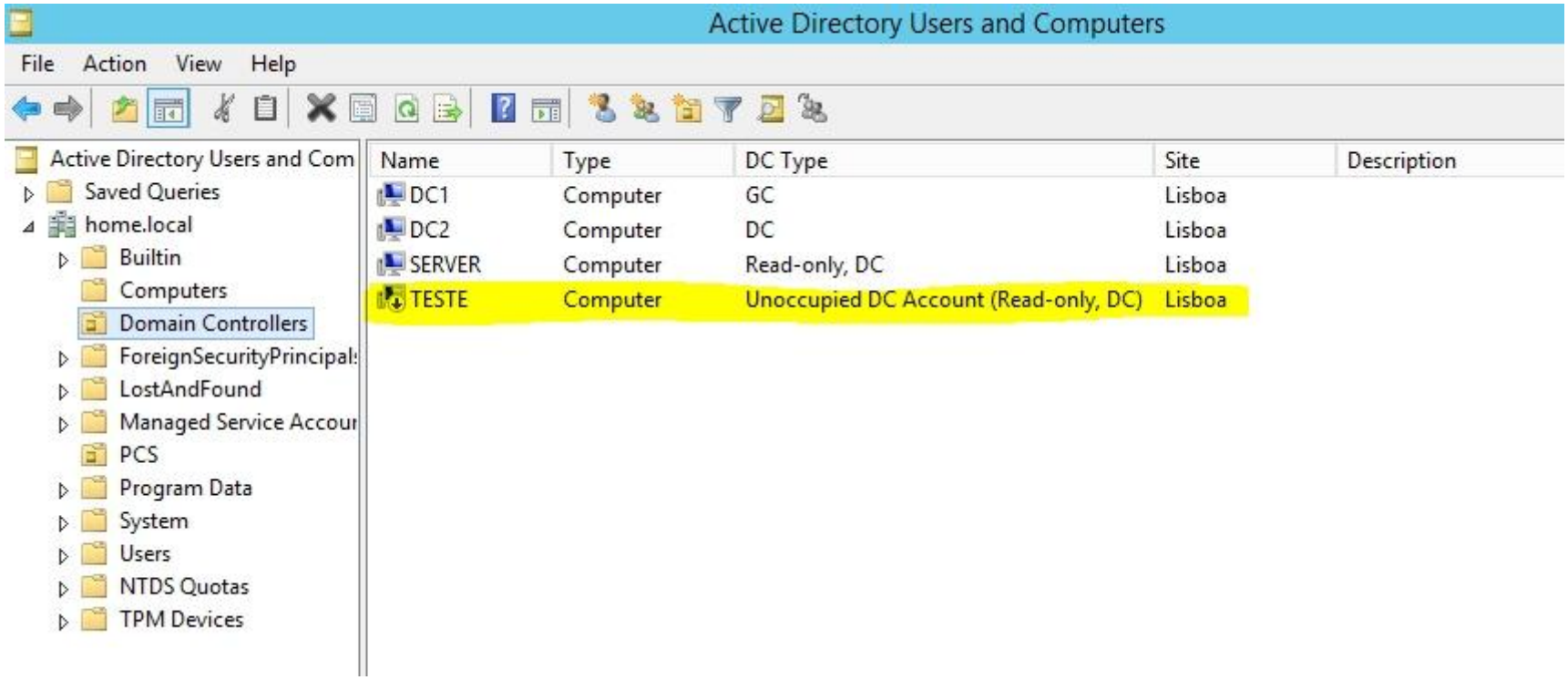
www.vceplus.com - Website designed to help IT pros advance their careers.

Administrator: Command Prompt

```
C:\Windows\system32>
C:\Windows\system32>dcpromo.exe /CreateDCAccount /ReplicaDomainDNSName:home.loca
l /unattend:C:\Users\Administrator\Desktop\dcp.txt
The dcpromo unattended operation is replaced by the ADDSDeployment module for Wi
ndows PowerShell. For more information, see http://go.microsoft.com/fwlink/?Link
Id=220924
Active Directory Domain Services Setup

Validating environment and parameters...
Windows Server 2012 R2 domain controllers have a default for the security settin
g named "Allow cryptography algorithms compatible with Windows NT 4.0" that prev
ents weaker cryptography algorithms when establishing security channel sessions.


For more information about this setting, see Knowledge Base article 942564 (http
://go.microsoft.com/fwlink/?LinkId=104751).

------------------------------------------
The following actions will be performed:
Create a computer account for a new read-only domain controller for the domain "
home.local".

Computer name: TESTE.home.local
Site: Lisboa

Additional Options:
  Read-only domain controller: "Yes"
  Global catalog: No
  DNS Server: No

Source DC: DC1.home.local

Password Replication Policy:
  Allow: HOME\Allowed RODC Password Replication Group
  Deny:  BUILTIN\Administrators
  Deny:  BUILTIN\Server Operators
  Deny:  BUILTIN\Backup Operators
  Deny:  BUILTIN\Account Operators
  Deny:  HOME\Denied RODC Password Replication Group

Delegation for RODC Installation and Administration:
HOME\user1


------------------------------------------


Starting...
.
You have successfully created an account for a read-only domain controller (RODC
). You will be able to attach the server that you want to be the RODC to this ac
count by running the Add Roles Wizard in Server Manager on that server.

An account for the read-only domain controller "TESTE" is now created in the dom
ain "home.local".

The domain controller account is assigned to the site "Lisboa". You can manage s
```

Activate
Go to Sys
activate W

eers.



http://technet.microsoft.com/en-us/library/cc732887.aspx
http://technet.microsoft.com/en-us/library/jj574152.aspx

QUESTION 142
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2008 R2.
The domain contains three servers that run Windows Server 2012.
The servers are configured as shown in the following table.

Server name	Configuration
Server1	Web Server (IIS) server role
Server2	Web Server (IIS) server role
Server3	Microsoft SQL Server

Server1 and Server2 are configured in a Network Load Balancing (NLB) cluster. The NLB cluster hosts a website named Web1 that uses an application pool named App1.
Web1 uses a database named DB1 as its data store. You create an account named User1. You configure User1, as the identity of App1.
You need to ensure that contoso.com domain users accessing Web1 connect to DB1 by using their own credentials.

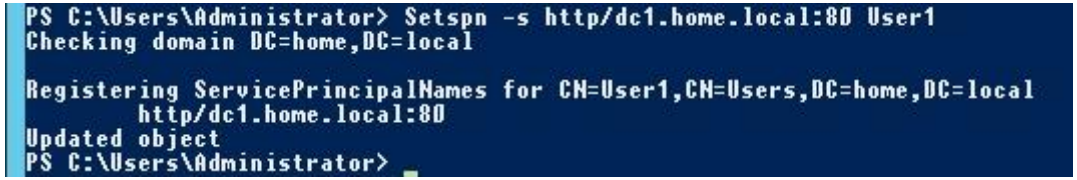
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

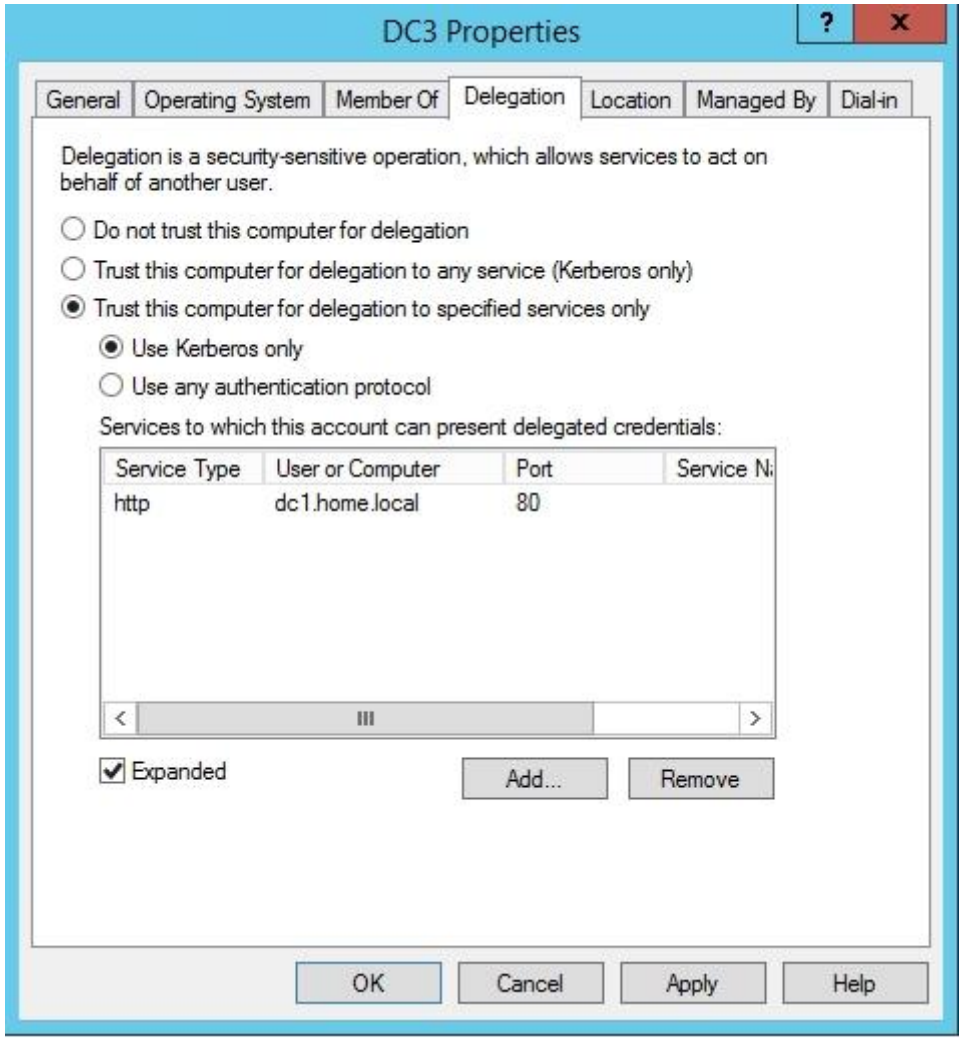
A. Configure the delegation settings of Server3.
B. Create a Service Principal Name (SPN) for User1.
C. Configure the delegation settings of User1.
D. Create a matching Service Principal Name (SPN) for Server1 and Server2.
E. Configure the delegation settings of Server1 and Server2.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
To create a service principal name
Open an elevated command prompt. Click **Start**, and in the search window, type **Command Prompt**.
Right-click **Command Prompt**, and then click **Run as administrator**.
At the command prompt, create the SPN. The syntax is:

setspn -S InstanceName/FullyQualifiedDomainNameOfServer:Port Domain \User





If your version of setspn.exe does not recognize -S, retry the command (windows 2008!) using -A. See Walkthrough: Installing the Three Tiers on Three Computers for an example of how to create SPNs when deploying Microsoft Dynamics NAV.

Delegating Access to the SQL Server Service

Configuring delegation means explicitly configuring the Microsoft Dynamics NAV Server service to delegate its access to the database server on behalf of the RoleTailored client. To make the access more secure, you specify delegation to a specific service on a specific server.

To delegate access to the SQL Server service

On any server computer in the domain, click **Start**, and then click **Run**.
In the **Open** field, type **dsa.msc**.
This opens the Active Directory Users and Computers utility.
To configure delegation, the functional level for the domain must be Windows Server 2003 or higher. To verify the domain functional level, right-click the node for the domain where you have installed Microsoft Dynamics NAV, and then click **Raise Domain Functional Level**. If the level is not at least Windows Server 2003, then raise it to that level.
Right-click the node for the domain where you have installed Microsoft Dynamics NAV, and then click **Find**.
In the **Find Users, Contacts, and Group** dialog box, type the name of the domain user in the **Name** field, and then press ENTER.
In the **Search results** area, right-click the domain user, and then click **Properties**.
On the **Delegation** tab, click **Trust this user for delegation to specified services only**, and then click **Use Kerberos only**.
Click **Add** to open the **Add Services** dialog box.
In the **Add Services** window, click **Users or Computers**, and then type the name of the domain user.
In the list of services for the domain user, click **MSSQLSvc**, which is the name of the SQL Server service.
Click **OK** to exit the **Add Services** dialog box.
Click **OK** to close all open dialog boxes.

http://msdn.microsoft.com/en-us/library/dd568720.aspx
http://www.iis.net/learn/manage/configuring-security/application-pool-identities

QUESTION 143
Your network contains an Active Directory domain named contoso.com. Domain controllers run either Windows Server 2003, Windows Server 2008 R2, or Windows Server 2012.
A support technician accidentally deletes a user account named User1.
You need to use tombstone reanimation to restore the User1 account.

Which tool should you use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Tombstone reanimation for Active Directory was **introduced in Windows Server 2003.**
This feature takes advantage of the fact that Active Directory keeps deleted objects in the database for a period of time before physically removing them.
use Ldp.exe to restore a single, deleted Active Directory object
http://www.petri.co.il/manually-undeleting-objects-windows-active-directory-ad.htm

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

QUESTION 144
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC4 that runs Windows Server 2012.
You create a DCCloneConfig.xml file.
You need to clone DC4.

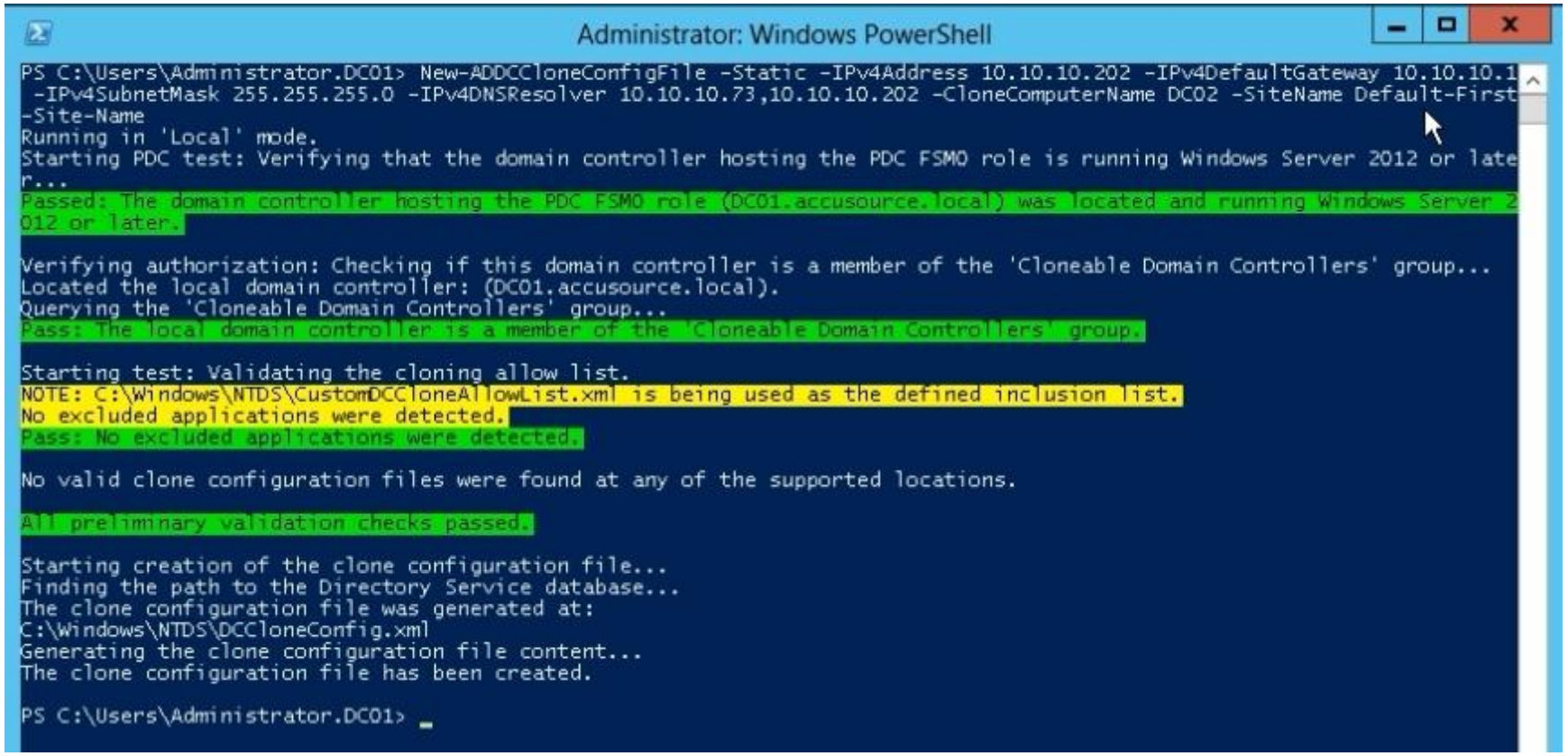
Where should you place DCCloneConfig.xml on DC4?

A. %Systemroot%\SYSVOL
B. %Programdata%\Microsoft
C. %Systemroot%\NTDS
D. %Systemdrive%

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
http://blogs.technet.com/b/askpfeplat/archive/2012/10/01/virtual-domain-controller-cloning-in-windows-server-2012.aspx

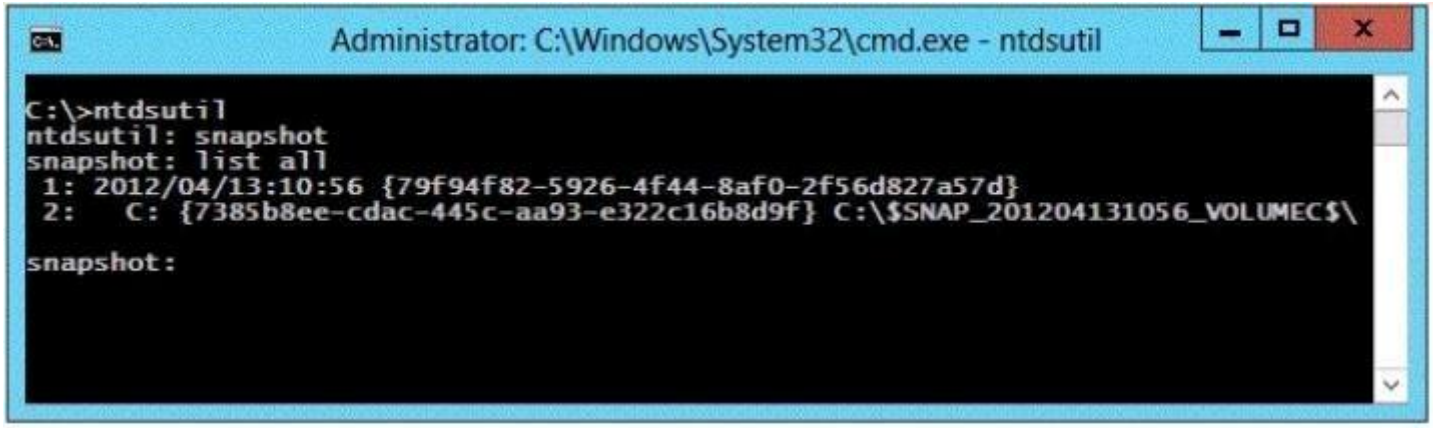
As the output shows, the XML file is written to c:\windows\ntds. That's one of **three** valid locations where the file can be placed for cloning. All three locations are:
%windir%\NTDS
Wherever the DIT lives (if you've changed the path to D:\NTDS, for example)
The root of any removable media.



QUESTION 145
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1. You run ntdsutil {as shown in the exhibit}.
You need to ensure that you can access the contents of the mounted snapshot.

What should you do?

Exhibit:



A. From a command prompt, run dsamain.exe -dbpath c:\$snap_201204131056_volumec$\windows\ntds\ntds.dit - Idapport 33389.
B. From a command prompt, run dsamain.exe -dbpath c:\$snap_201204131056_volumec$\windows\ntds\ntds.dit - Idapport 389.
C. From the snapshot context of ntdsutil, run activate instance "NTDS".
D. From the snapshot context of ntdsutil, run mount (79f94f82-5926-4f44-8af0-2f56d827a57d).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Administrator: Command Prompt - dsamain -dbpath c:\$SNAP_201212101208_...

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

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

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

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

snapshot: mount {062d937f-9cdd-4286-8938-9c29ce83c8a6}
Snapshot {d41683c7-ae91-48fc-a639-1e9b82138bf4} mounted as C:\$SNAP_201212101208
_VOLUMEC$\
snapshot: quit
ntdsutil: quit

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



Current value of VM Generation ID: 6680128214492828164

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



msDS-GenerationId attribute value:
6680128214492828164

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

eers.

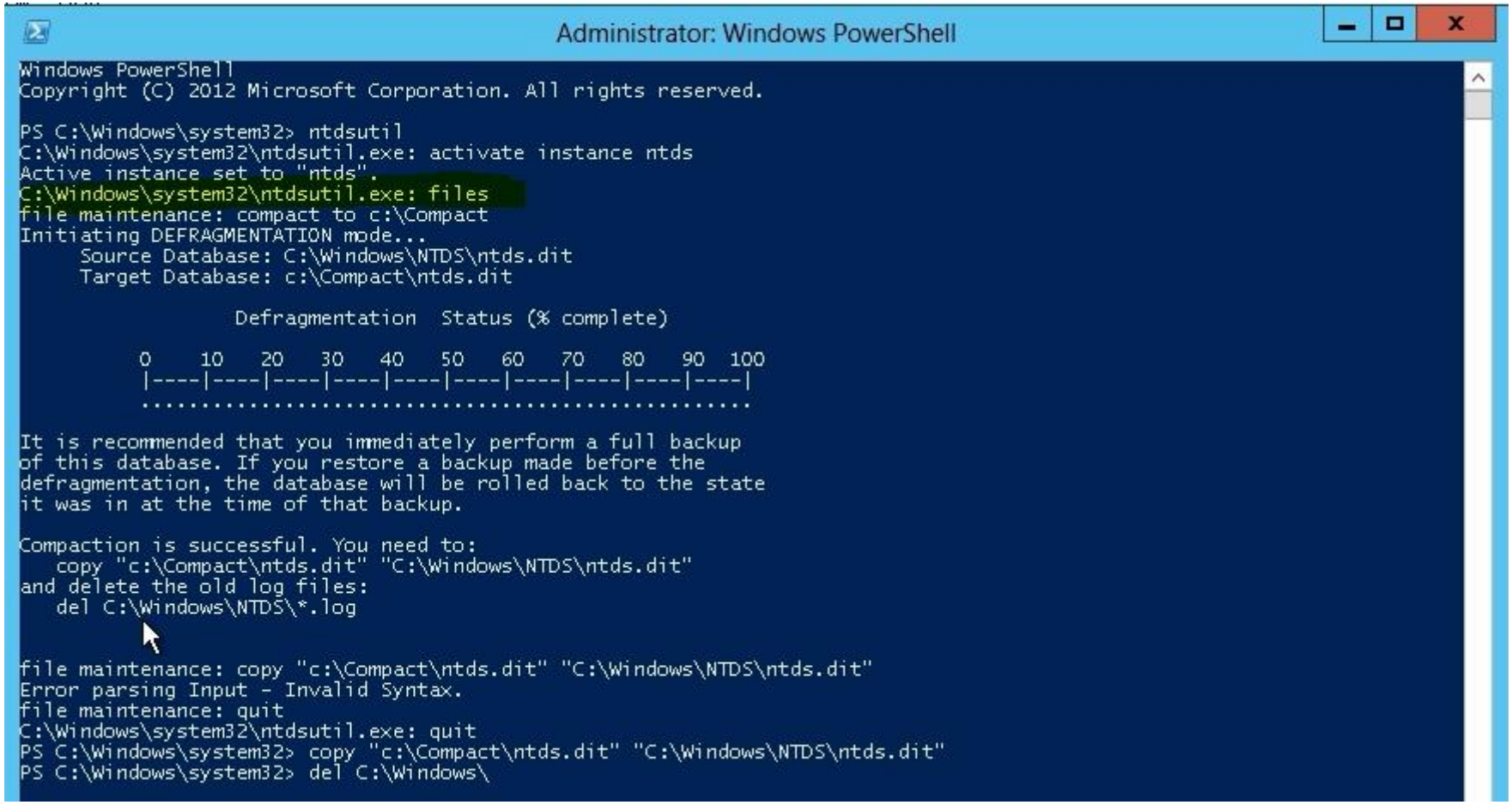
QUESTION 146
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1.
On DC1, you add a new volume and you stop the Active Directory Domain Services (AD DS) service.
You run ntdsutil.exe and you set NTDS as the active instance.
You need to move the Active Directory database to the new volume.

Which Ntdsutil context should you use?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:



http://support.microsoft.com/kb/257420/en-us

QUESTION 147
Your network contains an Active Directory domain named contoso.com. You create a user account named User1.
The properties of User1 are shown in the exhibit. (Click the Exhibit button.)
You plan to use the User1 account as a service account. The service will forward authentication requests to other servers.
You need to ensure that you can view the Delegation tab from the properties of the User1 account.

What should you do first?

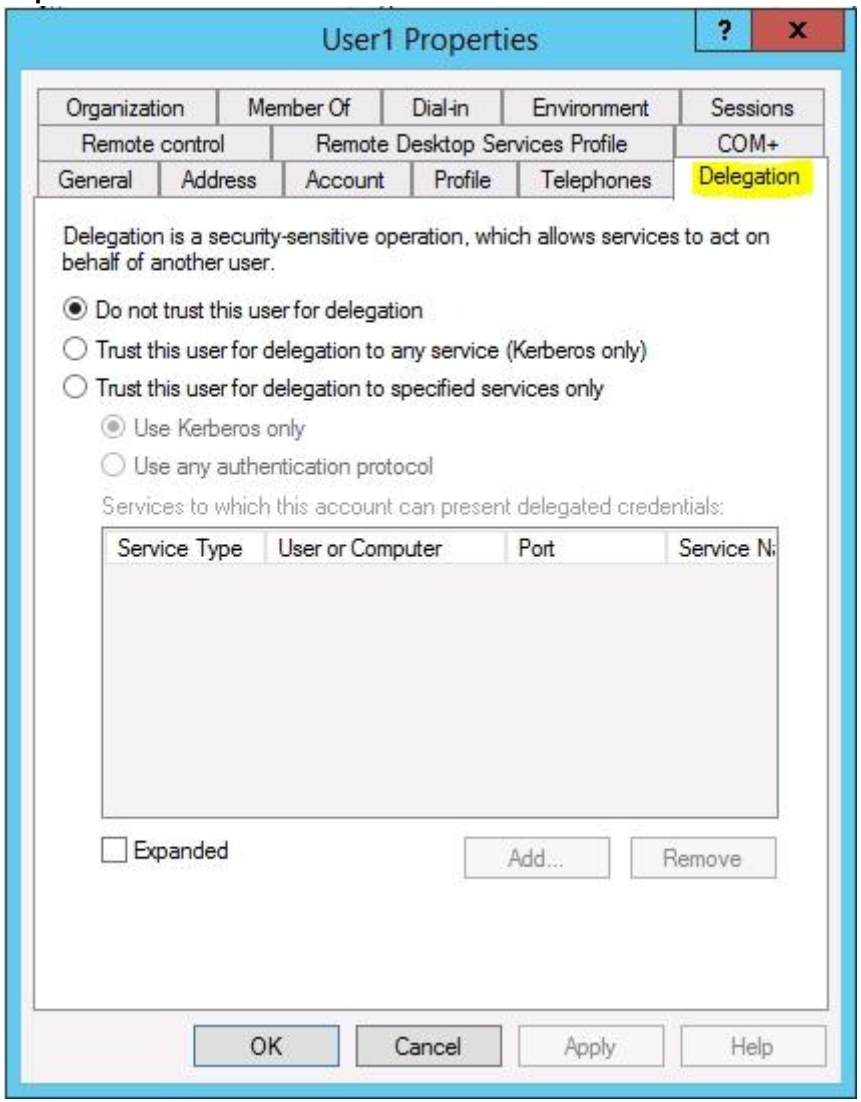
Exhibit:

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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:



http://blogs.msdn.com/b/mattlind/archive/2010/01/14/delegation-tab-in-aduc-not-available-until-a-spn-is-set.aspx

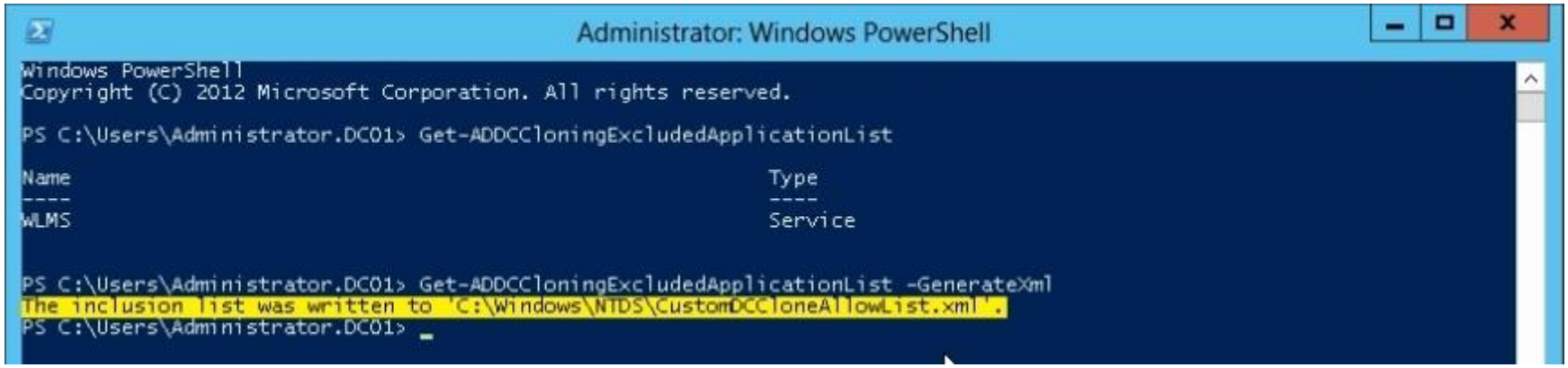
QUESTION 148
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012. On all of the domain controllers, Windows is installed in C:\Windows and the Active Directory database is located in D:\Windows\NTDS\.
All of the domain controllers have a 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 D:\Windows\NTDS\, create an XML file named CustomDCCloneAllowList.xml and add the application information to the file.
C. In the root of a USB flash drive, add the application information to an XML file named DefaultDCCloneAllowList.xml.
D. In D:\Windows\NTDS, create an XML file named DefaultDCCloneAllowList.xml and add the application information to the file.

Correct Answer: B
Section: (none)
Explanation

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



QUESTION 149
Your network contains an Active Directory domain named adatum.com. The domain contains a domain controller named DC1. On DC1, you create a new volume named E.
You restart DC1 in Directory Service Restore Mode. You open ntdsutil.exe and you set NTDS as the active instance.
You need to move the Active Directory logs to E:\NTDS\.

Which Ntdsutil context should you use?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
How to Move Log Files

Use the move logs to command to move the directory service log files to another folder. For the new settings to take effect, restart the computer after you move the log files.
To move the log files, follow these steps:
- Click Start, click Run, type **ntdsutil** in the Open box, and then press ENTER.
- At the **Ntdsutil** command prompt, type **files**, and then press ENTER.
- At the file maintenance command prompt, type **move logs to new location** (where new location is an existing folder that you have created for this purpose), and then press ENTER.
- Type **quit**, and then press ENTER.
- Restart the computer.

http://support.microsoft.com/kb/257420/en-us
http://support.microsoft.com/kb/816120#5

QUESTION 150
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1.
Server1 runs Windows Server 2012 and has the Hyper-V server role installed.
Server1 hosts 10 virtual machines. A virtual machine named VM1 runs Windows Server 2012 and hosts a processor-intensive application names App1.
Users report that App1 responds more slowly than expected.
You need to monitor the processor usage on VM1 to identify whether changes must be made to the hardware settings of VM1.

Which performance object should you monitor on Server1?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Traditionally, processor performance can be measured using the “\Processor(*)\% Processor Time” performance monitor counter. This is not an accurate counter for evaluating processor utilization of a guest operating system though because Hyper-V measures and reports this value relative to the number of processors allocated to the virtual machine.
Hyper-V provides hypervisor performance objects to monitor the performance of both logical and virtual processors.

To accurately measure the processor utilization of a guest operating system, use the “\Hyper-V Hypervisor Logical Processor(_Total)\% Total Run Time” performance monitor counter on the Hyper-V host operating system. Use the following thresholds to evaluate guest operating system processor utilization using the “\Hyper-V Hypervisor Logical Processor(_Total)\% Total Run Time” performance monitor counter:

Less than 60% consumed = Healthy
60% - 89% consumed = Monitor or Caution
90% - 100% consumed = Critical, performance will be adversely affected

To troubleshoot processor performance of guest operating systems on a Hyper-V environment, it is best to strive for a balance between the values reported by the host operating system for “\Hyper-V Hypervisor Logical Processor(_Total)\% Total Run Time” (LPTR) and “\Hyper-V Hypervisor Virtual Processor(_Total)\% Total Run Time” (VPTR). If LPTR is high and VPTR is low then verify that there are not more processors allocated to virtual machines than are physically available on the physical computer.

http://msdn.microsoft.com/en-us/library/cc768535(v=bts.10).aspx
http://windowsitpro.com/blog/perfmon-hyper-v-hypervisor-virtual-processor-versus-hyper-v-hypervisor-logical-processor

QUESTION 151
You have a RODC named Server1 running Server 2012 .

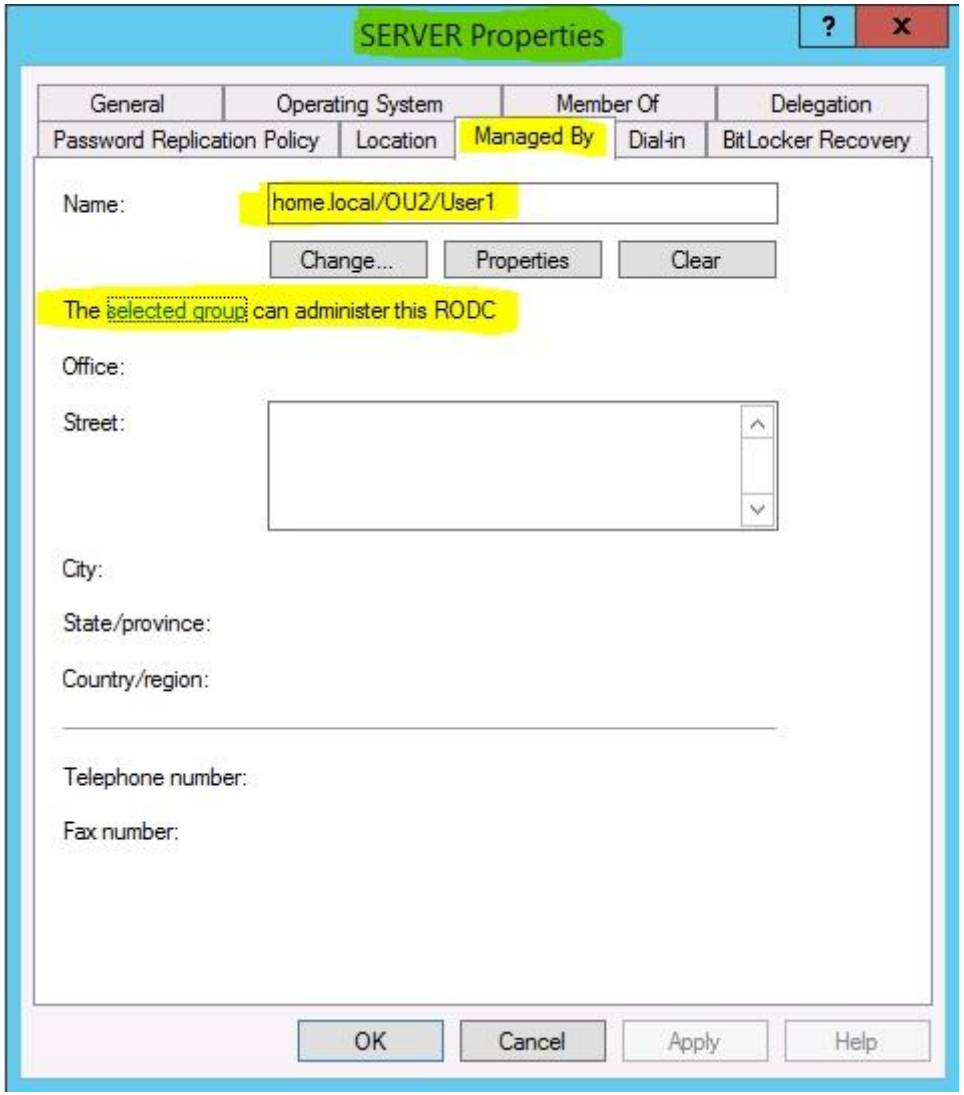
You need to add a RODC Administrator.

How do you complete the task?

A. dsmgmt.exe
B. ntdsutil
C. Add user to Local Administrator Group on Server1
D. Use Security Group and modify RODC Delegated Administrator

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
D. Using ntdsutil or dsmgmt to specify the delegated RODC administrator account is not recommended because the information is stored only locally on the RODC. You can only specify one security principal to be the delegated RODC administrator. As a best practice, you should create a security group for each RODC and assign that group to be the delegated administrator. Then, you can add individual user accounts to the group, and each user can manage the RODC.



http://windowsitpro.com/security/q-how-can-i-delegate-administrator-role-given-rodc-single-administrator-account
http://technet.microsoft.com/en-us/library/cc755310(v=ws.10).aspx

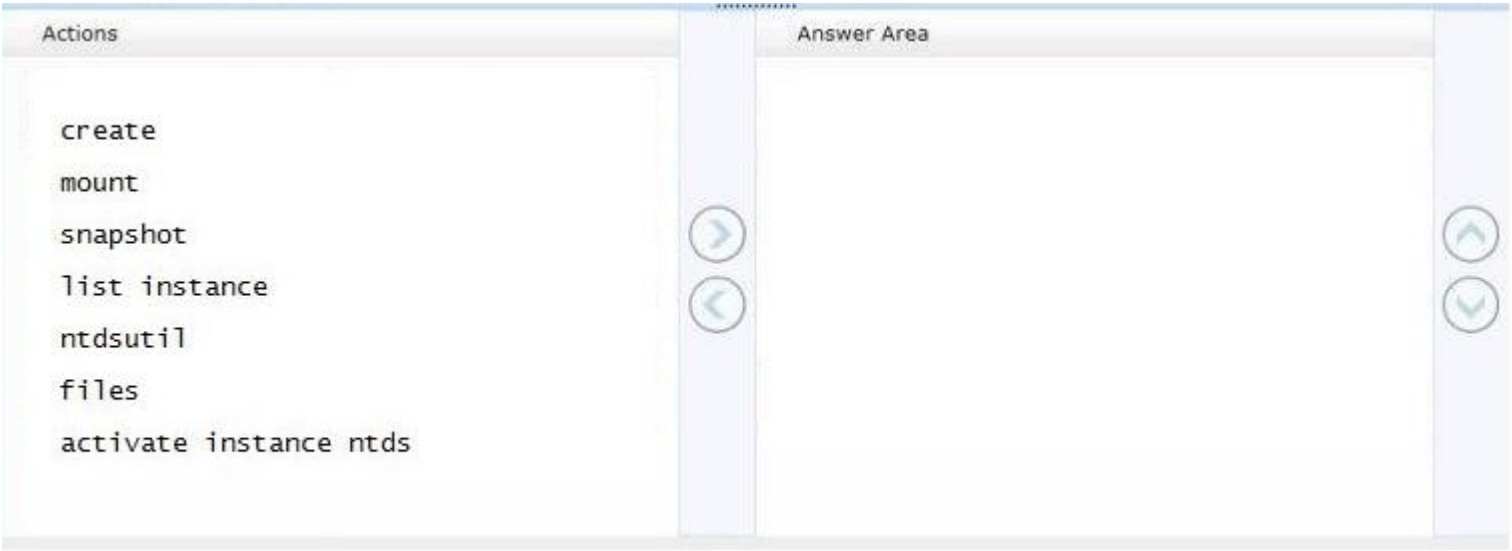
QUESTION 152

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

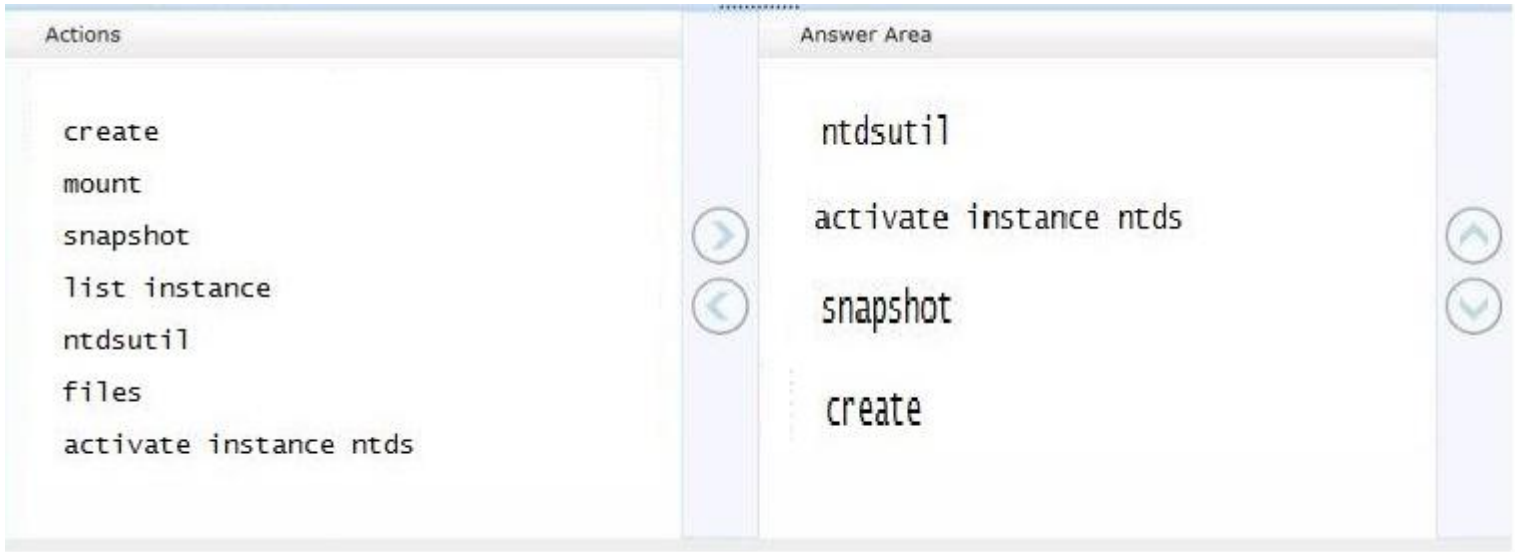
You need to create a AD Snapshot

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

Select and Place:

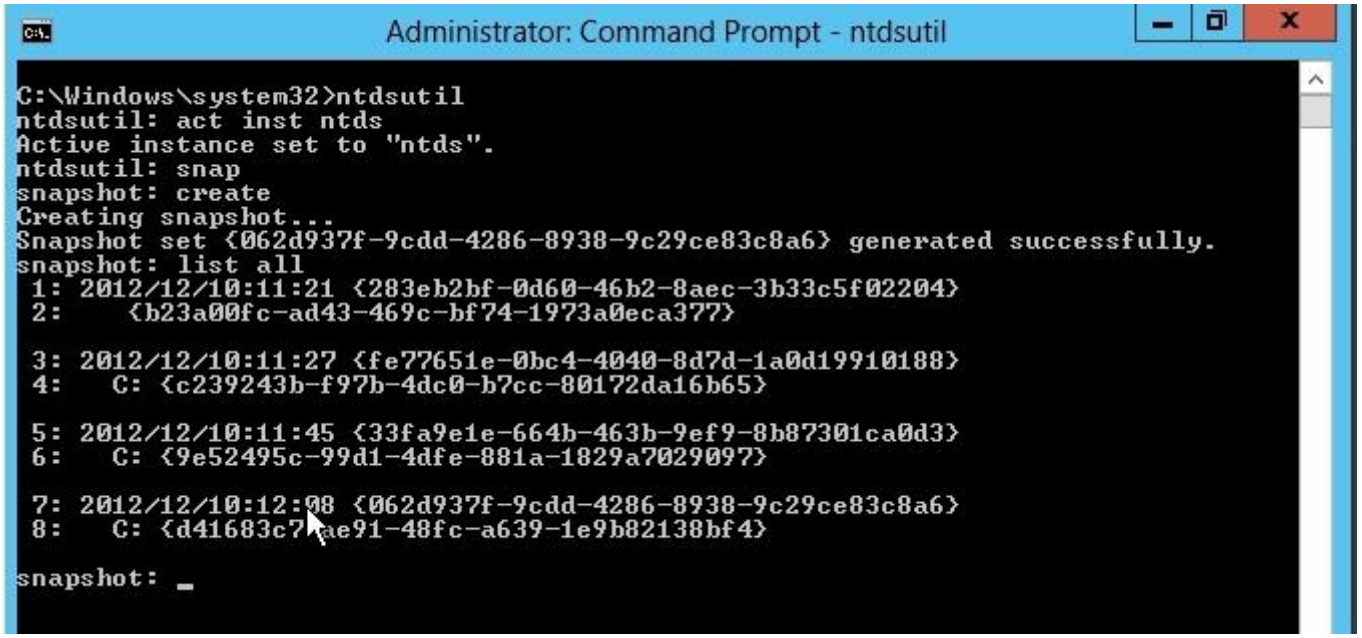


Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Before you can run the snapshot subcommand, you must run the activate instance subcommand in NTDSUTIL to set an active instance.



http://www.petri.co.il/working-active-directory-snapshots-windows-server-2008.htm#
Creating an Active Directory snapshot

In order to create an Active Directory snapshot you need to use the NTDSUTIL command. NTDSUTIL is built into Windows Server 2008. It is available if you have the Active Directory Domain Services (AD DS) server role or the AD LDS server role installed.

Please follow these steps:

Log on as a member of the Domain Admins group to one of your Windows Server 2008 Domain Controllers.
Open a Command Prompt window by clicking on the CMD shortcut in the Start menu, or by typing CMD and pressing Enter in the Run or Quick Search parts of the Start menu.

Note: You ***must run NTDSUTIL from an elevated command prompt***. To open an elevated command prompt, click Start, right-click Command Prompt, and then click Run as administrator.
In the CMD window, type the following command:
ntdsutil

In the CMD window, type the following command:
snapshot

Note: NTDSUTIL uses nested menu commands that you type one after the other. You can type "?" at any time to get the different command options at any menu

level. Also note that you can usually type in the first few letters of each command. For example, instead of typing "snapshots" you can simply type "sna".

In the CMD window, type the following command:
activate instance ntds

Before you can run the snapshot subcommand, you must run the activate instance subcommand in NTDSUTIL to set an active instance.

In the CMD window, type the following command:
activate instance ntds

The result should look like this:
snapshot: Activate Instance ntds
Active instance set to "ntds".

In the CMD window, type the following command:
create

The result should look like this:

snapshot: create
Creating snapshot...
Snapshot set {3a861a35-2f33-4d7a-8861-a10e47afdaba} generated successfully.

To view all available snapshots, in the CMD window, type the following command:
list all

The result should look like this:

snapshot: create
snapshot: List All
1: 2008/10/25:03:14 {ec53ad62-8312-426f-8ad4-d47768351c9a}
2: C: {15c6f880-cc5c-483b-86cf-8dc2d3449348}

Next, you can leave the NTDSUTIL running, or you can quit by typing quit 2 times.

Note: NTDSUTIL allows you to run the above commands in one line. Run the following command:

ntdsutil "Activate Instance NTDS" snapshot create quit quit

You can easily automate this process. Read my "Automating the Creation of Active Directory Snapshots" article for more info.

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

QUESTION 153
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.
Contoso.com contains two servers. The servers are configured as shown in the following table.

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

Server 1 and Server2 host a load-balanced application pool named AppPool1.
You need to ensure that AppPool1 uses a group Manged Service Account as its identity.
Which 3 actions should you perform?

Select and Place:

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

Correct Answer:

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

Section: (none)
Explanation

Explanation/Reference:
New-ADServiceAccount
Creates a new Active Directory service account.

```
New-ADServiceAccount service1 -ServicePrincipalNames "MSSQLSVC/Machine3.corp.contoso.com"
```

Standalone Managed Service Accounts, which were introduced in Windows Server 2008 R2 and Windows 7, are managed domain accounts that provide automatic password management and simplified SPN management, including delegation of management to other administrators.

The group Managed Service Account provides the same functionality within the domain but also extends that functionality over multiple servers. When connecting to a service hosted on a server farm, such as Network Load Balance, the authentication protocols supporting mutual authentication require that all instances of the services use the same principal. When group Managed Service Account are used as service principals, the Windows operating system manages the password for

the account instead of relying on the administrator to manage the password.

The Microsoft Key Distribution Service (kdssvc.dll) provides the mechanism to securely obtain the latest key or a specific key with a key identifier for an Active Directory account. **This service is new to Windows Server 2012 and does not run on previous versions of the Windows Server operating system.** The Key Distribution Service shares a secret which is used to create keys for the account. These keys are periodically changed. For a group Managed Service Account the Windows Server 2012 domain controller computes the password on the key provided by the Key Distribution Services in addition to other attributes of the group Managed Service Account. Windows Server 2012 and Windows 8 member hosts can obtain the current and preceding password values by contacting a Windows Server 2012 domain controller.

http://technet.microsoft.com/en-us/library/hh831782.aspx
http://technet.microsoft.com/en-us/library/jj128431.aspx

"You can create a gMSA only if the forest schema has been updated to Windows Server 2012, the master root key for Active Directory has been deployed, and there is at least one Windows Server 2012 DC in the domain in which the gMSA will be created.")

QUESTION 154
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012. The domain contains two domain controllers. The domain controllers are configured as shown in the following table.

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

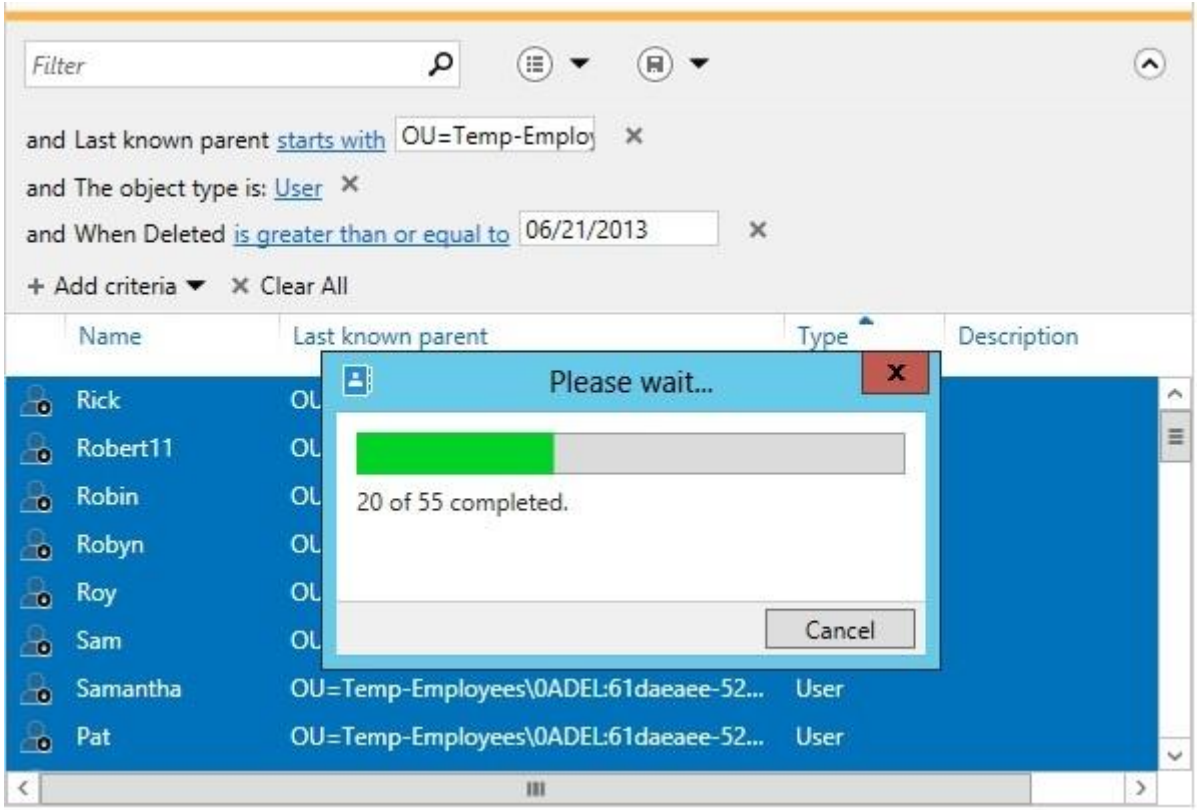
Active Directory Recycle Bin is enabled.
You discover that a support technician accidentally removed 100 users from an Active Directory group named Group1 an hour ago.
What should you do?

A. Perform a non-authoritative restore.
B. Modify the is Recycled attribute of Group1.
C. Perform an authoritative restore.
D. Recover the items by using Active Directory Recycle Bin.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
All deleted AD object information including attributes, passwords and group membership can be selected in mass then undeleted from the user interface instantly or via Powershell
Need to know what objects were deleted so you can filter for them or a specific time period

- You could undelete all objects during a specific time period but if you have multiple location where admins are making changes to AD, an intentional change may have occurred which you may not be aware of at the time. It is possible that users were terminated during the same time as the accidental deletions so you want to be cautious to not accidently undelete a terminated employee for security reasons.



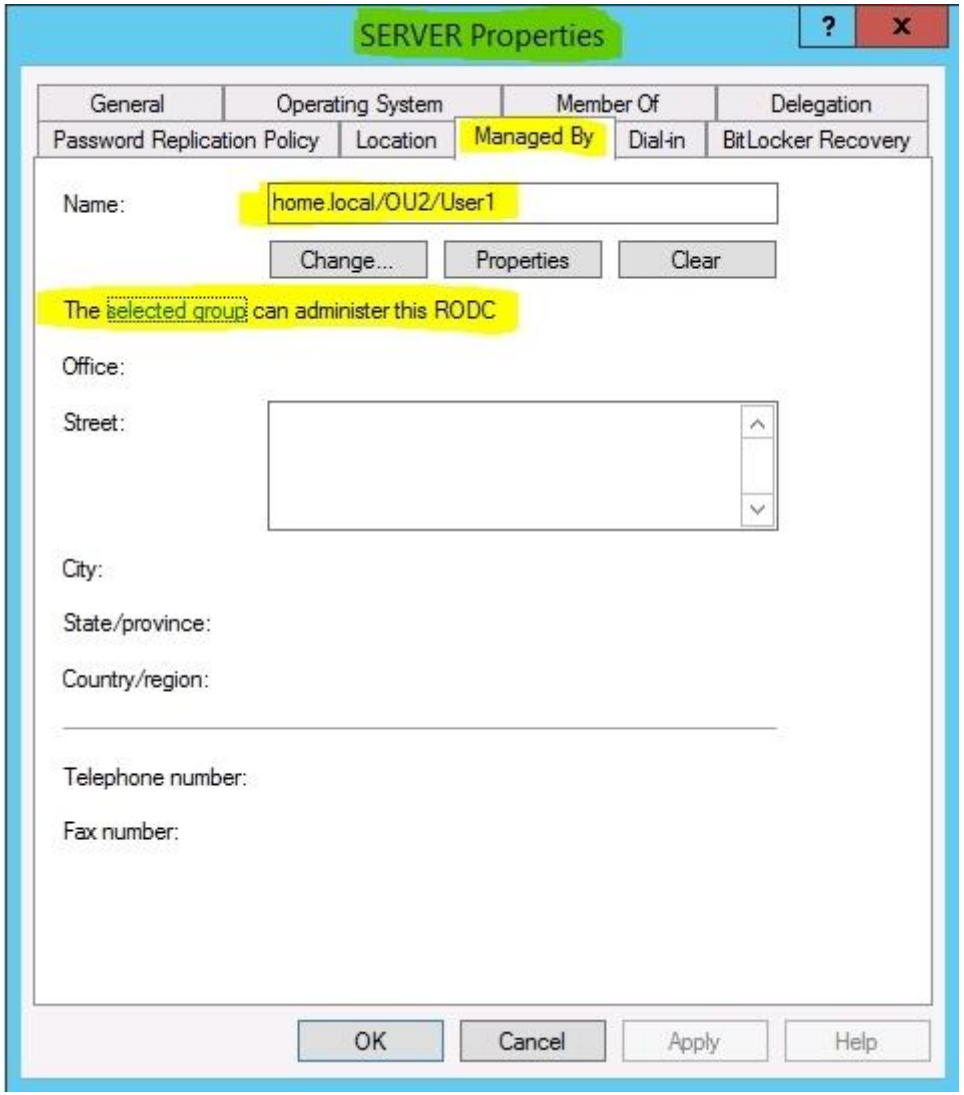
http://technet.microsoft.com/en-us/library/ff625687(v=ws.10).aspx)
http://windowsitpro.com/active-directory/windows-server-2012-active-directory-recycle-bin
http://communities.quest.com/community/quest-itexpert/blog/2012/09/24/the-windows-server-2012-recycle-bin-and-recovery-manager-for-active-directory

QUESTION 155
Your network contains an Active Directory domain named contoso.com. The domain contains a read-only domain controller (RODC) named RODC1.
You create a global group named RODC_Admins.
You need to provide the members of RODC_Admins with the ability to manage the hardware and the software on RODC1. The solution must not provide RODC_Admins with the ability to manage Active Directory objects.
What should you do?

A. From Active Directory Users and Computers, configure the Managed By settings of the RODC1 account.
B. From Active Directory Sites and Services, run the Delegation of Control Wizard
C. From Active Directory Users and Computers, run the Delegation of Control Wizard.
D. From a command prompt, run the dsadd computer command.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



http://technet.microsoft.com/en-us/library/cc755310%28v=ws.10%29.aspx

QUESTION 156

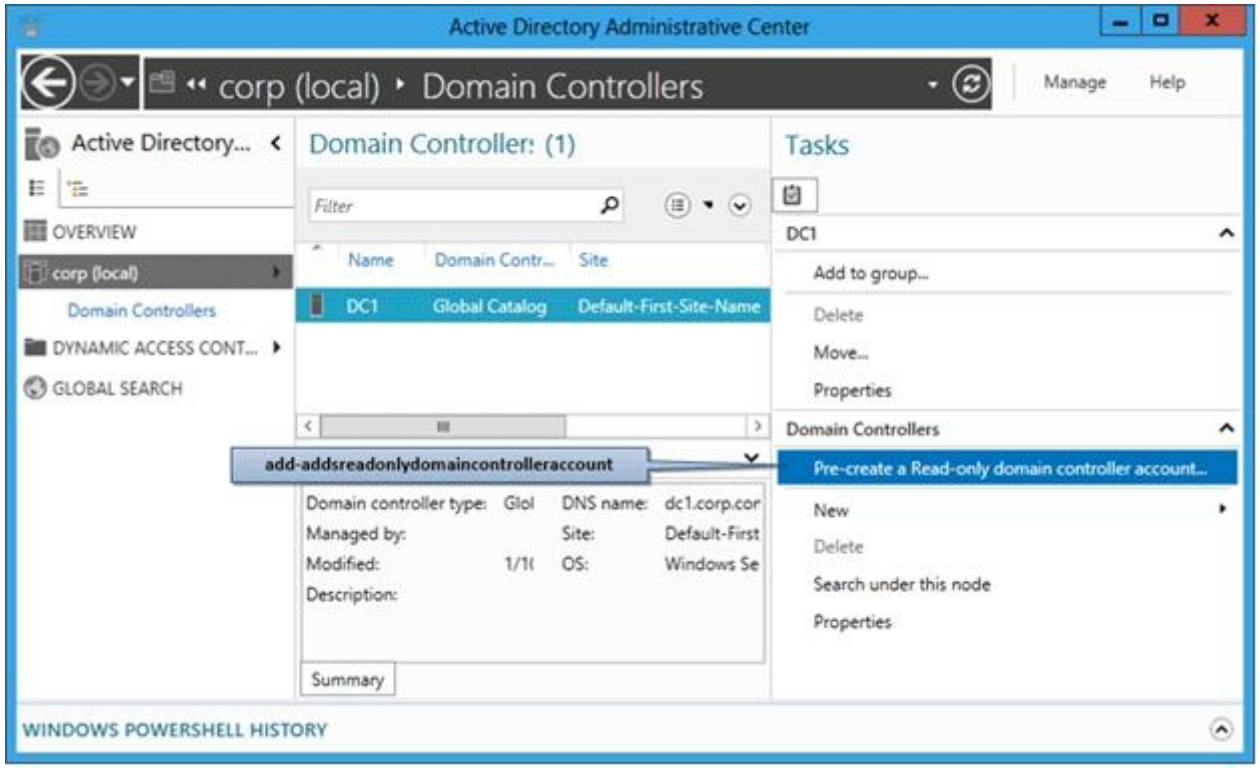
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.
In a remote site, a support technician installs a server named DC10 that runs Windows Server 2012. DC10 is currently a member of a workgroup.

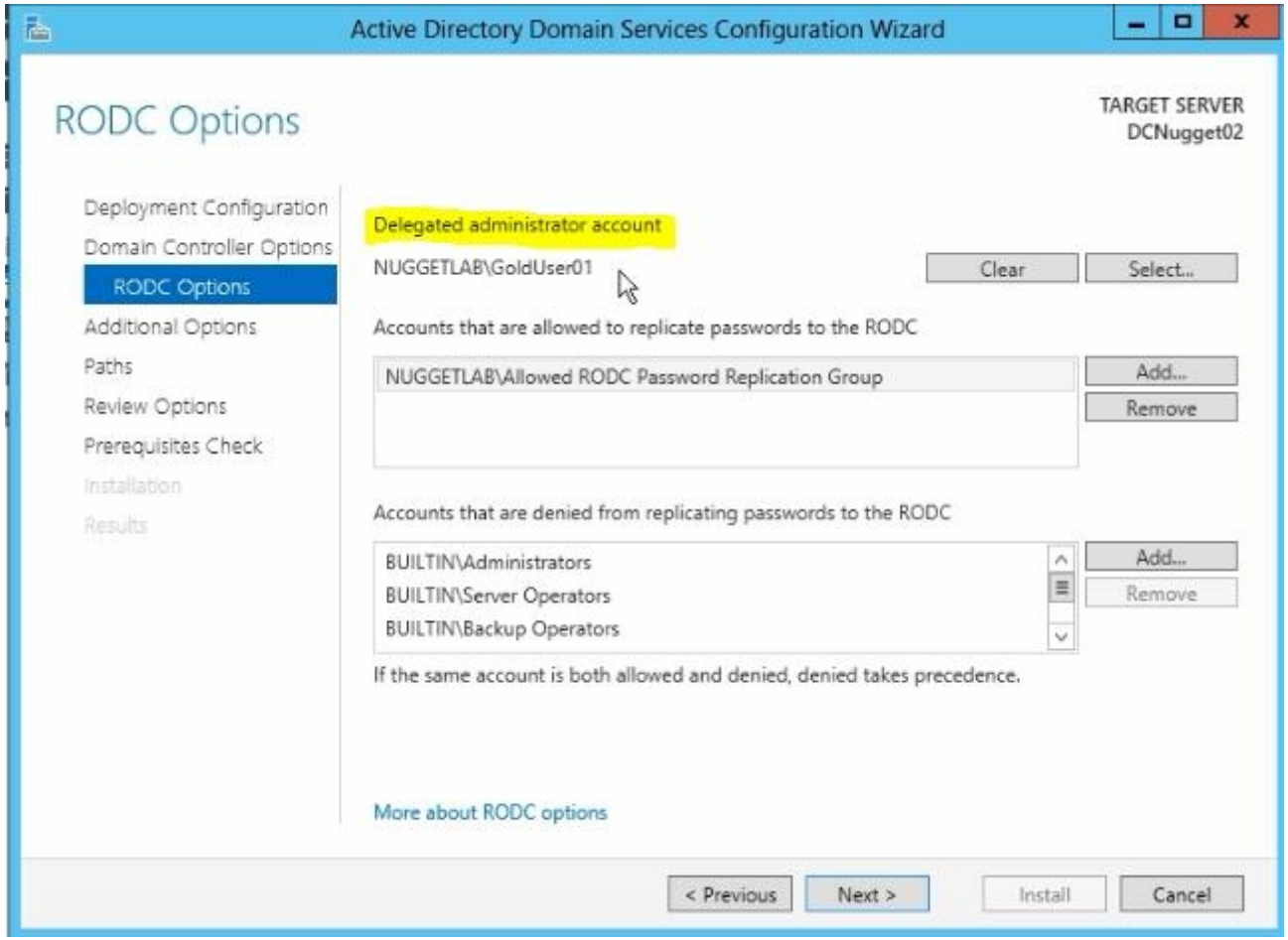
You plan to promote DC10 to a read-only domain controller (RODC).
You need to ensure that a user named Contoso/User1 can promote DC10 to a RODC in the contoso.com domain. The solution must minimize the number of permissions assigned to User1.
What should you do?

A. Join DC10 to the domain. Modify the properties of the DC10 computer account
B. From Active Directory Administrative Center, pre-create an RODC computer account.
C. Join DC10 to the domain. Run dsmod and specify the /server switch
D. From Active Directory Administrative Center, modify the security settings of the Domain Controllers organizational unit (OU).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
A staged read only domain controller (RODC) installation works in two discrete phases:
1. Staging an unoccupied computer account
2. Attaching an RODC to that account during promotion


Active Directory Administrative Center
corp (local) ▸ Domain Controllers
Manage
Help
Active Directory...
OVERVIEW
corp (local)
Domain Controllers
DYNAMIC ACCESS CONT...
GLOBAL SEARCH
Domain Controller: (1)
Filter
Name
Domain Contr...
Site
DC1
Global Catalog
Default-First-Site-Name
add-addsreadonlydomaincontrolleraccount
Domain controller type:
Glol
DNS name:
dc1.corp.cor
Managed by:
Site:
Default-First
Modified:
1/1(
OS:
Windows Se
Description:
Summary
Tasks
DC1
Add to group...
Delete
Move...
Properties
Domain Controllers
Pre-create a Read-only domain controller account...
New
Delete
Search under this node
Properties
WINDOWS POWERSHELL HISTORY



http://technet.microsoft.com/en-us/library/jj574152.aspx

QUESTION 157

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

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

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

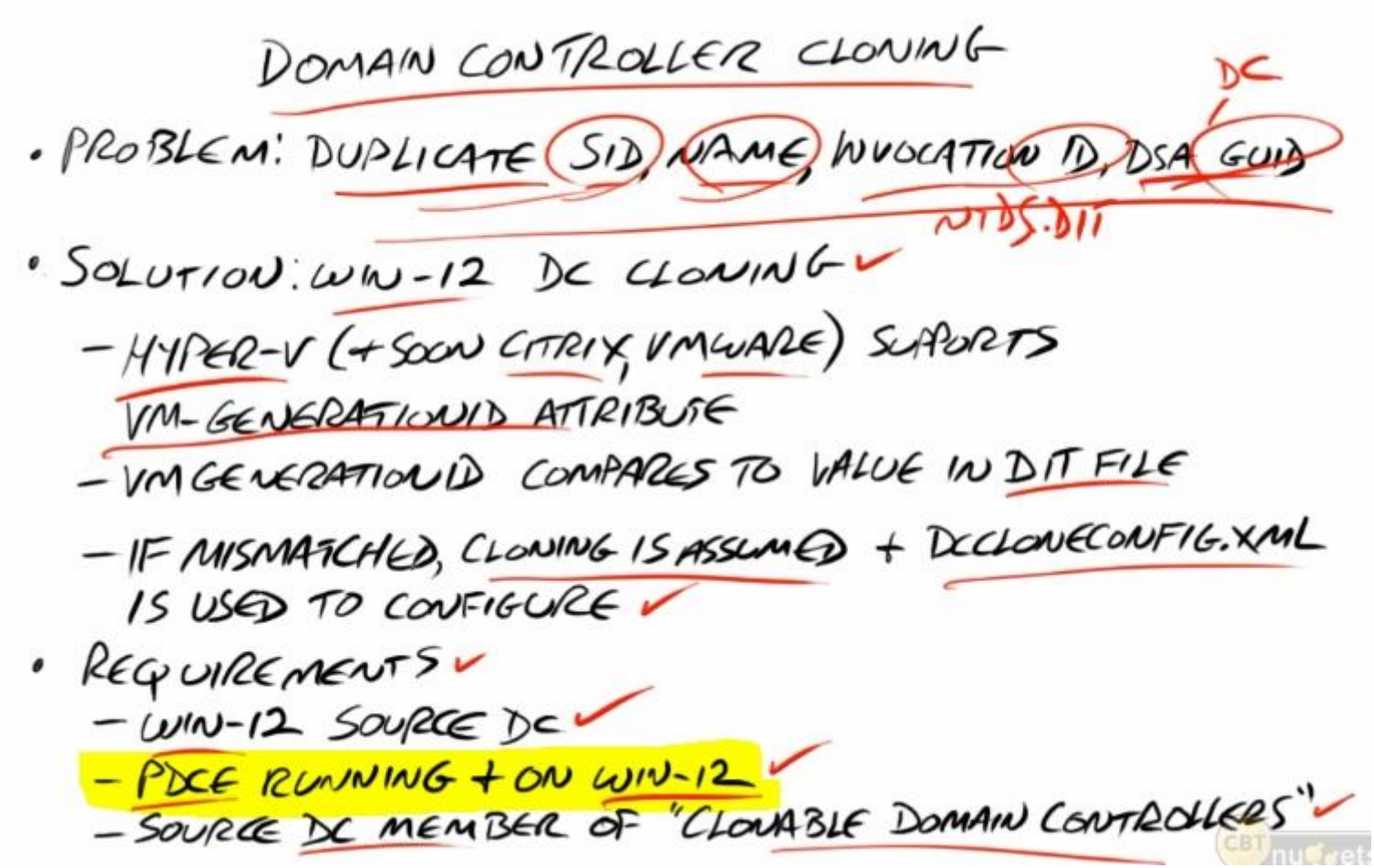
You need to ensure that you can clone DC6.

What should you do?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
PDC must run on a Windows 2012



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

QUESTION 158
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2012.

You need to create a custom Active Directory application partition.

Which tool should you use?

A. Dsadd
B. Dsmod
C. Netdom
D. Ntdsutil

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

ntdsutil The `ntdsutil` utility is the main method by which system administrators create and manage application data partitions on their Windows Server 2012 domain controllers. This utility's specific commands are covered later in this chapter.

Creating and managing application data partitions can be fairly complex. Such a project's success depends on the quality of the architecture design. This is a good example of where IT staff and application developers must cooperate to ensure that data is stored effectively and that it is replicated efficiently.

You can create an application data partition in one of three different locations within an Active Directory forest:

- As a new tree in an Active Directory forest
- As a child of an Active Directory domain partition

  For example, you can create an Accounting application data partition within the `Finance.MyCompany.com` domain.

- As a child of another application data partition

  This method allows you to create a hierarchy of application data partitions.

Explanation: * To create or delete an application directory partition

* partition management
Manages directory partitions for Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS).
This is a subcommand of Ntdsutil and Dsmgmt. Ntdsutil and Dsmgmt are command-line tools that are built into Windows Server 2008 and Windows Server 2008 R2.
/ partition management create nc %s1 %s2
Creates the application directory partition with distinguished name %s1, on the Active Directory domain controller or AD LDS instance with full DNS name %s2. If you specify "NULL" for %s2, this command uses the currently connected Active Directory domain controller. Use this command only with AD DS. For AD LDS, use create nc %s1 %s2 %s3.

Note:

* An application directory partition is a directory partition that is replicated only to specific domain controllers. A domain controller that participates in the replication of a particular application directory partition hosts a replica of that partition.

http://technet.microsoft.com/en-us/library/cc779691%28v=ws.10%29.aspx

QUESTION 159
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012. The domain contains two servers.

The servers are configured as shown in the following table.

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

Server1 and Server2 host a load-balanced website named Web1. Web1 runs by using an application pool named WebApp1. WebApp1 uses a group Managed Service Account named gMSA1 as its identity.

Domain users connect to Web1 by using either the name webl.contoso.com or the alias myweb.contoso.com.

You discover the following:

- When the users access Web1 by using webl.contoso.com, they authenticate by using Kerberos.
- When the users access Web1 by using myweb.contoso.com, they authenticate by using NTLM.

You need to ensure that the users can authenticate by using Kerberos when they connect by using myweb.contoso.com.

What should you do?

A. Modify the properties of the WebApp1 application pool.
B. Run the Add-ADComputerServiceAccount cmdlet.
C. Modify the properties of the Web1 website.
D. Modify the properties of the gMSA1 service account.

Correct Answer: B
Section: (none)
Explanation

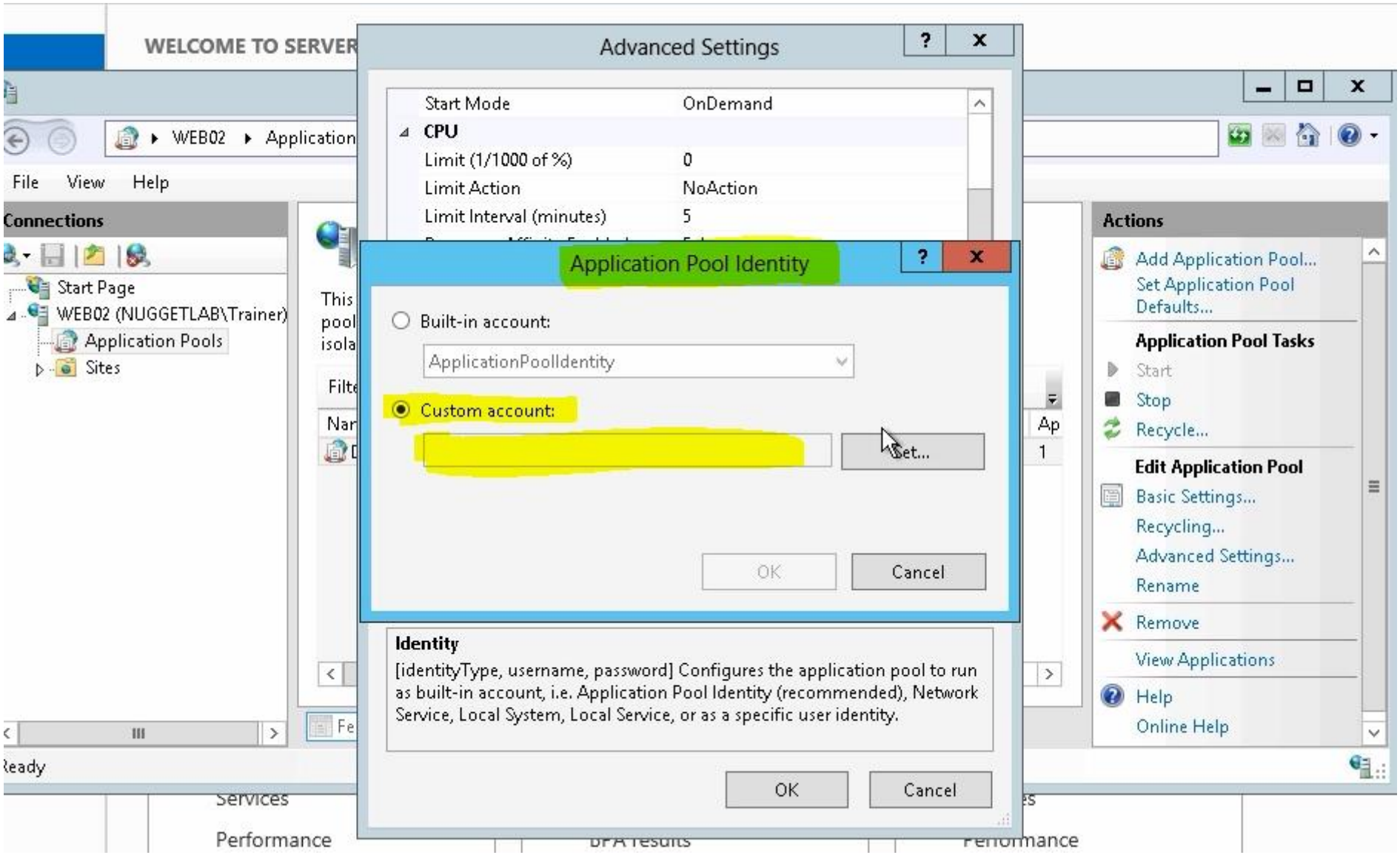
Explanation/Reference:
Managed service accounts and virtual accounts are two new types of accounts introduced in Windows Server 2008 R2/2012 and Windows 7/8 to enhance the service isolation and manageability of network applications such as Microsoft SQL Server and Internet Information Services (IIS).

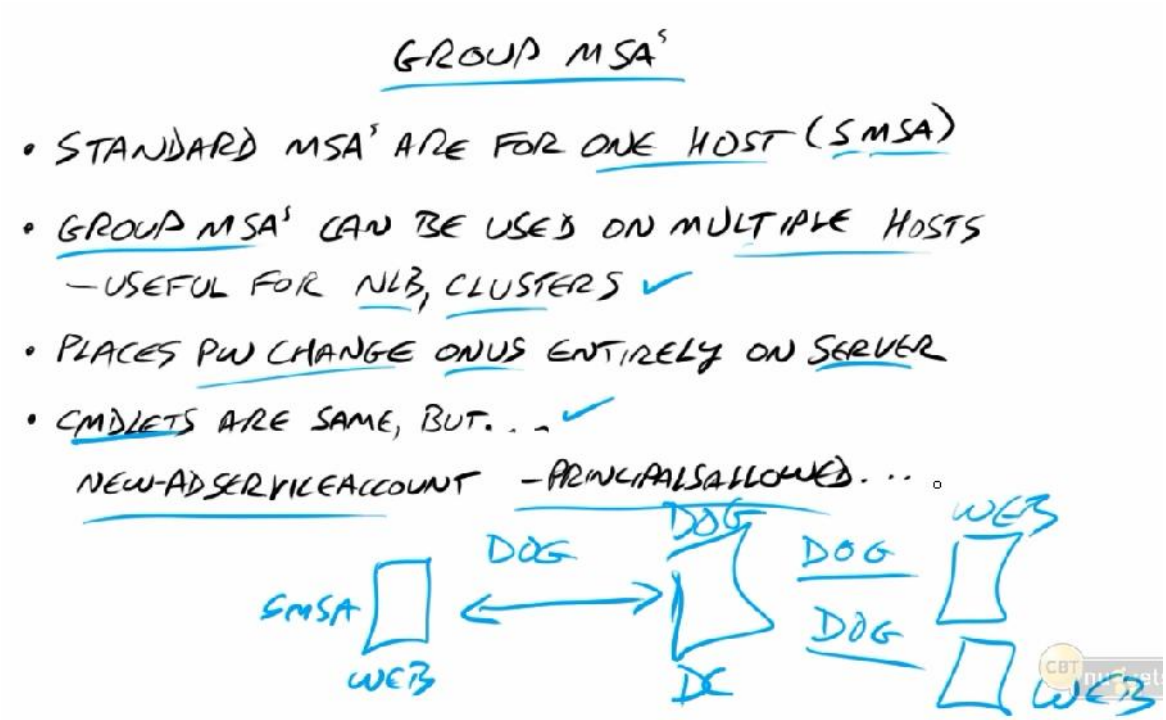
If you configure the application to use a domain account, you can isolate the privileges for the application, but you need to manually manage passwords or create a custom solution for managing these passwords. Many SQL Server and IIS applications use this strategy to enhance security, but this strategy requires additional administration and complexity. In these deployments, service administrators spend a considerable amount of time on maintenance tasks such as managing service passwords and service principal names (SPNs), which are required for Kerberos authentication. In addition, these maintenance tasks can disrupt service.
Two new types of accounts available in Windows Server 2008 R2 and Windows 7--the managed service account and the virtual account--are designed to provide crucial applications such as SQL Server or IIS with the isolation of their own accounts, while eliminating the need for an administrator to manually administer the SPN and credentials for these accounts.

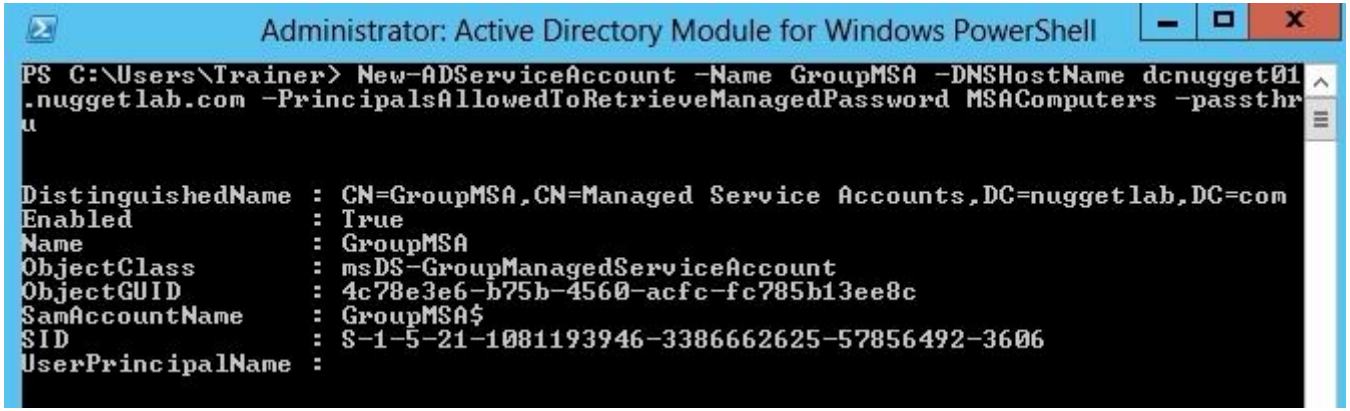
The Add-ADComputerServiceAccount cmdlet adds one or more computer service accounts to an Active Directory computer.
The Computer parameter specifies the Active Directory computer that will host the new service accounts.

Administrator: Active Directory Module for Windows PowerShell

```
PS C:\Users\Trainer> Add-KDSRootKey -EffectiveTime ((Get-Date).AddHours(-10))

Guid
----
8e63775d-68ac-cfe9-24a0-ec6e6a88ed30


PS C:\Users\Trainer> New-ADServiceAccount -Name WebMSA -DNSHostname dcnugget01.n
uggetlab.com -Passthru


DistinguishedName : CN=WebMSA,CN=Managed Service Accounts,DC=nuggetlab,DC=com
Enabled           : True
Name              : WebMSA
ObjectClass       : msDS-GroupManagedServiceAccount
ObjectGUID        : 1be1300d-69d5-4ed1-98f1-f555938c81ca
SamAccountName    : WebMSA$
SID               : S-1-5-21-1081193946-3386662625-57856492-3103
UserPrincipalName :



PS C:\Users\Trainer> Add-ADComputerServiceAccount -identity web02 -ServiceAccoun
t WebMSA -Passthru


DistinguishedName : CN=WEB02,CN=Computers,DC=nuggetlab,DC=com
DNSHostName       : WEB02.nuggetlab.com
Enabled           : True
Name              : WEB02
ObjectClass       : computer
ObjectGUID        : f5cc8ec3-e77b-4ef7-a16b-8387e26b9a13
SamAccountName    : WEB02$
SID               : S-1-5-21-1081193946-3386662625-57856492-2603
UserPrincipalName :


PS C:\Users\Trainer> _
```


WELCOME TO SERVER
Advanced Settings
Start Mode
OnDemand
CPU
Limit (1/1000 of %)
0
Limit Action
NoAction
Limit Interval (minutes)
5
Application Pool Identity
Built-in account:
ApplicationPoolIdentity
Custom account:
Set...
OK
Cancel
Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.
OK
Cancel
WEB02 ▸ Application
File View Help
Connections
Start Page
WEB02 (NUGGETLAB\Trainer)
Application Pools
Sites
Actions
Add Application Pool...
Set Application Pool Defaults...
Application Pool Tasks
Start
Stop
Recycle...
Edit Application Pool
Basic Settings...
Recycling...
Advanced Settings...
Rename
Remove
View Applications
Help
Online Help
Ready
Services
Performance





QUESTION 160
Your network contains an Active Directory domain named contoso.com. The domain contains six domain controllers named DC1, DC2, DC3, DC4, DC5, and DC6. Each domain controller has the DNS Server server role installed and hosts an Active Directory-integrated zone for contoso.com.

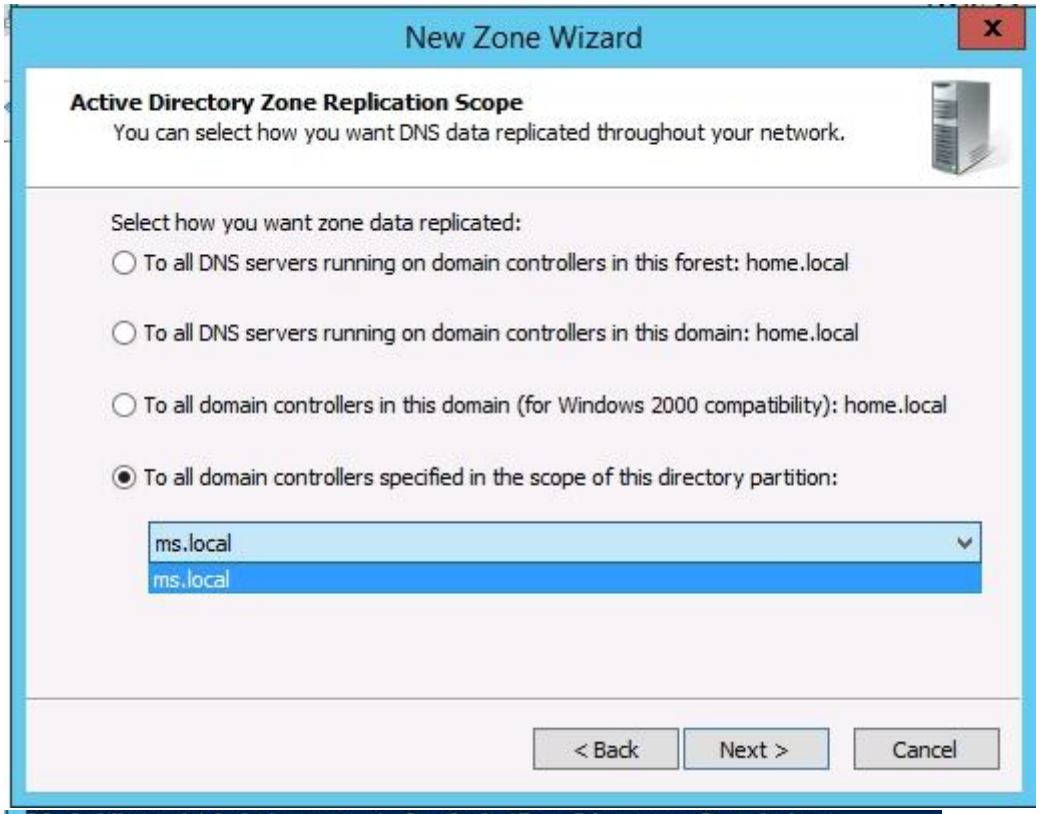
You plan to create a new Active Directory-integrated zone named litwareinc.com that will be used for testing.
You need to ensure that the new zone will be available only on DC5 and DC6.

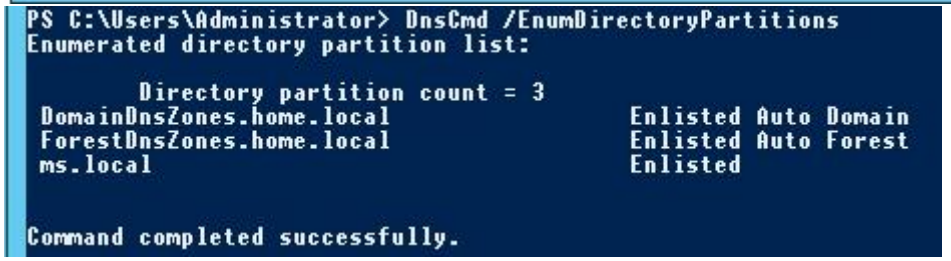
What should you do first?

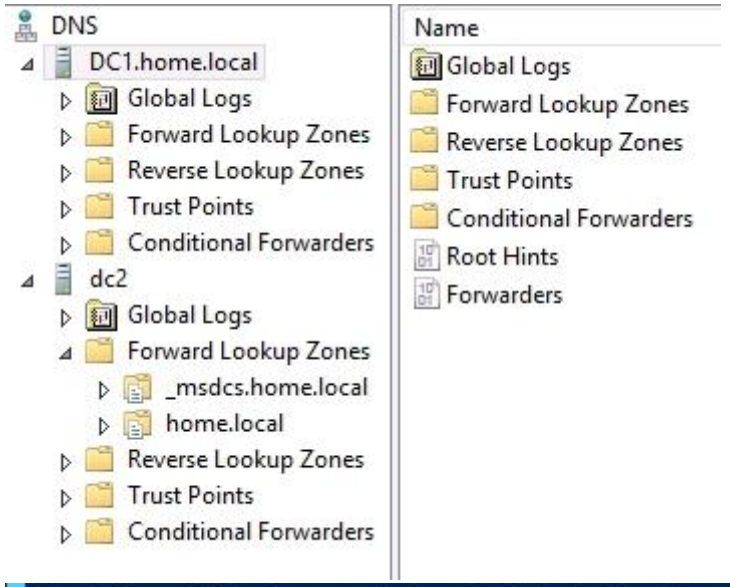
A. Create an application directory partition.
B. Change the zone replication scope.
C. Create an Active Directory connection object.
D. Create an Active Directory site link.

Correct Answer: A
Section: Configure Network Services and Access Services
Explanation

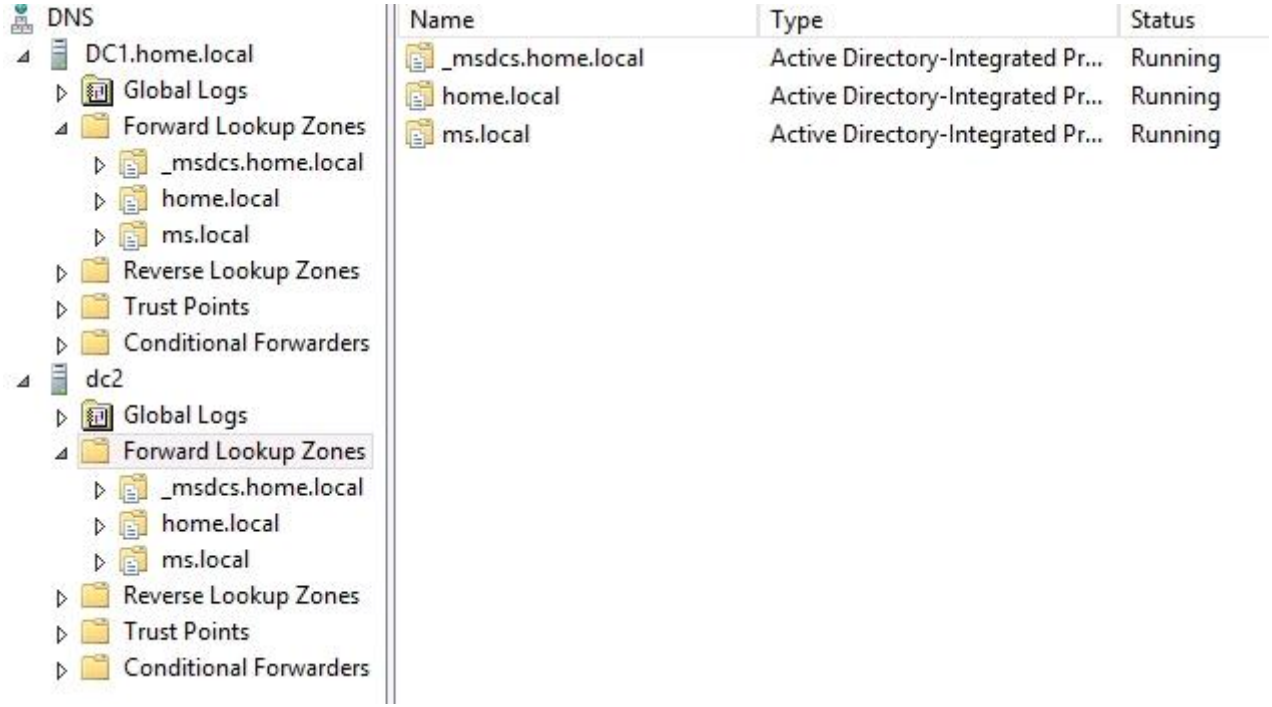
Explanation/Reference:
Active Directory–integrated DNS enables Active Directory storage and replication of DNS zone databases.
Only DNS servers that run on domain controllers can load Active Directory–integrated zones.


New Zone Wizard
Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated:
To all DNS servers running on domain controllers in this forest: home.local
To all DNS servers running on domain controllers in this domain: home.local
To all domain controllers in this domain (for Windows 2000 compatibility): home.local
To all domain controllers specified in the scope of this directory partition:
ms.local
ms.local
< Back
Next >
Cancel


PS C:\Users\Administrator> DnsCmd /EnumDirectoryPartitions
Enumerated directory partition list:
Directory partition count = 3
DomainDnsZones.home.local Enlisted Auto Domain
ForestDnsZones.home.local Enlisted Auto Forest
ms.local Enlisted
Command completed successfully.




```
PS C:\Users\Administrator> dnscmd DC2 /enlistdirectorypartition  ms.local

DNS Server DC2 enlisted directory partition: ms.local
Command completed successfully.
```



http://support.microsoft.com/kb/884116/en-us
http://technet.microsoft.com/en-us/library/cc754292.aspx

QUESTION 161
Your network contains AD named contoso.com. The domain contains RADIUS server named Server1 that runs Windows Server 2012. You add a VPN server named Server2 to the network. On Server1, you created several network policies.

You need to configure Server1 to accept authentication requests from Server2.

Which tool should you use on Server1?

A. Set-RemoteAccessRadius
B. CMAK
C. NPS
D. Routing and Remote Access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
When users attempt to connect to your network through network access servers (also called RADIUS clients), such as wireless access points, 802.1X authenticating switches, dial-up servers, and virtual private network (VPN) servers, Network Policy Server (NPS) authenticates and authorizes the connection request before allowing or denying access.

Because authentication is the process of verifying the identity of the user or computer attempting to connect to the network, NPS must receive proof of identity from the user or computer in the form of credentials.

Some authentication methods use password-based credentials. For example, Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) requires that users type in a user name and password. These credentials are then passed to the NPS server by the network access server, and NPS verifies the credentials against the user accounts database.

Other authentication methods use certificate-based credentials for the user, the client computer, the NPS server, or some combination. Certificate-based authentication methods provide strong security and are recommended over password-based authentication methods.

When you deploy NPS, you can specify the type of authentication method that is required for access to your network.

http://technet.microsoft.com/en-us/library/hh918417.aspx
Set-RemoteAccessRadius
Edits the properties associated with an external RADIUS server being used for VPN authentication, accounting for DirectAccess (DA) and VPN, and one-time password (OTP) authentication for DA.

```
PS C:\> Set-RemoteAccessRadius -ServerName 10.1.2.1 -Purpose Authentication -Timeout 10 -SharedSecret "n3ws3cr3t" -PassThru
```

```
ServerName    Purpose         Score   Timeout(s)   Port   AccountingOnOffMsg MsgAuthenticator
----------    -------         -----   ----------   ----   ------------------ ----------------
10.1.2.1      Authentication  30       10          1812                      Disabled
```

http://technet.microsoft.com/en-us/library/cc731694%28v=ws.10%29.aspx
http://technet.microsoft.com/en-us/library/cc754114.aspx

QUESTION 162
How to configure IIS to change the authentication (kerberos or ntlm)

A. cscript adsutil.vbs set w3svc/*WebSite*/root/NTAuthenticationProviders "Negotiate,NTLM"
B. .
C. .
D. .

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
http://support.microsoft.com/kb/215383/en-us

QUESTION 163
You have a server that runs Windows Server 2012.

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

You plan to apply several updates to Windows2012.vhd.

You need to mount Windows2012.vhd to H:\.

Which tool should you use?

A. Device Manager
B. Diskpart
C. Mountvol
D. Server Manager

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Administrator: Command Prompt - diskpart

```
C:\Windows\system32>diskpart

Microsoft DiskPart version 6.3.9600

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: DC1

DISKPART> SELECT VDISK FILE="c:\Windows2012.vhd"

DiskPart successfully selected the virtual disk file.

DISKPART> ATTACH VDISK

  100 percent completed

DiskPart successfully attached the virtual disk file.

DISKPART> LIST VOLUME

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0         System Rese  NTFS   Partition    350 MB  Healthy    System
  Volume 1     C                NTFS   Partition    126 GB  Healthy    Boot
  Volume 2     D   New Volume   NTFS   Partition    126 GB  Healthy
  Volume 3         New Volume   NTFS   Partition     97 MB  Healthy

DISKPART> SELECT VOLUME 3

Volume 3 is the selected volume.

DISKPART> ASSIGN MOUNT=H:

DiskPart successfully assigned the drive letter or mount point.

DISKPART> LIST VOLUME

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0         System Rese  NTFS   Partition    350 MB  Healthy    System
  Volume 1     C                NTFS   Partition    126 GB  Healthy    Boot
  Volume 2     D   New Volume   NTFS   Partition    126 GB  Healthy
* Volume 3     H   New Volume   NTFS   Partition     97 MB  Healthy

DISKPART>
```

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

http://technet.microsoft.com/en-us/library/cc753321.aspx

QUESTION 164
Your network contains an Active Directory domain named contoso.com. The domain contains a RADIUS server named Server1 that runs Windows Server 2012.

You add a VPN server named Server2 to the network.

On Server1, you create several network policies.

You need to configure Server1 to accept authentication requests from Server2.

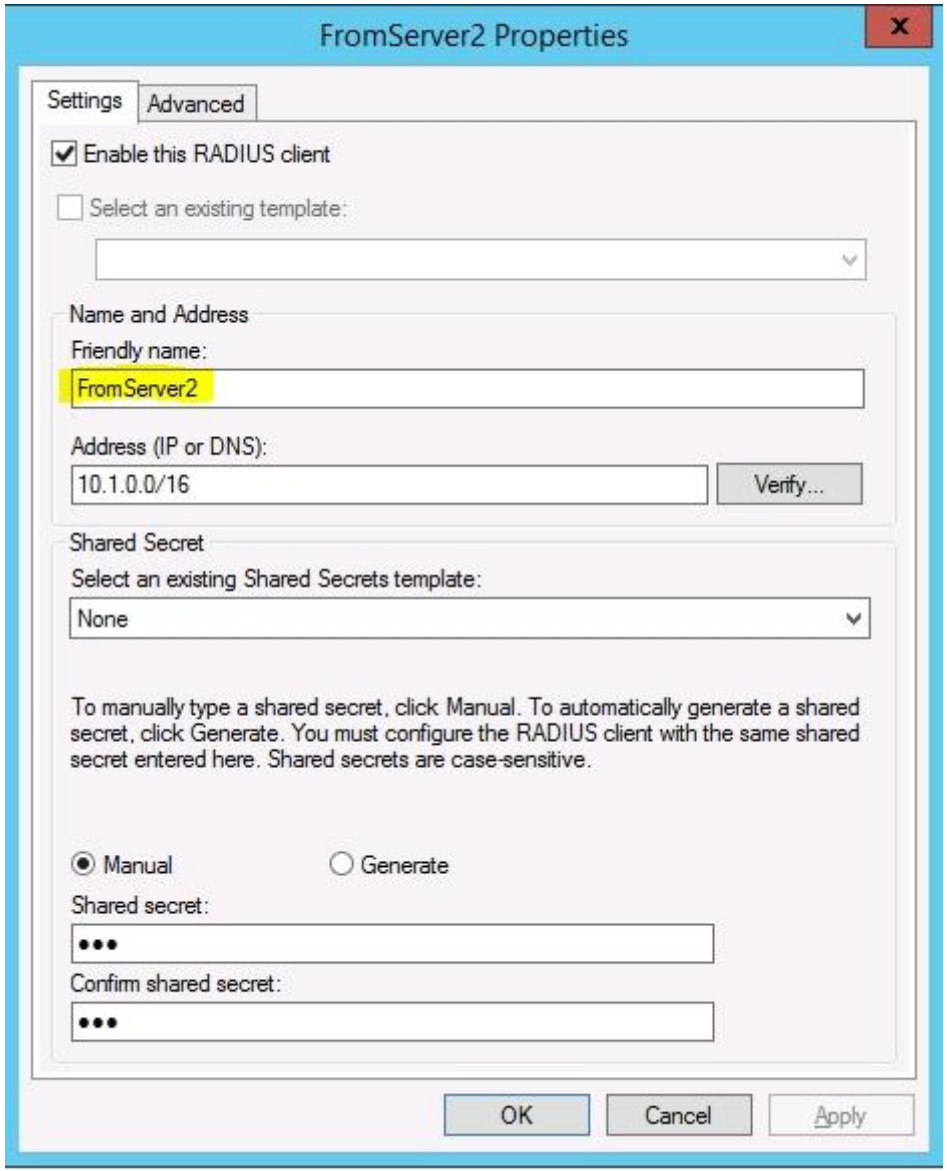
Which tool should you use on Server1?

A. Add-RemoteAccessRadius
B. New-NpsRadiusClient
C. Remote Access Management Console
D. Routing and Remote Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A. Adds a new external RADIUS server for VPN authentication, accounting for DirectAccess (DA) and VPN, or one-time password (OTP) authentication for DA.
B. Creates a RADIUS client.
New-NpsRadiusClient -Name "NameOfMyClientGroup" -Address "10.1.0.0/16" -AuthAttributeRequired 0 -NapCompatible 0 -SharedSecret "SuperSharedSecretxyz" -VendorName "RADIUS Standard"

```
PS C:\Users\Administrator> New-NpsRadiusClient -Name "FromServer2" -Address "10.1.0.0/16" -AuthAttributeRequired 0 -NapC
ompatible 0 -SharedSecret "123" -VendorName "RADIUS Standard"


Name                  : FromServer2
Address               : 10.1.0.0/16
AuthAttributeRequired : False
NapCompatible         : False
SharedSecret          : 123
VendorName            : RADIUS Standard
Enabled               : True
```



C. GUI to manage Remote Access

D. The Routing and Remote Access service (RRAS) supports Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) network routing and remote user or site-to-site connectivity by using virtual private network (VPN) or dial-up connections. http://technet.microsoft.com/en-us/library/hh918425(v=wps.620).aspx

http://technet.microsoft.com/en-us/library/jj872740(v=wps.620).aspx http://technet.microsoft.com/en-us/library/dd469790.aspx

QUESTION 165
Your network contains an Active Directory domain named contoso.com. The domain contains client computers that run either Windows XP, Windows 7, or Windows 8.

Network Policy Server (NPS) is deployed to the domain.

You plan to create a system health validator (SHV).

You need to identify which policy settings can be applied to all of the computers.

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

A. A firewall is enabled for all network connections.
B. An antispyware application is on.
C. Automatic updating is enabled.
D. Antivirus is up to date.
E. Antispyware is up to date.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

Note

You can only choose **An antispyware application is on** if the client computer is running Windows Vista® or Windows® 7. The WSHA on NAP client computers running Windows XP SP3 does not monitor the status of antispyware applications.
The antispyware application is responsible for acquiring and installing spyware definitions. If the client computer is evaluated as noncompliant because spyware definitions are out of date, Windows Security Center will not automatically download and install an update.

Explanation: * System health agent (SHA) is a NAP component.
* System health agent (SHA)
A component that checks the state of the client computer to determine whether the settings monitored by the SHA are up-to-date and configured correctly. For example, the Windows Security Health Agent (WSHA) **can monitor Windows Firewall**, whether **antivirus software is installed**, **enabled**, and **updated**, whether antispyware software is installed, enabled, and updated, and whether **Microsoft Update Services is enabled and the computer has the most recent security updates from Microsoft Update Services**. There might also be SHAs (and corresponding system health validators) available from other companies that provide

different functionality.

System health validators (SHVs) are server software counterparts to system health agents (SHAs). Each SHA on the client has a corresponding SHV in Network Policy Server (NPS). SHVs allow NPS to verify the statement of health (SoH) that is made by its corresponding SHA on the client computer.

Windows Security Health Agent (WSHA)

The WSHA is included with Windows Vista and Windows XP with Service Pack 3 and monitors the operational status of the Windows Security Center (WSC) on NAP client computers. The WSHA monitors the following:

· **Firewall**: If required, the NAP client must have a firewall enabled for all network connections.

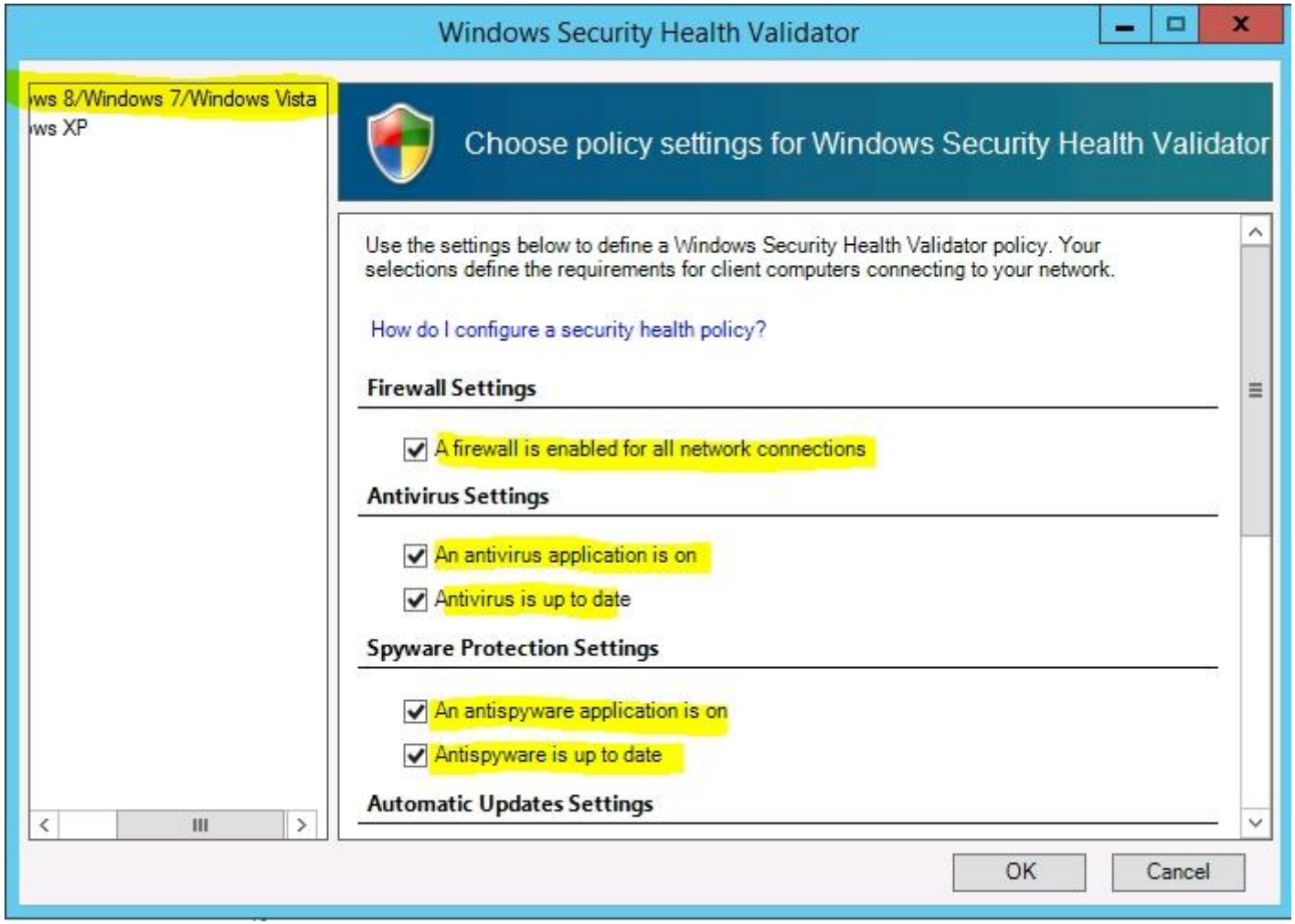
· **Virus Protection**: If required, the NAP client computer must have an antivirus application installed, registered with WSC, and turned on. The NAP client can also be required to have an up-to-date antivirus signature file installed.

· Spyware Protection: If required, the NAP client must have an antispyware application installed, registered with WSC, and turned on. The NAP client can also be required to have an up-to-date antispyware signature file installed. Spyware protection only applies to NAP clients running Windows Vista.

· **Automatic Updating**: If required, the NAP client must be configured to check for updates from Windows Update. You can also require the NAP client to automatically download and install updates.

· **Security Update Protection**: If required, the NAP client must have security updates installed based on one of four possible values that match security severity ratings from the Microsoft Security Response Center (MSRC). You can also specify the use of Windows Server Update Services (WSUS) or Windows Update to obtain security updates.

Windows Security Health Validator
Windows 8/Windows 7/Win
Windows XP
Choose policy settings for Windows Security Health Validator
Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.
How do I configure a security health policy?
Firewall Settings
A firewall is enabled for all network connections
Antivirus Settings
An antivirus application is on
Antivirus is up to date
Automatic Updates Settings
Automatic updating is enabled
Security Updates Settings
Restrict access for clients that do not have all available security updates installed
OK
Cancel



http://technet.microsoft.com/en-us/library/cc731260.aspx

QUESTION 166

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. All domain controllers run Windows Server 2012.

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

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

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

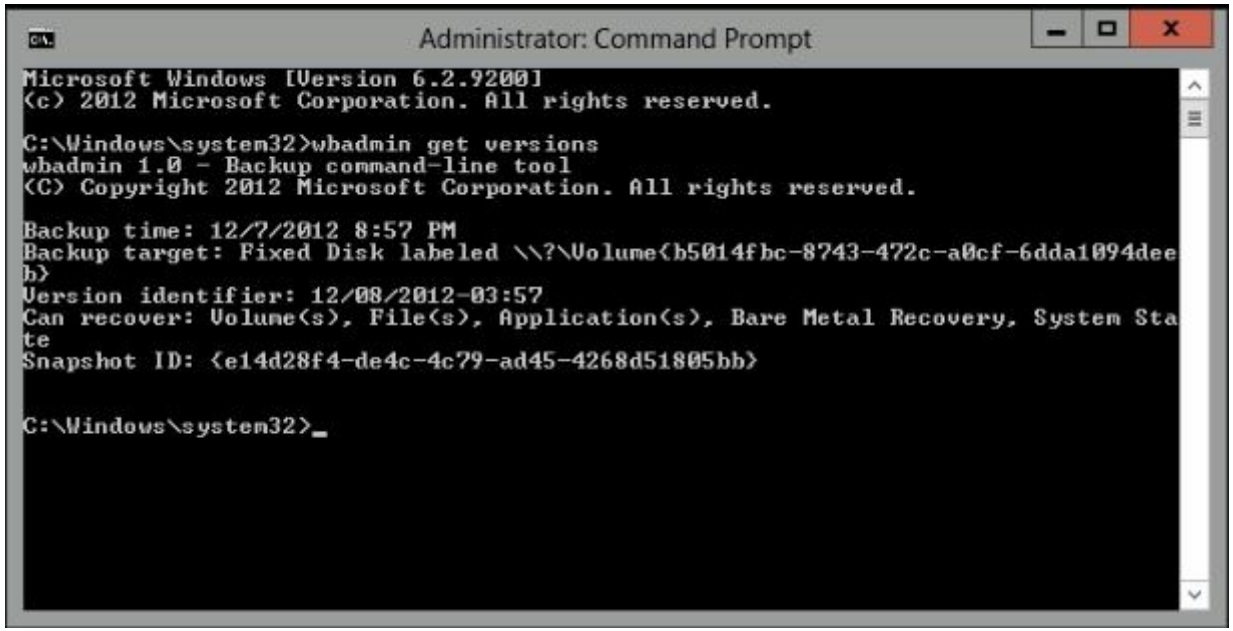
You need to restore the membership of Group1.

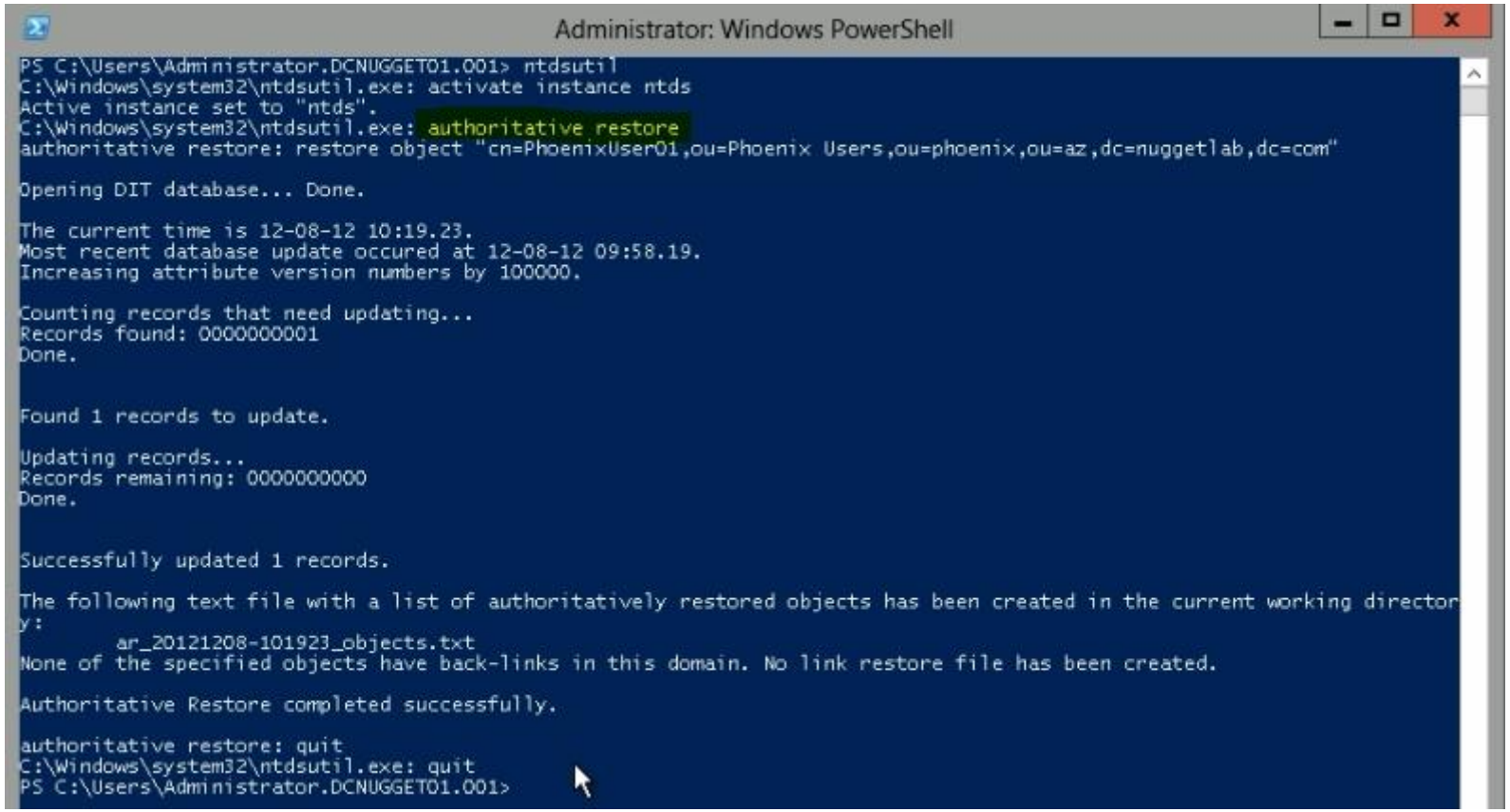
What should you do?

A. Apply a virtual machine snapshot to VM1.
B. Perform an authoritative restore.
C. Perform a non-authoritative restore.
D. Perform tombstone reanimation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Tombstone Reanimation will just restore the object. The membership of the object will not be restored.


Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Windows\system32>wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2012 Microsoft Corporation. All rights reserved.
Backup time: 12/7/2012 8:57 PM
Backup target: Fixed Disk labeled \\?\Volume{b5014fbc-8743-472c-a0cf-6dda1094dee
b}
Version identifier: 12/08/2012-03:57
Can recover: Volume(s), File(s), Application(s), Bare Metal Recovery, System Sta
te
Snapshot ID: {e14d28f4-de4c-4c79-ad45-4268d51805bb}
C:\Windows\system32>_



Explanation: Authoritative restore allows the administrator to recover a domain controller, restore it to a specific point in time, and mark objects in Active Directory as being authoritative with respect to their replication partners. For example, you might need to perform an authoritative restore if an administrator inadvertently deletes an organizational unit containing a large number of users. If you restore the server from tape, the normal replication process would not restore the inadvertently deleted organizational unit. Authoritative restore allows you to mark the organizational unit as authoritative and force the replication process to restore it to all of the other domain controllers in the domain.

Incorrect:
Not C: A nonauthoritative restore returns the domain controller to its state at the time of backup and then allows normal replication to overwrite that state with any changes that occurred after the backup was taken. After you restore the system state, the domain controller queries its replication partners. The replication partners replicate any changes to the restored domain controller, ensuring that the domain controller has an accurate and updated copy of the Active Directory database.

Reference: Performing an Authoritative Restore

QUESTION 167

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

The domain contains two organizational units (OUs) named OU1 and OU2 in the root of the domain.

Two Group Policy objects (GPOs) named GPO1 and GP02 are created. GPO1 is linked to OUl. GPO2 is linked to OU2.

OU1 contains a client computer named Computer1. OU2 contains a user named User1.

You need to ensure that the GPOs applied to Computer1 are applied to User1 when User1 logs on.

What should you configure?

A. Block Inheritance
B. Group Policy loopback processing mode
C. Item-level targeting
D. WMI Filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Note: Loopback processing allows the administrator to apply user Group Policy settings based on where the computer accounts are located rather than basing it on the user account. This is an invaluable setting to use when deploying kiosk computers where you do not want the user settings to be applied.

QUESTION 168
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012.

You mount an Active Directory snapshot on DC1.

You need to expose the snapshot as an LDAP server.

Which tool should you use?

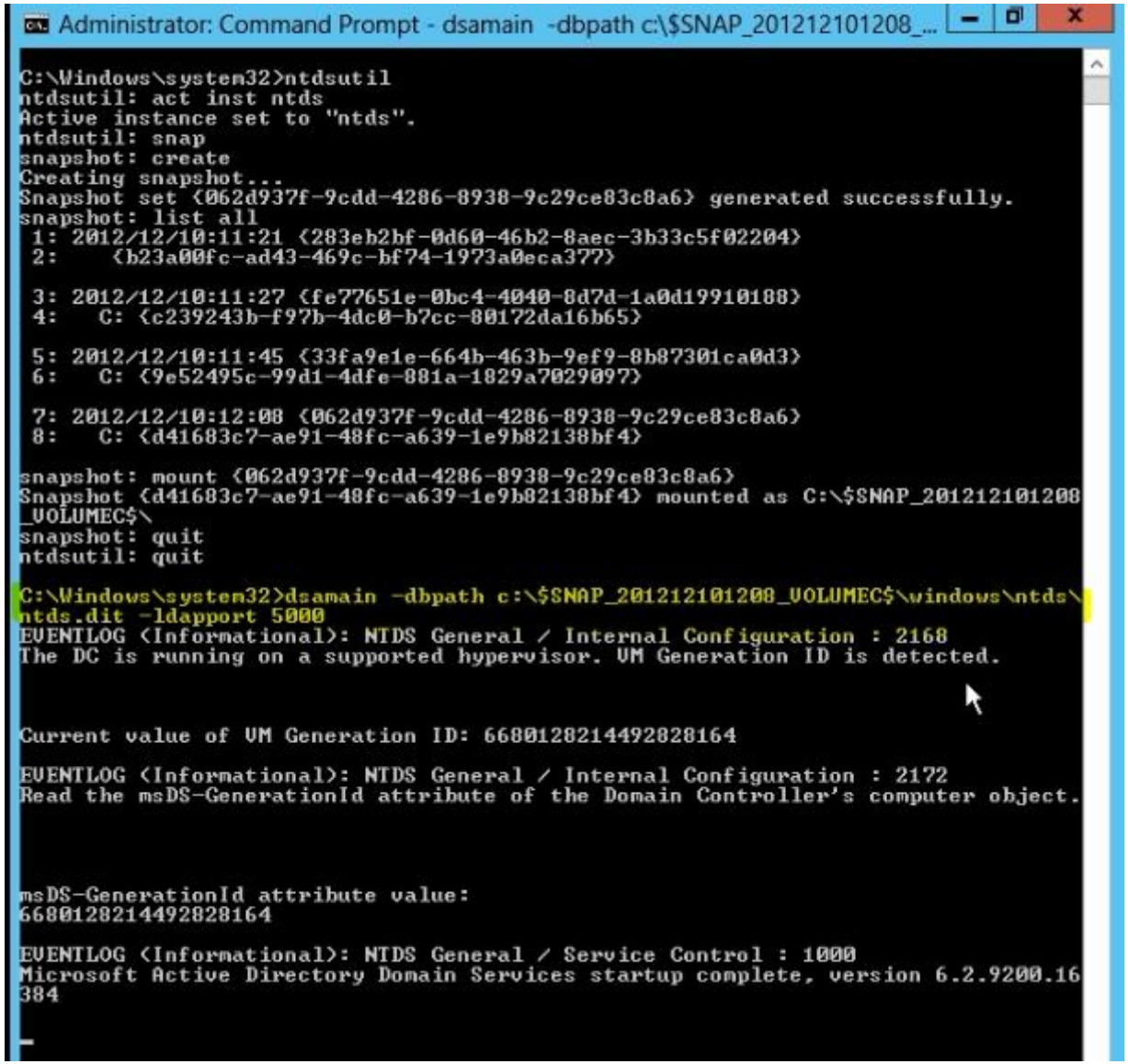
A. ADSI Edit
B. Ntdsutil
C. Dsamain
D. Ldp

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

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



QUESTION 169
You have a server named Server1 that has a Server Core Installation on Windows Server 2012.

You need to view the time-to-live (TTL) value of a host name that is cached on Server1.

What should you run?

A. dnscacheugc.exe
B. ipconfig.exe /displaydns
C. nslookup.exe
D. Show-DNSServerCache

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
ipconfig /displaydns lists the TTL
The difference is, this is typically for client side cache, whereas Show-DnsServerCache is for the cached records on the DNS server in the DNS server cache.

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

Windows IP Configuration

    _gc._tcp.lisboa._sites.dc1.home.local
    ----------------------------------------
    Name does not exist.

    _ldap._tcp.lisboa._sites.dc1.home.local
    ----------------------------------------
    Name does not exist.

    _ldap._tcp.dc1.home.local
    ----------------------------------------
    Name does not exist.

    _gc._tcp.dc1.home.local
    ----------------------------------------
    Name does not exist.

    dc3.home.local
    ----------------------------------------
    Record Name . . . . . : DC3.home.local
    Record Type . . . . . : 1
    Time To Live  . . . . : 670
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.1.12

    dc3
    ----------------------------------------
    Record Name . . . . . : DC3.home.local
    Record Type . . . . . : 1
    Time To Live  . . . . : 670
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.1.12


C:\Windows\system32>_
```

QUESTION 170

The contoso.com domain contains a a DNS server named Server1 that host a primary zone. Server2 contains a a secondary zone for the contoso.com domain You need to configure how long Server2 queries Server1 to renew the zone.

What should you configure?

A. Retry Interval
B. Minimum TTL
C. Refresh Interval
D. Authority Record

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A. The time, in seconds, a secondary server waits before retrying a failed zone transfer. Normally, this time is less than the refresh interval. The default value is 600 seconds (10 minutes).
B The default Time-To-Live (TTL) of the zone and the maximum interval for caching negative answers to name queries. The default value is 3,600 seconds (1 hour).
C. The time, in seconds, that a secondary DNS server waits before querying its source for the zone to attempt renewal of the zone. When the refresh interval expires, the secondary DNS server requests a copy of the current SOA record for the zone from its source, which answers this request. The secondary DNS server then compares the serial number of the source server's current SOA record (as indicated in the response) with the serial number in its own local SOA record. If they are different, the secondary DNS server requests a zone transfer from the primary DNS server. The default for this field is 900 seconds (15 minutes).
D.
http://technet.microsoft.com/en-us/library/cc779148(v=ws.10).aspx

QUESTION 171
You are a network administrator of an Active Directory domain named contoso.com. You have a server named Server1 that runs Windows Server 2012. Server1 has the DHCP Server server role and the Network Policy Server role service installed.

You enable Network Access Protection (NAP) on all of the DHCP scopes on Server1.

You need to create a DHCP policy that will apply to all of the NAP non-compliant DHCP clients.

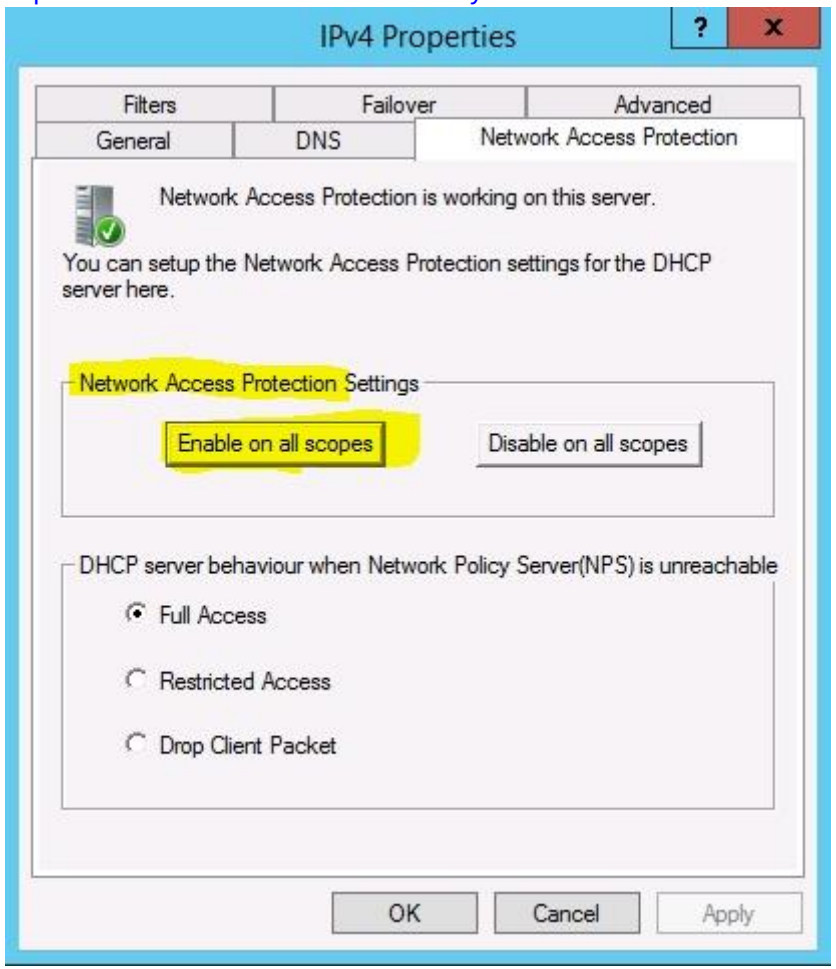
Which criteria should you specify when you create the DHCP policy?

A. The relay agent information
B. The user class
C. The vendor class

D. The client identifier

Correct Answer: B
Section: (none)
Explanation

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



QUESTION 172
Your network contains an Active Directory domain named adatum.com. The domain contains a server named Server1 that runs Windows Server 2012. Server1 is configured as a Network Policy Server (NPS) server and as a DHCP server.

The network contains two subnets named Subnet1 and Subnet2. Server1 has a DHCP scope for each subnet.

You need to ensure that noncompliant computers on Subnet1 receive different network policies than noncompliant computers on Subnet2.

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

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation: C: 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.

D: If policies are filtered by DHCP scope, then MS-Service Class is configured in policy conditions.

QUESTION 173
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. All of the DNS servers in both of the domains run Windows Server 2012.

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

Client computers that connect to Server1 for name resolution cannot resolve names in fabrikam.com.
You need to configure Server1 to resolve names in fabrikam.com. The solution must NOT require that changes be made to the fabrikam.com zone on Server2.

What should you create?

A. a secondary zone

B. a stub zone
C. a trust anchor
D. a zone delegation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012. 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 Windows PowerShell, run the Set-DnsServerForwarder cmdlet and specify the contoso.com zone as a target.
B. From Windows PowerShell, run the Set-DnsServerSetting cmdlet and specify DC1 as a target.
C. From Windows PowerShell, run the Set-DnsServerPrimaryZone cmdlet and specify the contoso.com zone as a target.
D. From DNS Manager, modify the Advanced settings of DC1.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
The **Set-DnsServerPrimaryZone** cmdlet changes settings for an existing Domain Name System (DNS) primary zone. You can change values that are relevant for either Active Directory-integrated zones or file-backed zones.

http://technet.microsoft.com/en-us/library/jj649865.aspx

QUESTION 175
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

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

You make a change to GPO1.

You need to force all of the computers in OU1 to refresh their Group Policy settings immediately. The solution must minimize administrative effort.
Which tool should you use?

A. the Secedit command
B. the Set-AdComputer cmdlet
C. Active Directory Users and Computers
D. the Invoke-GpUpdate cmdlet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Invoke-GPUpdate
Schedule a remote Group Policy refresh (gpupdate) on the specified computer.
Applies To: Windows Server 2012
The Invoke-GPUpdate cmdlet refreshes Group Policy settings, including security settings that are set on remote computers by scheduling the running of the Gpupdate command on a remote computer. You can combine this cmdlet in a scripted fashion to schedule the Gpupdate command on a group of computers.
The refresh can be scheduled to immediately start a refresh of policy settings or wait for a specified period of time, up to a maximum of 31 days. To avoid putting a load on the network, the refresh times will be offset by a random delay.

Note:
Group Policy is a complicated infrastructure that enables you to apply policy settings to remotely configure a computer and user experience within a domain. When the Resultant Set of Policy settings does not conform to your expectations, a best practice is to first verify that the computer or user has received the latest policy settings. In previous versions of Windows, this was accomplished by having the user run GPUpdate.exe on their computer. With Windows Server 2012 and Windows 8, you can remotely refresh Group Policy settings for all computers in an organizational unit (OU) from one central location by using the Group Policy Management Console (GPMC). Or you can use the Invoke-GPUpdate Windows PowerShell cmdlet to refresh Group Policy for a set of computers, including computers that are not within the OU structure--for example, if the computers are located in the default computers container.
The remote Group Policy refresh updates all Group Policy settings, including security settings that are set on a group of remote computers, by using the functionality that is added to the context menu for an OU in the Group Policy Management Console (GPMC). When you select an OU to remotely refresh the Group Policy settings on all the computers in that OU, the following operations happen:
An Active Directory query returns a list of all computers that belong to that OU. For each computer that belongs to the selected OU, a WMI call retrieves the list of signed in users.
A remote scheduled task is created to run GPUpdate.exe /force for each signed in user and once for the computer Group Policy refresh. The task is scheduled to

run with a random delay of up to 10 minutes to decrease the load on the network traffic. This random delay cannot be configured when you use the GPMC, but you can configure the random delay for the scheduled task or set the scheduled task to run immediately when you use the Invoke-GPUpdate cmdlet.

Reference: Force a Remote Group Policy Refresh (GPUpdate)

QUESTION 176
Your network contains an Active Directory domain named adatum.com. You have a standard primary zone named adatum.com.

You need to provide a user named User1 the ability to modify records in the zone. Other users must be prevented from modifying records in the zone.

What should you do first?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Your network contains two Active Directory domains named contoso.com and adatum.com. The contoso.com domain contains a server named Server1.contoso.com. The adatum.com domain contains a server named server2.adatum.com.

Server1 and Server2 run Windows Server 2012 and have the DirectAccess and VPN (RRAS) role service installed.

Server1 has the default network policies and the default connection request policies.

You need to configure Server1 to perform authentication and authorization of VPN connection requests to Server2. Only users who are members of Adatum\Group1 must be allowed to connect.

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

A. Network policies
B. Connection request policies
C. Create a network policy.

D. Create a connection request policy.

Correct Answer: AD
Section: (none)
Explanation

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

You can create connection request policies so that some RADIUS request messages sent from RADIUS clients are processed locally (NPS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (NPS is being used as a RADIUS proxy).

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

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

QUESTION 178
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012.

Server1 has a drive named E that is encrypted by using BitLocker Drive Encryption (BitLocker). A recovery key is stored on drive C.

Drive E becomes locked.

When you attempt to use the recovery key, you receive the following error message.

You need to access the data stored on drive E.

What should you run first?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Can I save the startup key on multiple USB flash drives?

Yes, you can save a computer's startup key on multiple USB flash drives.

Can I save multiple (different) startup keys on the same USB flash drive?

Yes, you can save BitLocker startup keys for different computers on the same USB flash drive.

Can I generate multiple (different) startup keys for the same computer?

You can generate different startup keys for the same computer through scripting. However, for computers that have a TPM, creating different startup keys prevents BitLocker from

Can I generate multiple PIN combinations?

It is technically possible to generate multiple PINs, but it is neither supported nor recommended.
http://technet.microsoft.com/en-us/library/cc766200%28v=ws.10%29.aspx#BKMK_MultiKeyOneUSB

Manage-bde: **protectors**
Manages the protection methods used for the BitLocker encryption key.
http://technet.microsoft.com/en-us/library/ff829848.aspx

Parameter	Description
-get	Displays all the key protection methods enabled on the drive and provides their type and identifier (ID).

Manage-bde: unlock
Unlocks a BitLocker-protected drive by using a recovery password or a recovery key.
http://technet.microsoft.com/en-us/library/ff829854.aspx
The following example illustrates using the **-unlock** command to unlock drive E with a recovery key file that has been saved to a backup folder on another drive.

```
manage-bde -unlock E: -recoverykey "F:\Backupkeys\recoverykey.bek"
```

QUESTION 180

Your network contains an Active Directory domain named contoso.com. All user accounts reside in an organizational unit (OU) named OU1.

You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preference of GPO1 to add a shortcut named Link1 to the desktop of each user.
You discover that when a user deletes Link1, the shortcut is removed permanently from the desktop.

You need to ensure that if a user deletes Link1, the shortcut is added to the desktop again.

What should you do?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Actions

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

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

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

QUESTION 181
Your network contains an Active Directory forest named contoso.com. The forest contains two sites named Main and Branch. The Main site contains 400 desktop computers and the Branch site contains 150 desktop computers. All of the desktop computers run Windows 8.

In Main, the network contains a member server named Server1 that runs Windows Server 2012.

You install the Windows Server Update Services server role on Server1.

You need to ensure that Windows updates obtained from Windows Server Update Services (WSUS) are the same for the computers in each site. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do?

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

E. From the Update Services console, configure the Synchronization Schedule options.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
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	File and Storage Services
Server3	Windows Server 2012	Active Directory Certificate Services

You plan to implement the BitLocker Drive Encryption (BitLocker) Network Unlock feature.

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

Which role should you identify?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Print1.

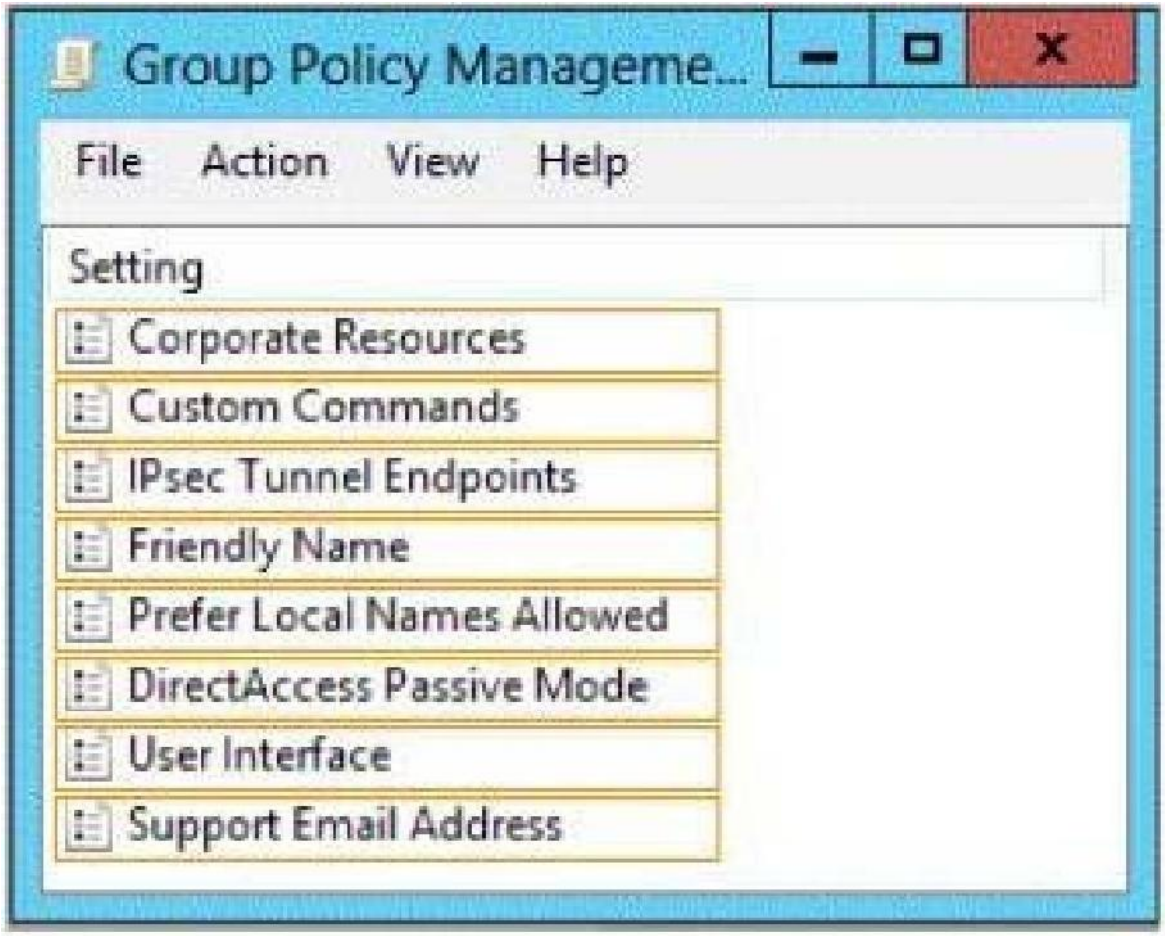
Your company implements DirectAccess.

A user named User1 frequently works at a customer's office. The customer's office contains a print server named Print1.

While working at the customer's office, User1 attempts to connect to Print1. User1 connects to the Print1 server in contoso.com instead of the Print1 server at the customer's office.

You need to provide User1 with the ability to connect to the Print1 server in the customer's office.

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

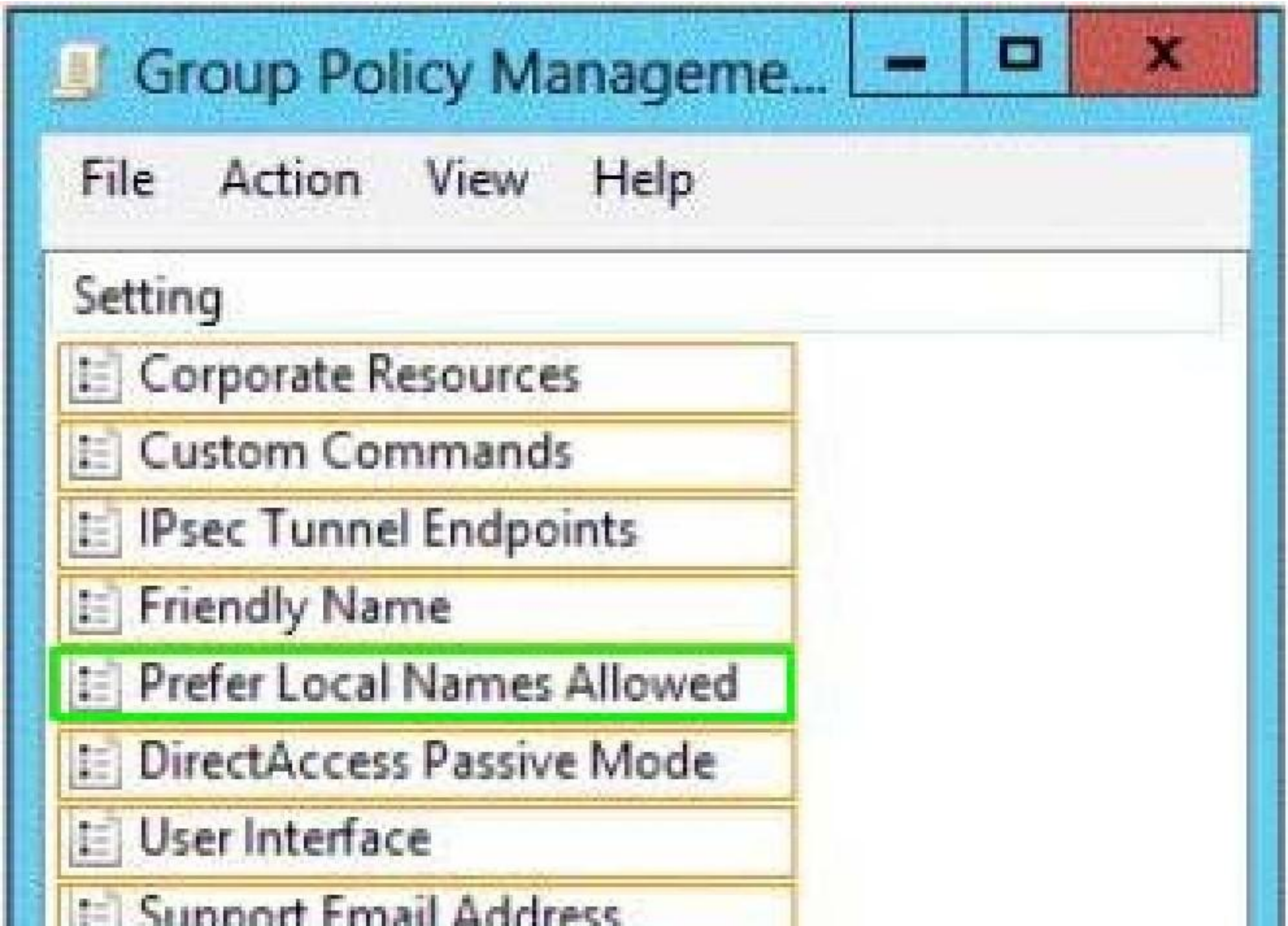


A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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


Group Policy Manageme...
File
Action
View
Help
Setting
Corporate Resources
Custom Commands
IPsec Tunnel Endpoints
Friendly Name
Prefer Local Names Allowed
DirectAccess Passive Mode
User Interface
Support Email Address

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

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

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

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

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

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

QUESTION 184
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

In a remote site, a support technician installs a server named DC10 that runs Windows Server 2012. DC10 is currently a member of a workgroup.

You plan to promote DC10 to a read-only domain controller (RODC).

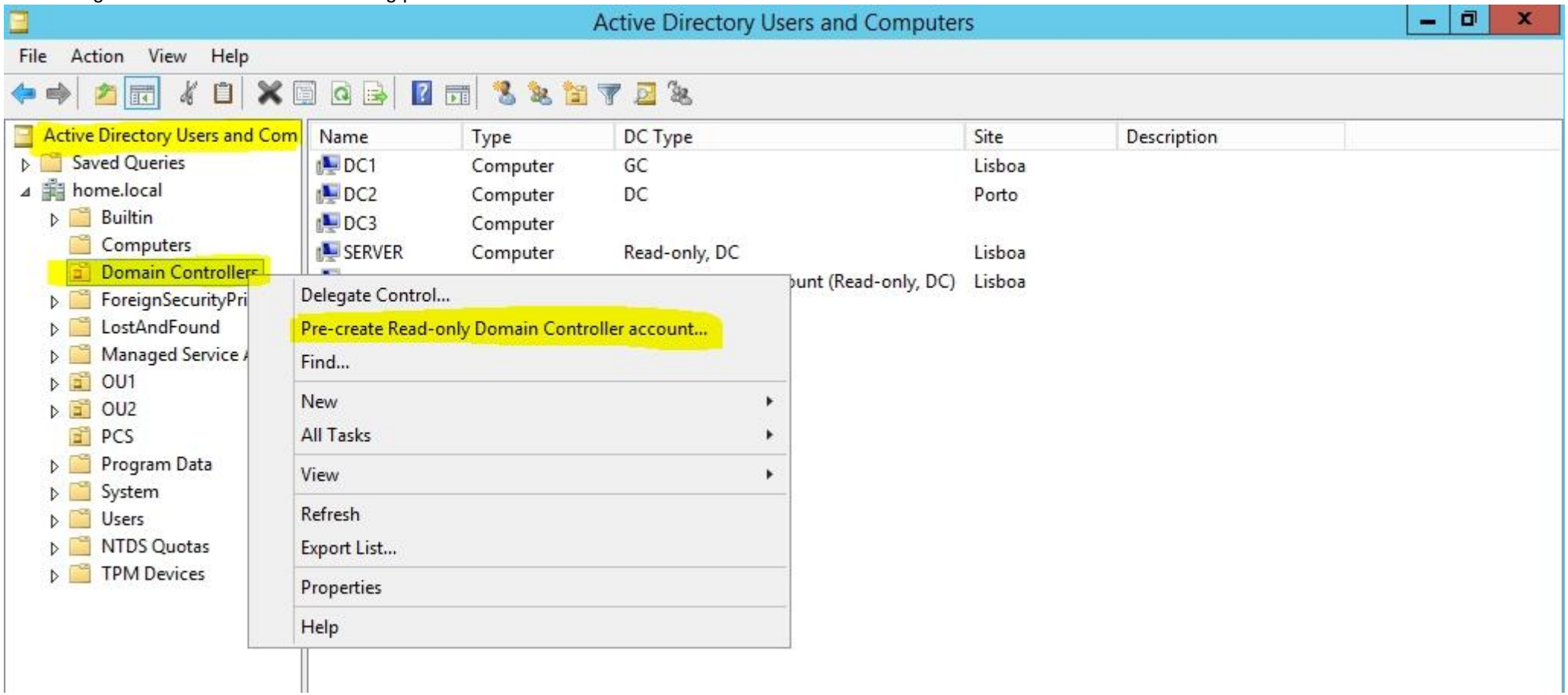
You need to ensure that a user named Contoso\User1 can promote DC10 to a RODC in the contoso.com domain. The solution must minimize the number of permissions assigned to User1.

What should you do?

A. From Ntdsutil, run the local roles command.
B. From Active Directory Users and Computers, pre-create an RODC computer account.
C. From Active Directory Users and Computers, run the Delegation of Control Wizard on the contoso.com domain object.
D. Join DC10 to the domain. Modify the properties of the DC10 computer account.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: A staged read only domain controller (RODC) installation works in two discrete phases:
1.Staging an unoccupied computer account
2.Attaching an RODC to that account during promotion

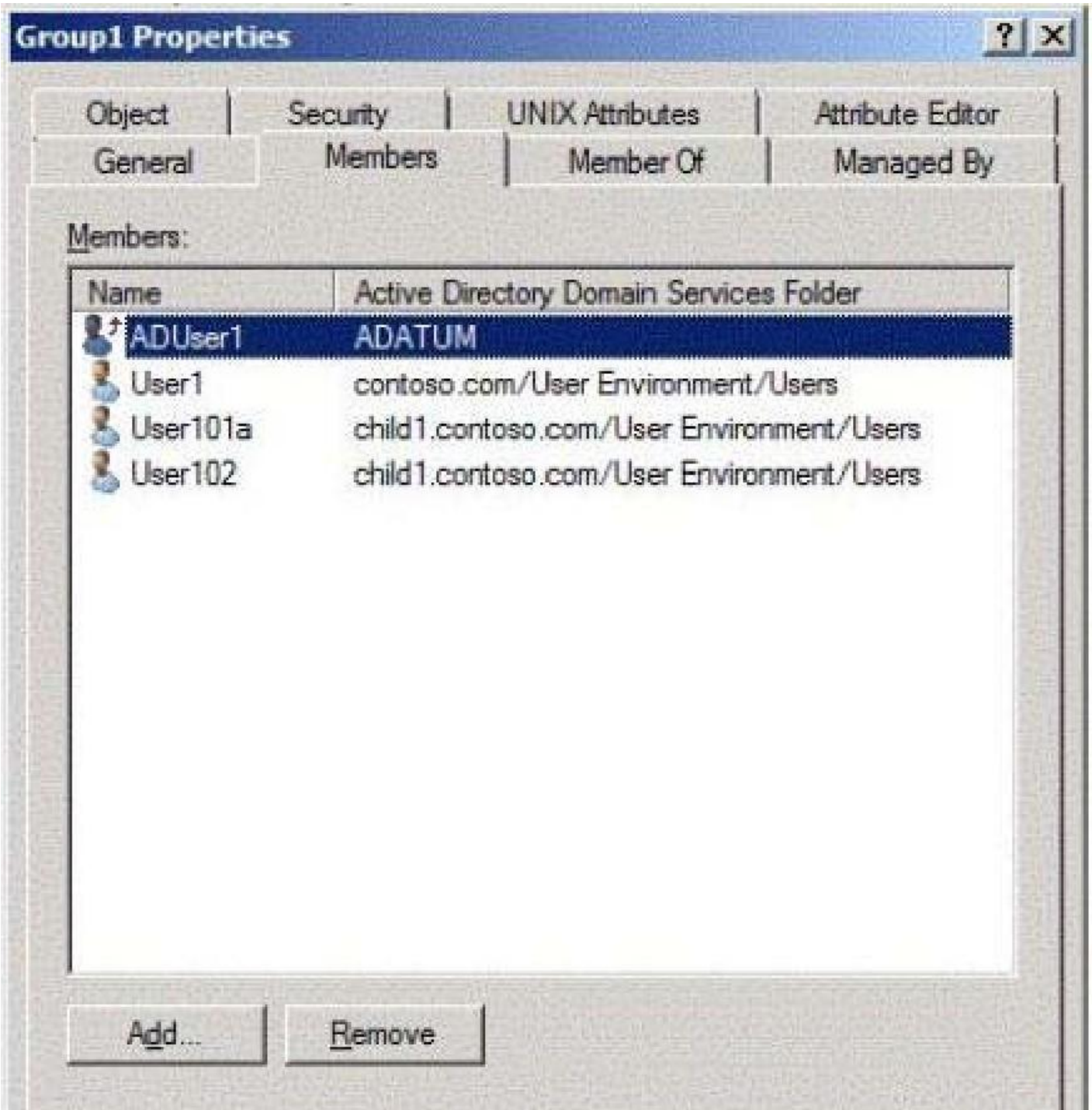


QUESTION 185
Your network contains an Active Directory forest named contoso.com. The forest contains two domains named contoso.com and childl.contoso.com. All domain controllers run Windows Server 2012.

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

Domain controller name	Domain name	Role
DC1	Contoso.com	PDC emulator RID master Schema master Domain naming master
DC2	Contoso.com	Infrastructure master
DC10	Child1.contoso.com	PDC emulator RID master
DC11	Child1.contoso.com	Infrastructure master

You open Active Directory Users and Computers on a client computer and connect to DC1. You display the members of a group named Group1 as shown in the Group1 Members exhibit. (Click the Exhibit button.)


Group1 Properties
Object
Security
UNIX Attributes
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
ADUser1
ADATUM
User1
contoso.com/User Environment/Users
User101a
child1.contoso.com/User Environment/Users
User102
child1.contoso.com/User Environment/Users
Add...
Remove

When you view the properties of a user named User102, you receive the error message shown in the Error exhibit. (Click the Exhibit button.)

The error message does not display for any other members of Group1.

You need to identify which domain controller causes the issue shown in the error message.

Which domain controller should you identify?

A. DC1
B. DC2
C. DC10
D. DC11

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
The infrastructure master is also responsible for updating the group-to-user references whenever the members of groups are renamed or changed. When you rename or move a member of a group (and that member resides in a different domain from the group), the group may temporarily appear not to contain that member. The infrastructure master of the group's domain is responsible for updating the group so it knows the new name or location of the member. This prevents the loss of group memberships associated with a user account when the user account is renamed or moved. .....There is no compromise to security during the time between the member rename and the group update. Only an administrator looking at that particular group membership would notice the temporary inconsistency.

QUESTION 186
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012. The domain contains a file server named Server1.

All client computers run Windows 8.

Users share the client computers and frequently log on to different client computers.

You need to ensure that when the users save files in the Documents folder, the files are saved automatically to \\Server1\Users\. The solution must minimize the amount of network traffic that occurs when the users log on to the client computers.

What should you do?

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

Correct Answer: C
Section: (none)
Explanation

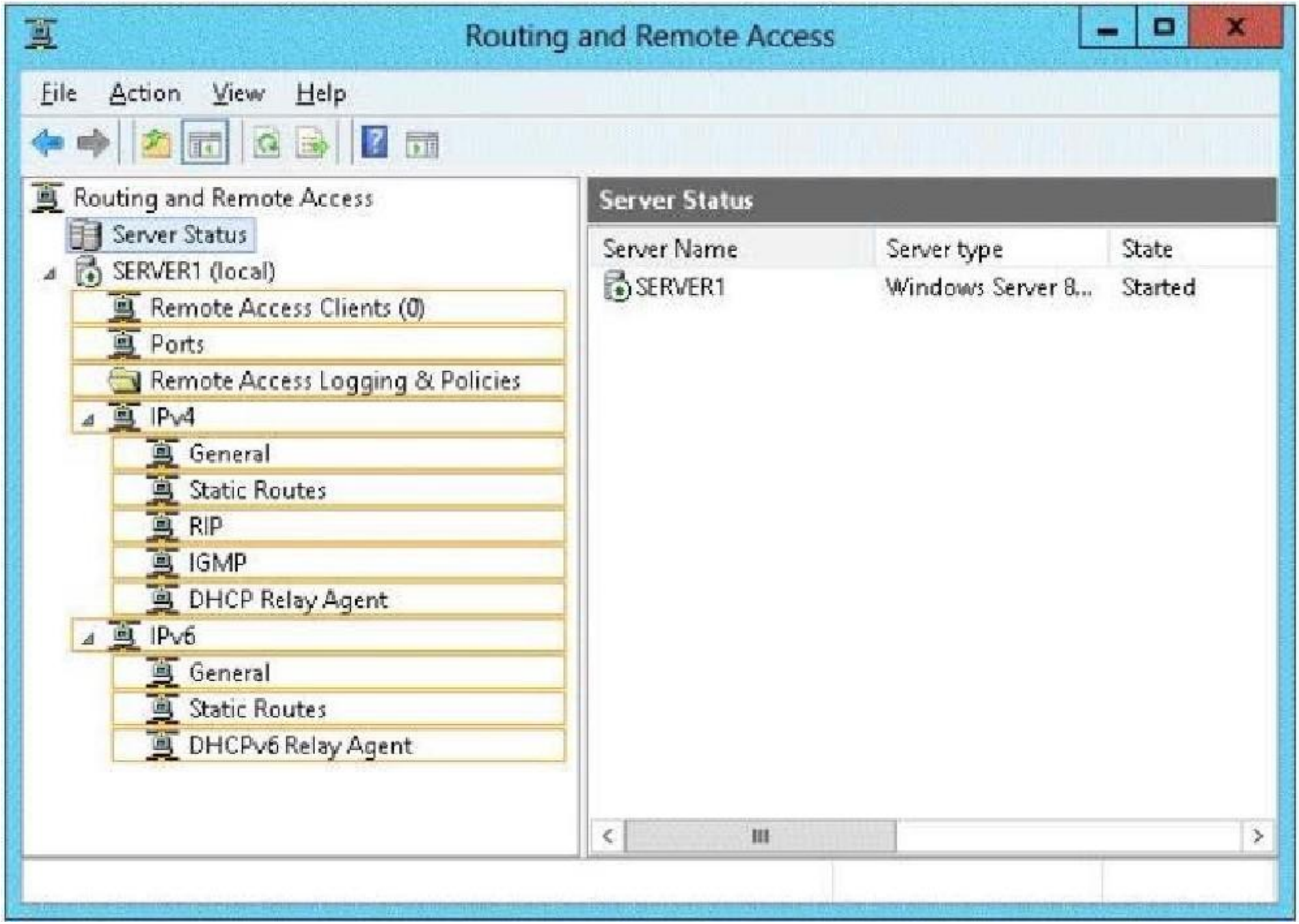
Explanation/Reference:

QUESTION 187
You have a server named Server1 that runs Windows Server 2012. Server1 has two network adapters and is located in a perimeter network.

You need to configure Server1 as a network address translation (NAT) server.

Which node should you use to add the NAT routing protocol?

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

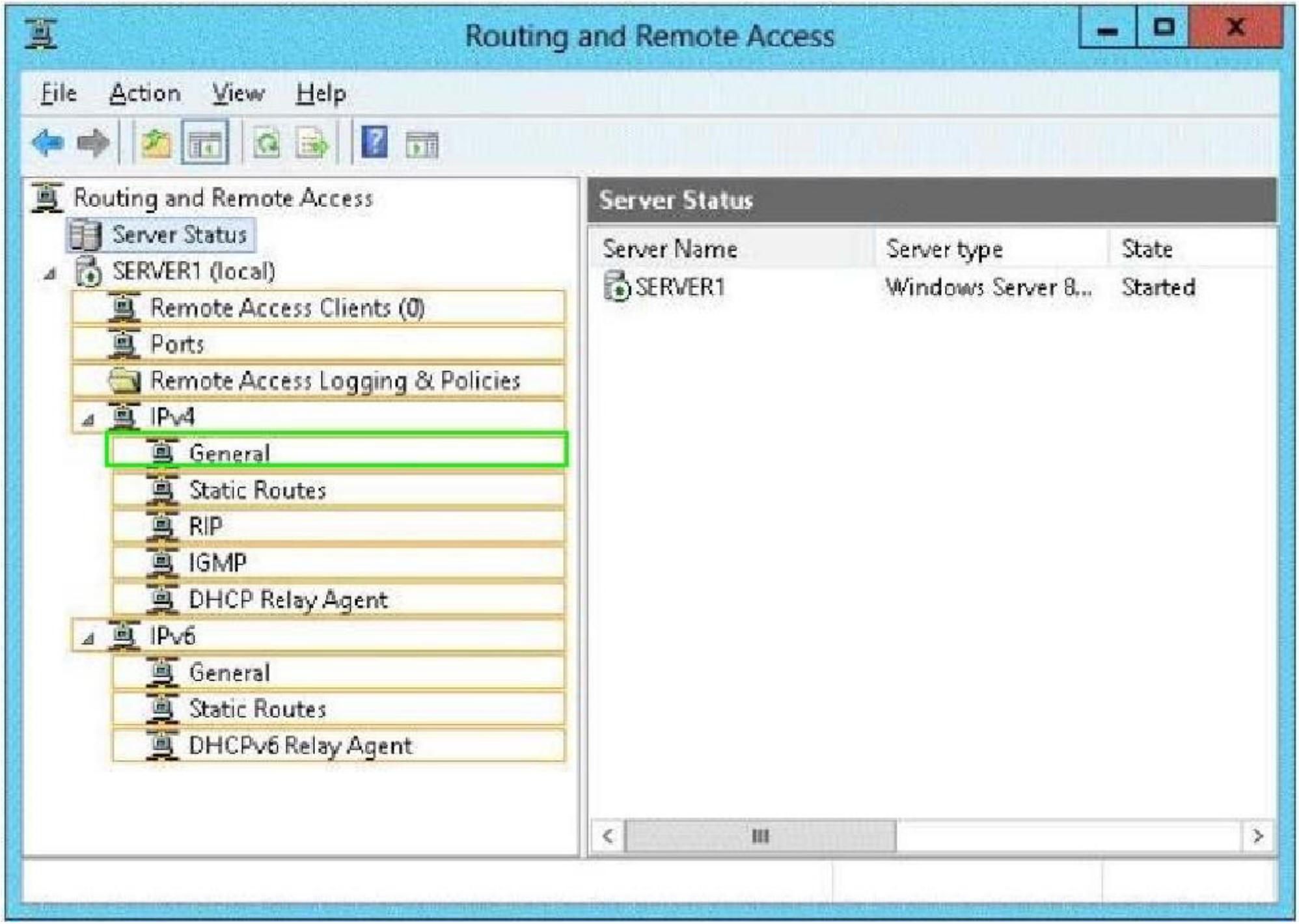

Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
SERVER1 (local)
Remote Access Clients (0)
Ports
Remote Access Logging & Policies
IPv4
General
Static Routes
RIP
IGMP
DHCP Relay Agent
IPv6
General
Static Routes
DHCPv6 Relay Agent
Server Status
Server Name
Server type
State
SERVER1
Windows Server 8...
Started

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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

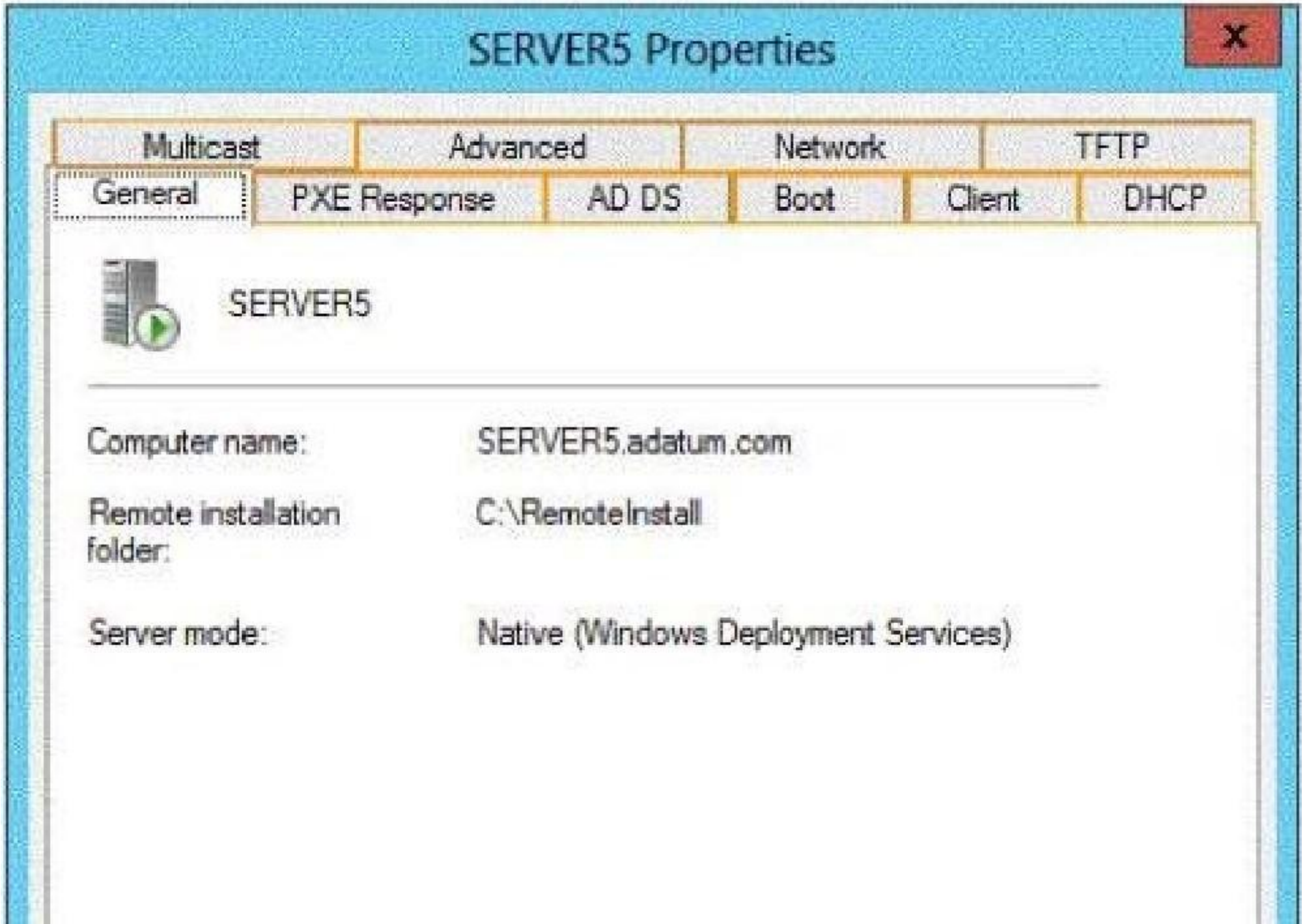

Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
SERVER1 (local)
Remote Access Clients (0)
Ports
Remote Access Logging & Policies
IPv4
General
Static Routes
RIP
IGMP
DHCP Relay Agent
IPv6
General
Static Routes
DHCPv6 Relay Agent
Server Status
Server Name
Server type
State
SERVER1
Windows Server 8...
Started

QUESTION 188
You have a server named Server5 that runs Windows Server 2012. Servers has the Windows Deployment Services server role installed.

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

What should you configure?

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

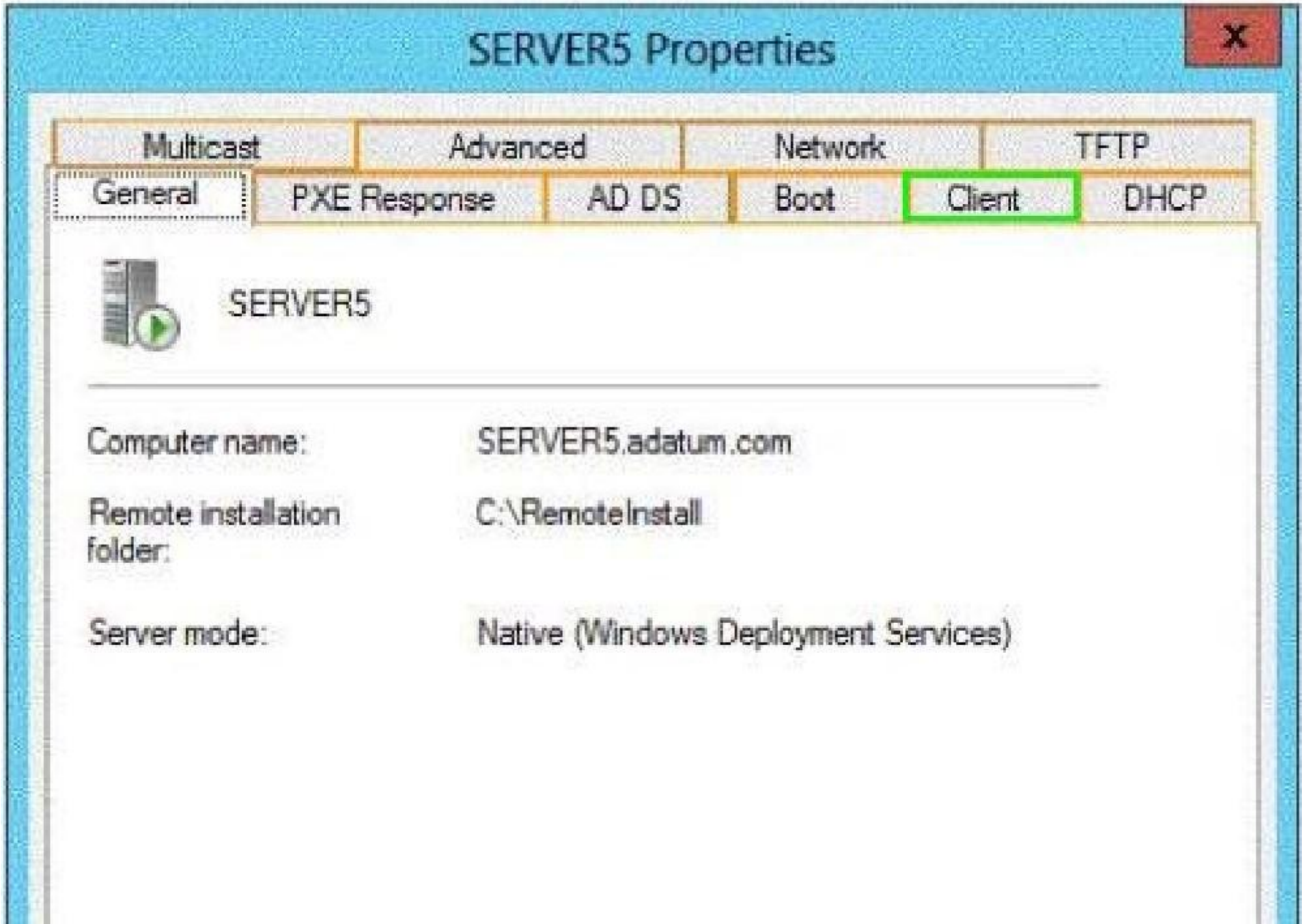

SERVER5 Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
SERVER5
Computer name:
SERVER5.adatum.com
Remote installation folder:
C:\RemoteInstall
Server mode:
Native (Windows Deployment Services)

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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


SERVER5 Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
SERVER5
Computer name:
SERVER5.adatum.com
Remote installation folder:
C:\RemoteInstall
Server mode:
Native (Windows Deployment Services)

QUESTION 189
Your network contains a server named Server1 that has the Network Policy and Access Services server role installed.

All of the network access servers forward connection requests to Server1.

You create a new network policy on Server1.

You need to ensure that the new policy applies only to connection requests from Microsoft RAS servers that are located on the 192.168.0.0/24 subnet.

A. Set the Called Station ID constraint to 192.168.0.0/24
B. Set the Called Station ID constraint to 192.168.0
C. Set the Client IP4 Address condition to 192.168.0.0/24
D. Set the Client IP4 Address condition to 192.168.0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Client IPv4 Address
Specifies the Internet Protocol (IP) version 4 address of the RADIUS client that forwarded the connection request to the NPS server.

QUESTION 190
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. Server1 is configured as a VPN server.

You need to configure Server1 to perform network address translation (NAT).

What should you do?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has the Remote Access server role installed.

DirectAccess is implemented on Server1 by using the default configuration.

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

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

What should you do?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
You have a DNS server named Server1 that runs Windows Server 2012. 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. Mail exchanger (MX)
C. Host information (HINFO)
D. Mailbox (MB)

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

```
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
```

QUESTION 193
You have a server named Server1 that runs Windows Server 2012.

You discover that the performance of Server1 is poor.

The results of a performance report generated on Server1 are shown in the following table.

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

You need to identify the cause of the performance issue.

What should you identify?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012.
An organizational unit (OU) named ResearchServers contains the computer accounts of all research servers.

All domain users are configured to have a minimum password length of eight characters.

You need to ensure that the minimum password length of the local user accounts on the research servers in the ResearchServers OU is 10 characters.

What should you do?

A. Create a universal group that contains the research servers. Create a Password Settings object (PSO) and assign the PSO to the group.
B. Configure a local Group Policy object (GPO) on each research server.
C. Create and link a Group Policy object (GPO) to the ResearchServers OU.
D. Create a global group that contains the research servers. Create a Password Settings object (PSO) and assign the PSO to the group.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195

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

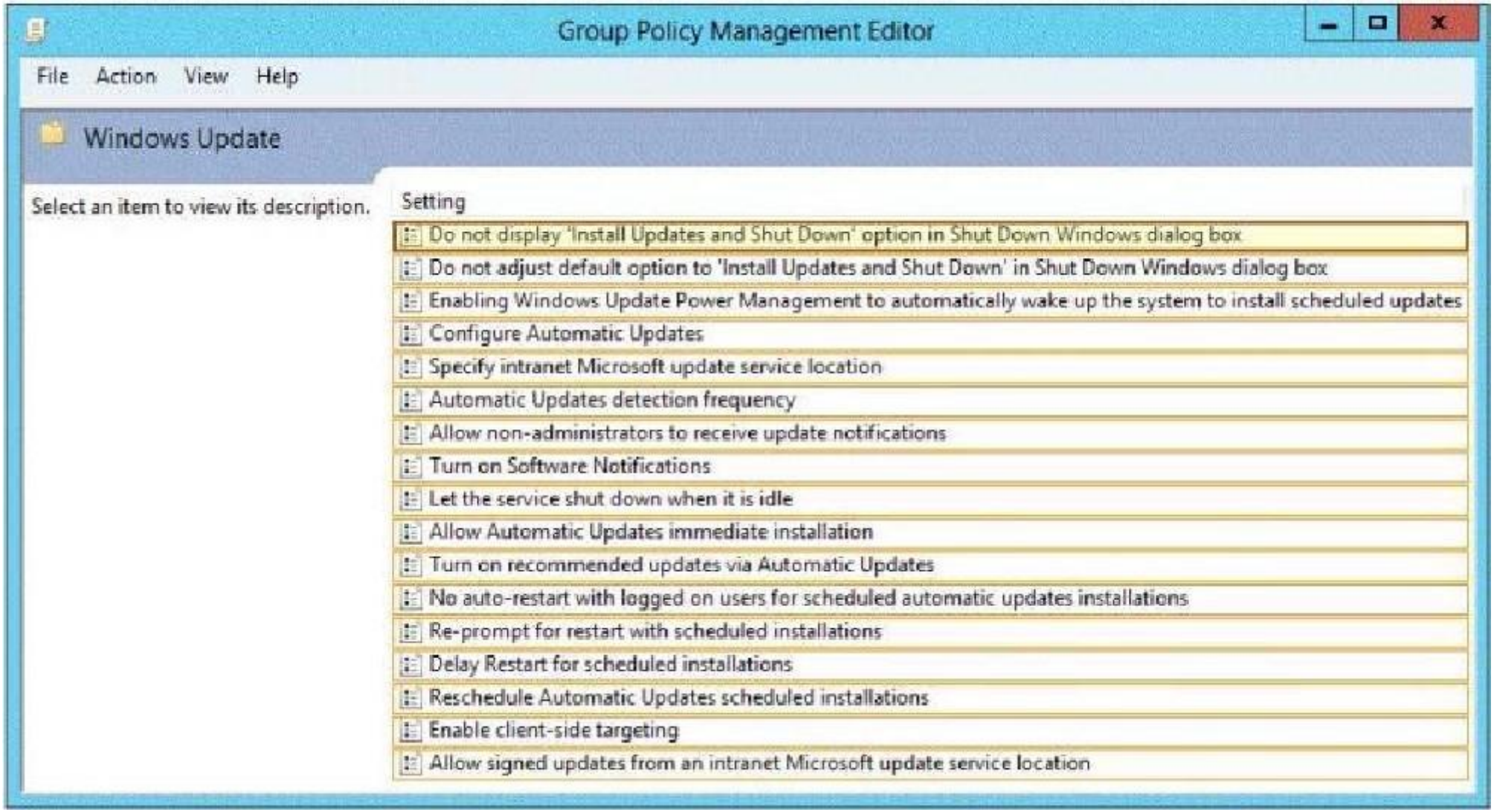
Server1 has the Windows Server Update Services server role installed. All client computers are configured to download updates from Server1.

You have a Group Policy object (GPO) named GPO1 that is linked to an organizational unit (OU) named Sales_OU.

You need to ensure that all of the computers in Sales_OU are added to a Windows Server Update Services (WSUS) computer group named SalesComputers.

Which setting should you configure in the GPO?

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


Group Policy Management Editor
File
Action
View
Help
Windows Update
Select an item to view its description.
Setting
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box
Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates
Configure Automatic Updates
Specify intranet Microsoft update service location
Automatic Updates detection frequency
Allow non-administrators to receive update notifications
Turn on Software Notifications
Let the service shut down when it is idle
Allow Automatic Updates immediate installation
Turn on recommended updates via Automatic Updates
No auto-restart with logged on users for scheduled automatic updates installations
Re-prompt for restart with scheduled installations
Delay Restart for scheduled installations
Reschedule Automatic Updates scheduled installations
Enable client-side targeting
Allow signed updates from an intranet Microsoft update service location

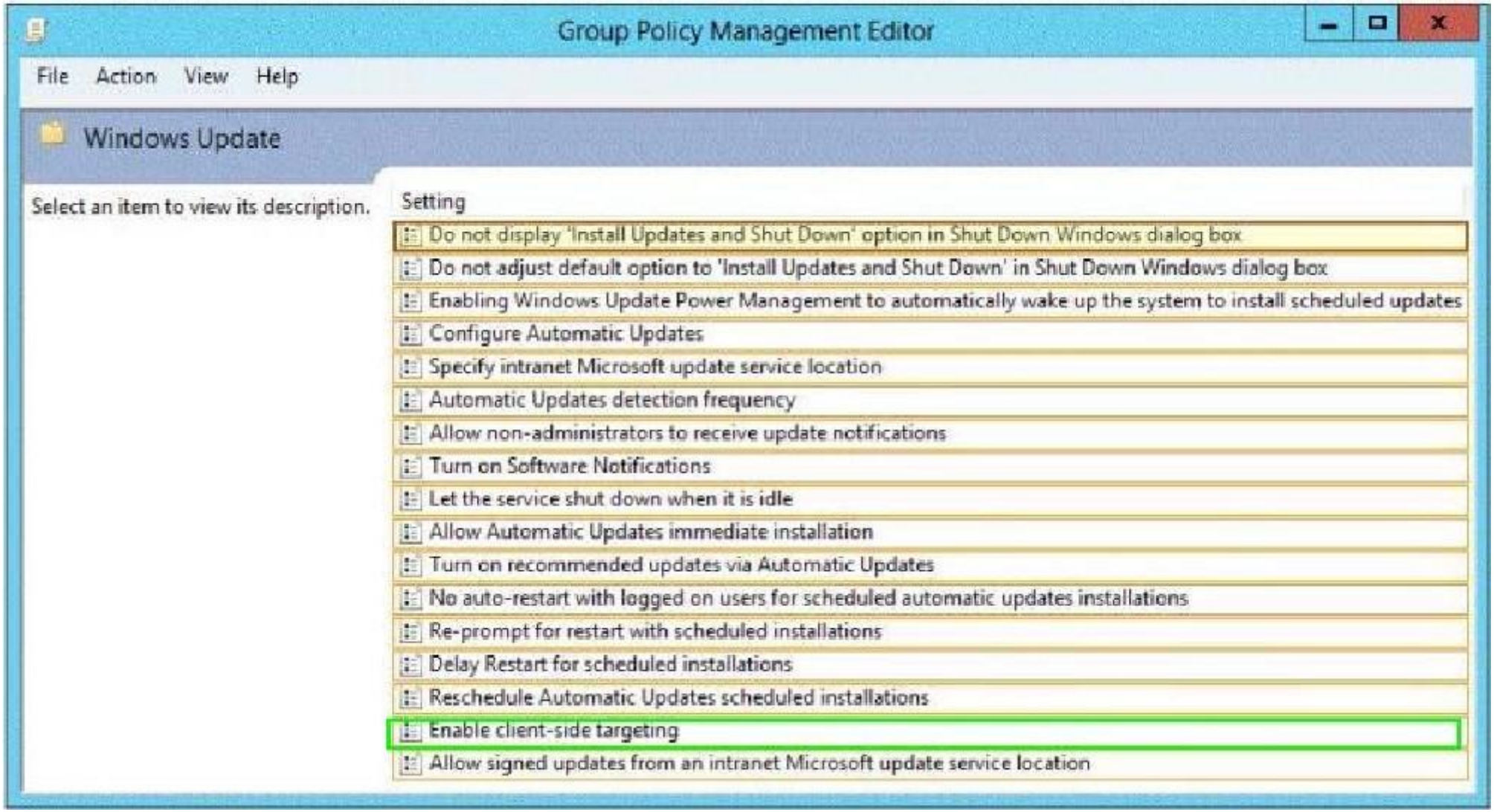
A.
B.
C.

D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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



QUESTION 196
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

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

Internal DNS name: Server1.contoso.com

External DNS name: dal.contoso.com

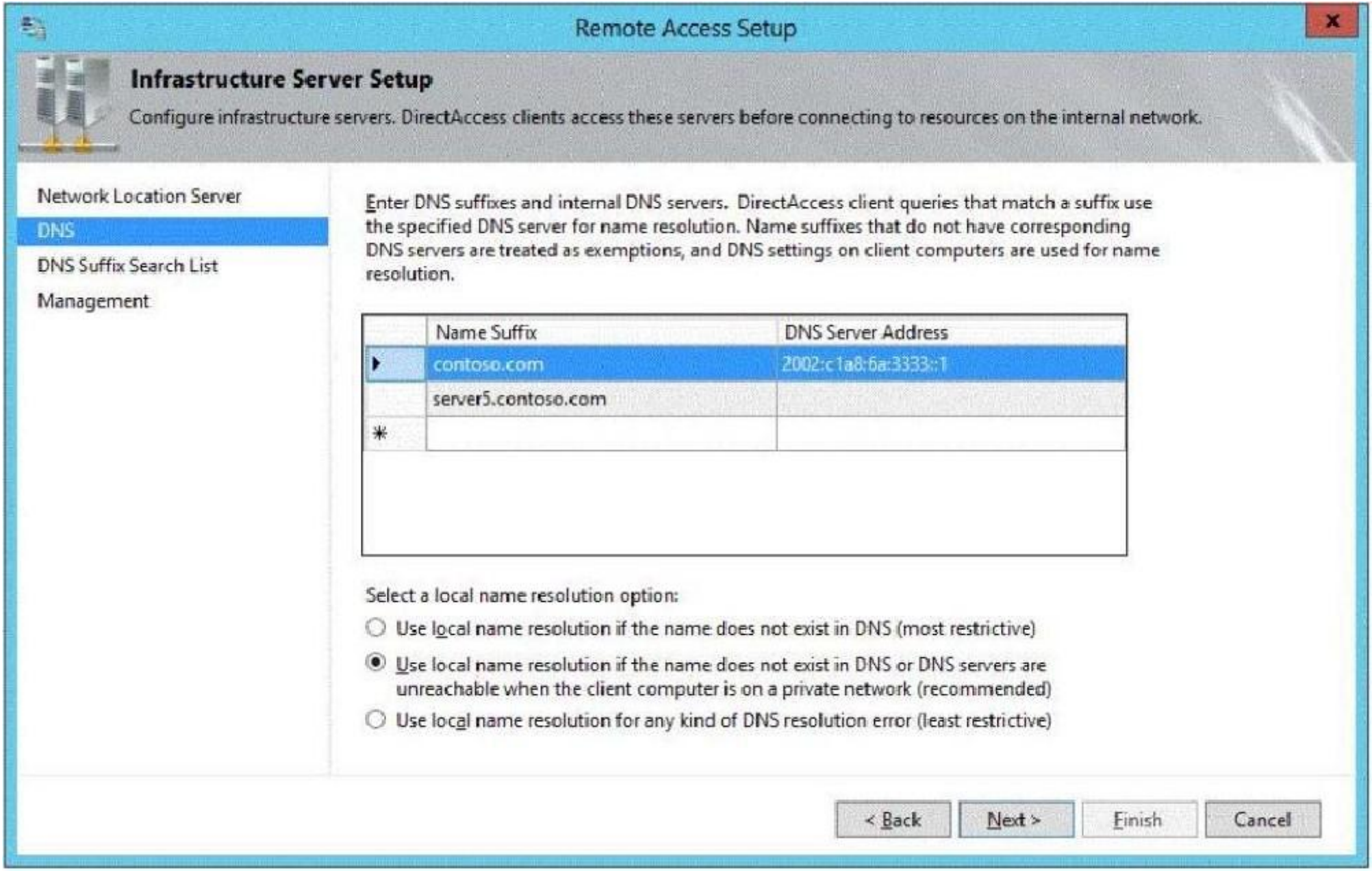
Internal IPv6 address: 2002:c1a8:6a:3333::1

External IPv4 address: 65.55.37.62

Your company uses split-brain DNS for the contoso.com zone.

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

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



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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012.

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

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

You need to add a system variable named App1Data to all of the client computers.

Which Group Policy preference should you configure?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

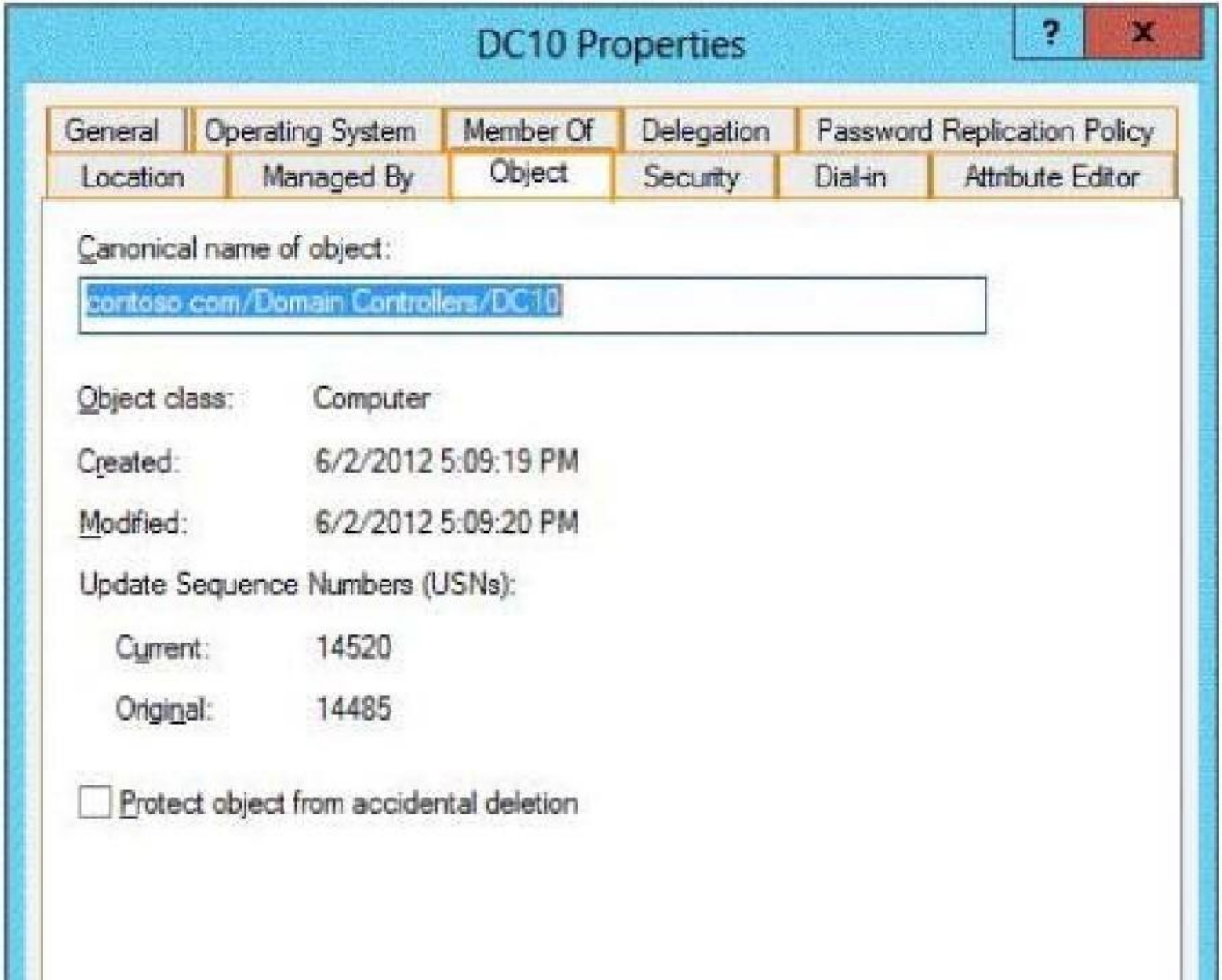
QUESTION 198
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. The forest contains two Active Directory sites named Site1 and Site2.

You plan to deploy a read-only domain controller (RODC) named DC10 to Site2. You pre- create the DC10 domain controller account by using Active Directory Users and Computers.

You need to identify which domain controller will be used for initial replication during the promotion of the RODC.

Which tab should you use to identify the domain controller?

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

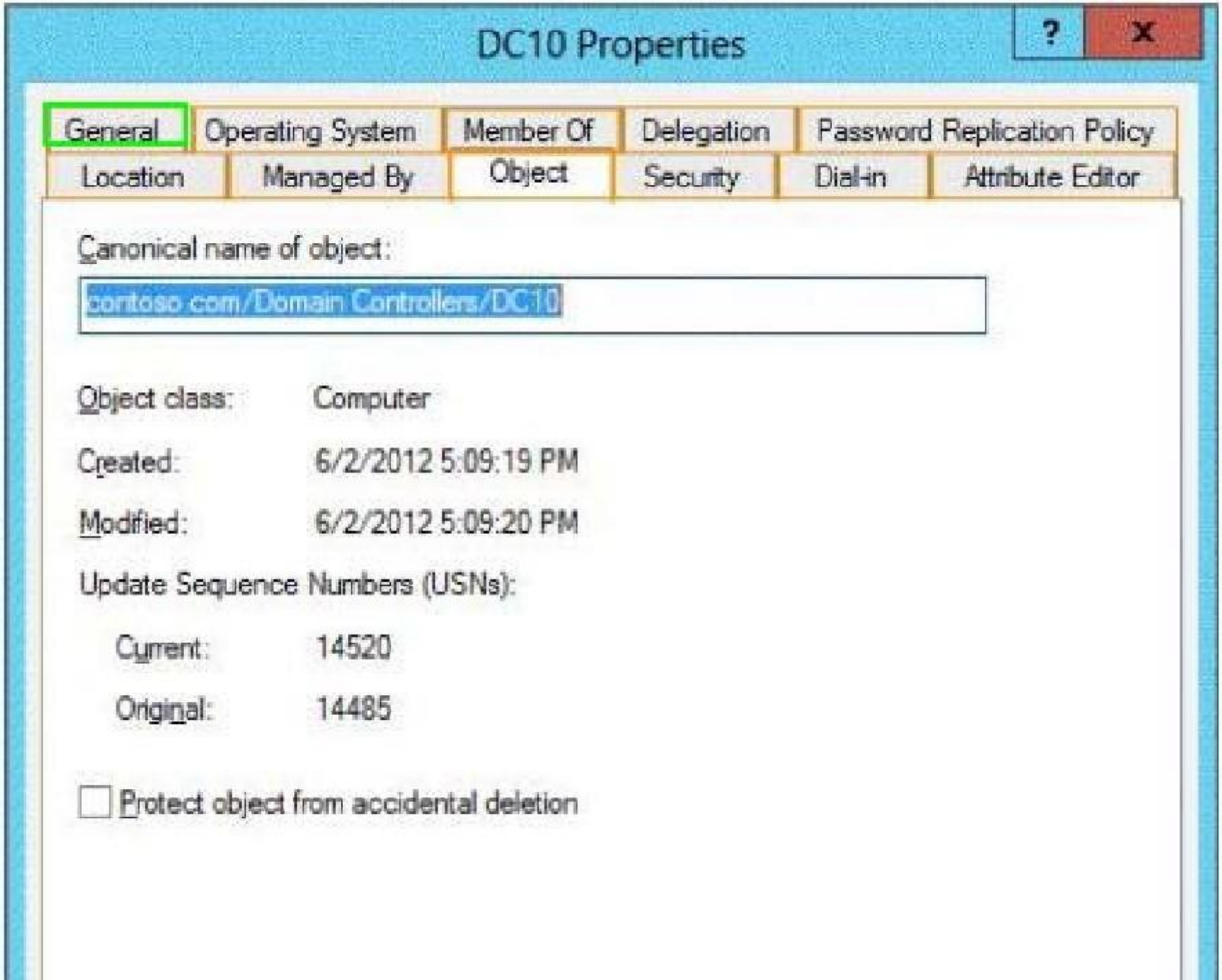

DC10 Properties
?
X
General
Operating System
Member Of
Delegation
Password Replication Policy
Location
Managed By
Object
Security
Dial-in
Attribute Editor
Canonical name of object:
contoso.com/Domain Controllers/DC10
Object class: Computer
Created: 6/2/2012 5:09:19 PM
Modified: 6/2/2012 5:09:20 PM
Update Sequence Numbers (USNs):
Current: 14520
Original: 14485
Protect object from accidental deletion

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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


DC10 Properties
?
X
General
Operating System
Member Of
Delegation
Password Replication Policy
Location
Managed By
Object
Security
Dial-in
Attribute Editor
Canonical name of object:
contoso.com/Domain Controllers/DC10
Object class: Computer
Created: 6/2/2012 5:09:19 PM
Modified: 6/2/2012 5:09:20 PM
Update Sequence Numbers (USNs):
Current: 14520
Original: 14485
Protect object from accidental deletion

QUESTION 199
Your network contains an Active Directory forest named contoso.com.

Recently, all of the domain controllers that ran Windows Server 2003 were replaced by domain controllers that run Windows Server 2012.

From Event Viewer, you discover SYSVOL journal wrap errors on a domain controller named dc10.contoso.com.

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

Which three actions should you perform on DC10?

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

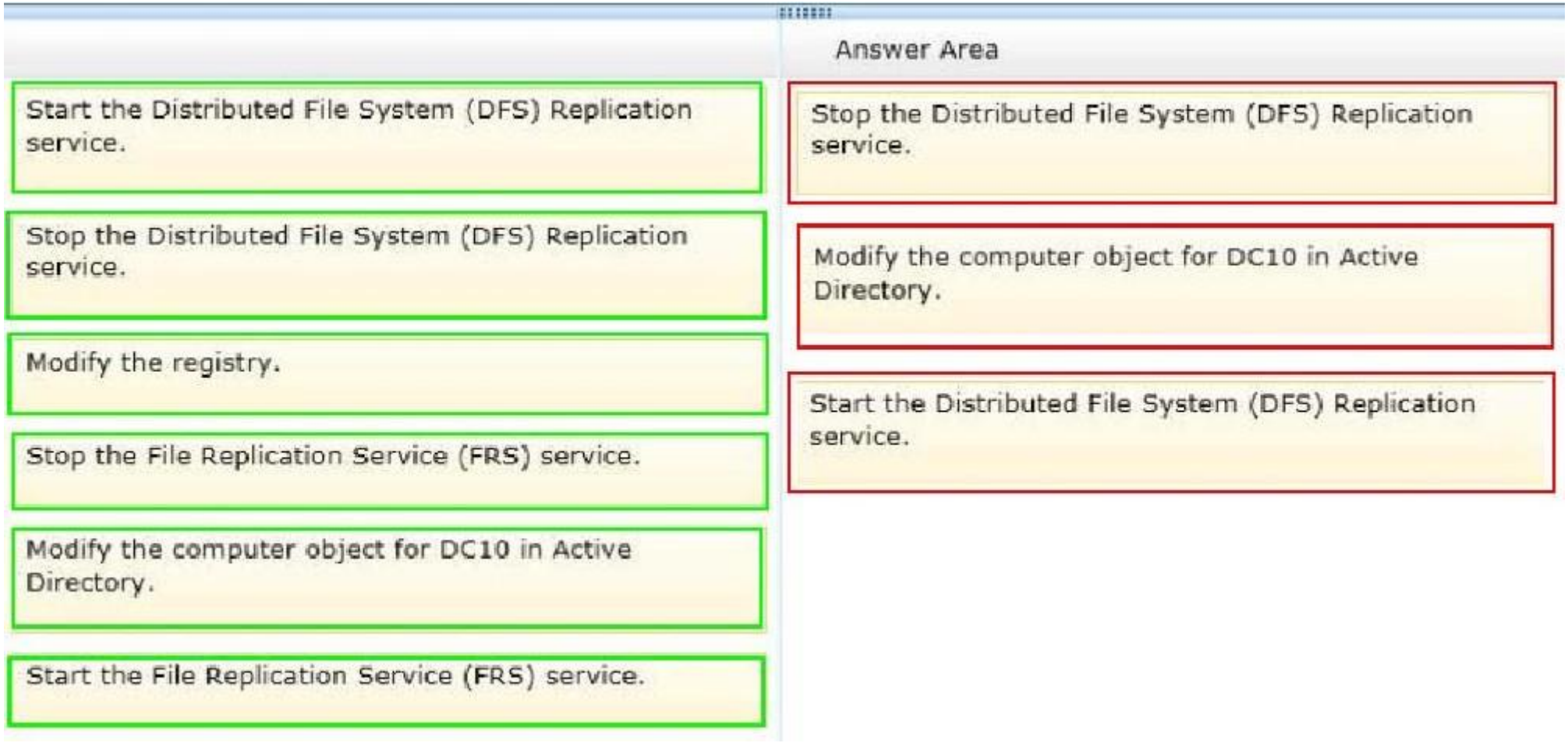
www.vceplus.com - Website designed to help IT pros advance their careers.

	Answer Area
Start the Distributed File System (DFS) Replication service.	
Stop the Distributed File System (DFS) Replication service.	
Modify the registry.	
Stop the File Replication Service (FRS) service.	
Modify the computer object for DC10 in Active Directory.	
Start the File Replication Service (FRS) service.	

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



QUESTION 200
You manage a server that runs Windows Server 2012. The server has the Windows Deployment Services server role installed.

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

```
Hyper-V
PXE Network Boot 09.14.2011
(C) Copyright 2011 Microsoft Corporation, All Rights Reserved.


CLIENT MAC ADDR: 00 15 5D 00 0F 13  GUID: 979708BF-C04B-4525-9FE0-C4150BB6C618
DHCP.-
```

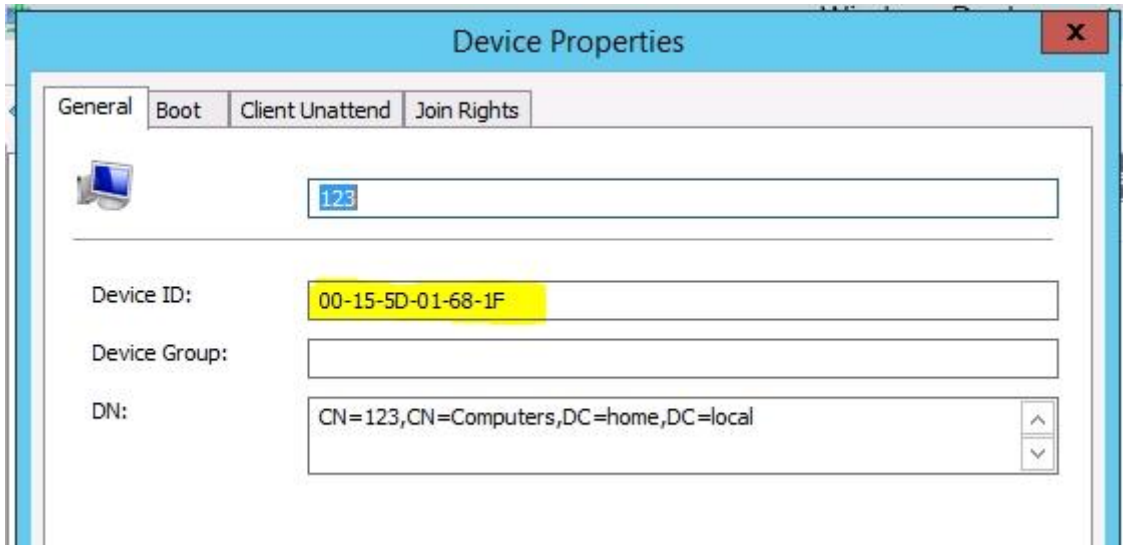
You need to configure a pre-staged device for VM1 in the Windows Deployment Services console.

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

A. 979708BFC04B45259FE0C4150BB6C618
B. 979708BF-C04B-4525-9FE0-C4150BB6C618
C. 00155D000F1300000000000000000000
D. 00000000000000000000000155D000F13
E. 00000000-0000-0000-0000-C4150BB6C618

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
When you pre-staged with 00000000000000000000000155D01681F it will let you do it but after will show at Device-ID just the mac address....



QUESTION 201
Your company has a main office and a branch office.

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

The main office contains a domain controller named DC1 that runs Windows Server 2012.
DC1 is a DNS server and hosts a primary zone for contoso.com.

The branch office contains a member server named Server1 that runs Windows Server 2012.
Server1 is a DNS server and hosts a secondary zone for contoso.com.

The main office connects to the branch office by using an unreliable WAN link.

You need to ensure that Server1 can resolve names in contoso.com if the WAN link in unavailable for three days.

Which setting should you modify in the start of authority (SOA) record?

A. Retry interval
B. Minimum (default) TTL
C. Refresh interval
D. Expires after

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 runs Windows Server 2012 and has the Windows Deployment Services (WDS) server role installed.

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

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

A. Install
B. Boot
C. Discover
D. Capture

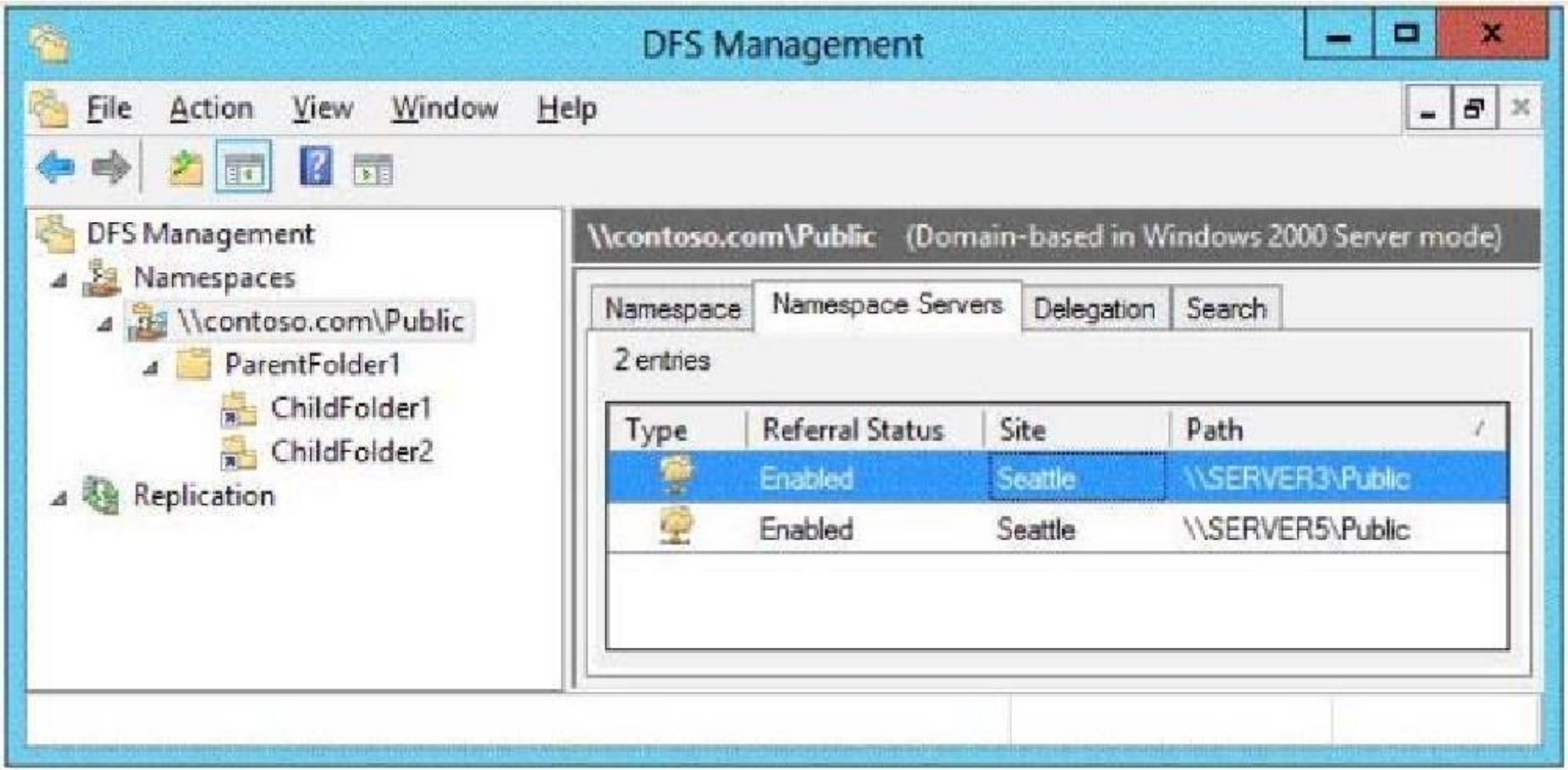
Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012. 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. Install the File Server Resource Manager role service on Server3 and Server5.
B. Raise the domain functional level.
C. Delete and recreate the namespace.

D. Raise the forest functional level.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

The domain contains two organizational units (OUs) named OU1 and OU2 in the root of the domain.

Two Group Policy objects (GPOs) named GPO1 and GPO2 are created. GPO1 is linked to OU1. GPO2 is linked to OU2.

OU1 contains a client computer named Computer1. OU2 contains a user named User1.

You need to ensure that the GPOs applied to Computer1 are applied to User1 when User1 logs on.

What should you configure?

A. The GPO Status
B. GPO links
C. The Enforced setting
D. Security Filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: * GPOs cannot be linked directly to users, computers, or security groups. They can only be linked to sites, domains and organizational units. However, by using security filtering, you can narrow the scope of a GPO so that it applies only to a single group, user, or computer.

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

Reference: Security filtering using GPMC

QUESTION 205
Your company deploys a new Active Directory forest named contoso.com. The first domain controller in the forest runs Windows Server 2012. The forest contains a domain controller named DC10.

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

You replace the failed disk. You stop the Distributed File System (DFS) Replication service.
You restore the SYSVOL folder.
You need to perform a non-authoritative synchronization of SYSVOL on DC10.

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

A. Dfsgui.msc
B. Replmon
C. Adsiedit.msc
D. Ultrasound

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: How to perform a non-authoritative synchronization of DFSR-replicated SYSVOL (like "D2" for FRS)
In the ADSIEDIT.MSC tool modify the following distinguished name (DN) value and attribute on each of the domain controllers that you want to make non-authoritative:CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR- LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain>msDFSR-Enabled=FALSE
Force Active Directory replication throughout the domain. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:DFSRDIAG POLLAD You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated.
On the same DN from Step 1, set:msDFSR-Enabled=TRUE Force Active Directory replication throughout the domain. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:DFSRDIAG POLLAD You will see Event ID 4614 and 4604 in the DFSR event log indicating SYSVOL has been initialized. That domain controller has now done a "D2" of SYSVOL.

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

Incorrect:
A: Dfsgui is for ealier versions of Windows Server.
B: Replmon is for Windows 2003 and earlier.

Reference: How to force an authoritative and non-authoritative synchronization for DFSR- replicated SYSVOL (like "D4/D2" for FRS)

QUESTION 206
Your network contains a Hyper-V host named Server1 that hosts 20 virtual machines.

You need to view the amount of memory resources and processor resources each virtual machine uses currently.

Which tool should you use on Server1?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Topic 5, Volume E

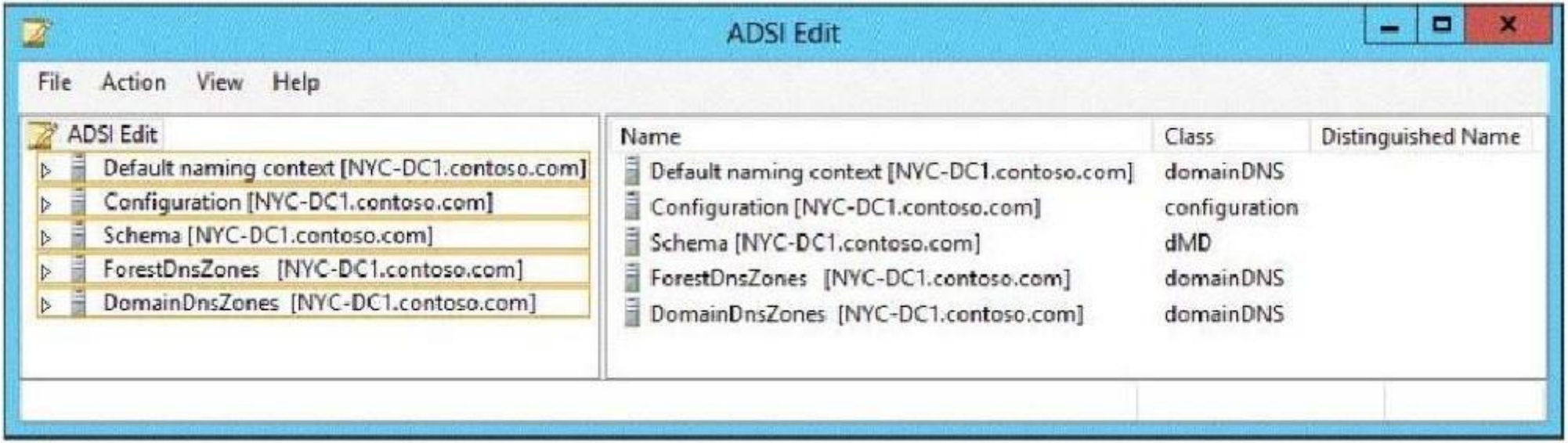
QUESTION 207
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. The contoso.com zone is Active Directory-integrated and configured to replicate to all of the domain controllers in the contoso.com domain.

Server1 has a DNS record in the contoso.com zone.

You need to verify when the DNS record for Server1 was last updated.

In which Active Directory partition should you view the DNS record of Server1?

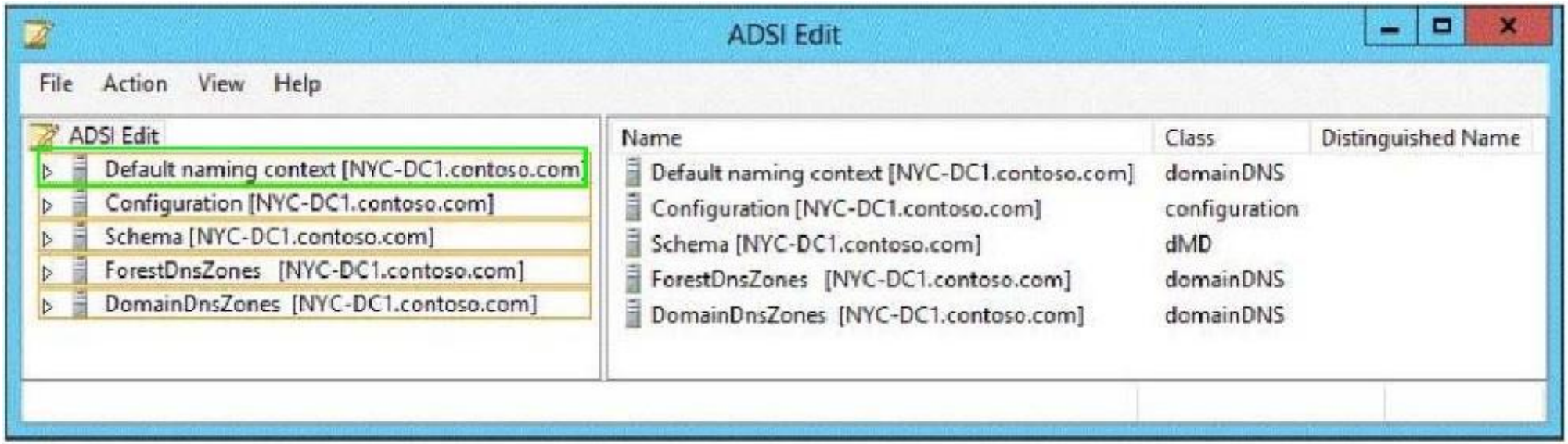
To answer, select the appropriate Active Directory partition in the answer area.



A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



QUESTION 208
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.

Server1 has the Windows Server Update Services (WSUS) server role installed. WSUS is configured to use a Windows Internal Database.

Server2 has Microsoft SQL Server 2008 R2 Standard deployed.

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

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

What should you do on Server1?

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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 209
Your network contains an Active Directory forest named contoso.com. The functional level of the forest is Windows Server 2008 R2.

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

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

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

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

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

You need to tell User1 what her minimum password length is.

What should you tell User1?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012. Server1 has the Remote Access server role installed.

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

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

Configure Remote Access

Configure Remote Access

Getting Started Wizard

This server does not comply with some DirectAccess prerequisites. Resolve all issues before proceeding with DirectAccess deployment. For more information, see Checklist: Before you configure DirectAccess.

Check prerequisites again

Warning The current user does not have the required permissions to configure WMI filtering in the domain. Verify permissions.

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

A. Enterprise Admins
B. Domain Admins
C. Server Operators
D. Account Operators

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012. 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.lx deployment.

Which authentication method should you identify?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

The domain contains an organizational unit (OU) named OU1. OU1 contains an OU named OU2. OU2 contains a user named User1.
User1 is the member of a group named Group1. Group1 is in the Users container.

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

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

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

Which three GPOs should you identify in sequence?

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

Actions	Answer Area
GPO1	
GPO2	
GPO4	
GPO5	

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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

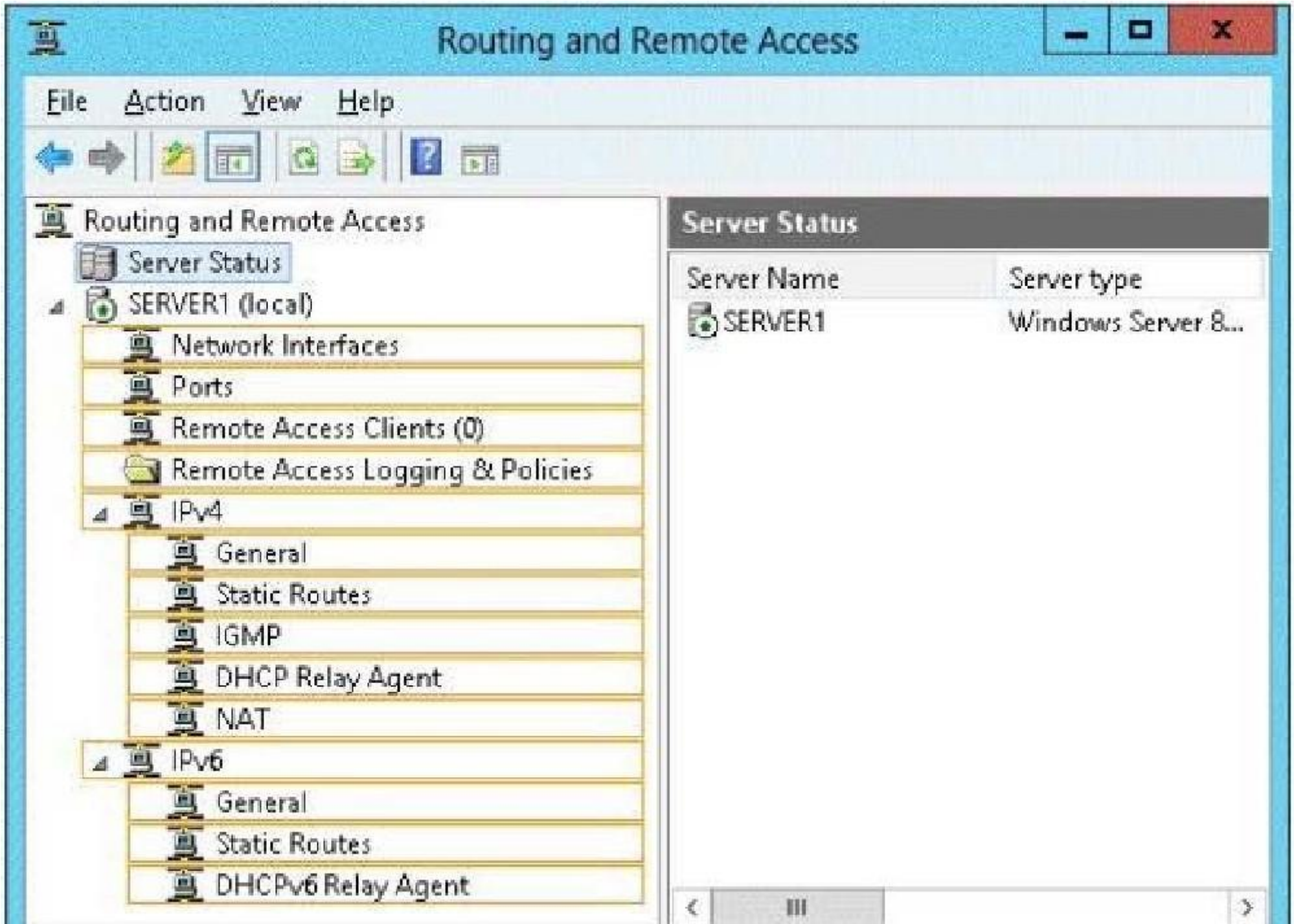
Actions	Answer Area
GPO1	GPO1
GPO2	GPO3
GPO4	GPO4
GPO5	

QUESTION 213
You have a server named Server1 that runs Windows Server 2012. Server1 has two network adapters and is located in a perimeter network.

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

Which node should you use to add the RIP version 2 routing protocol?

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

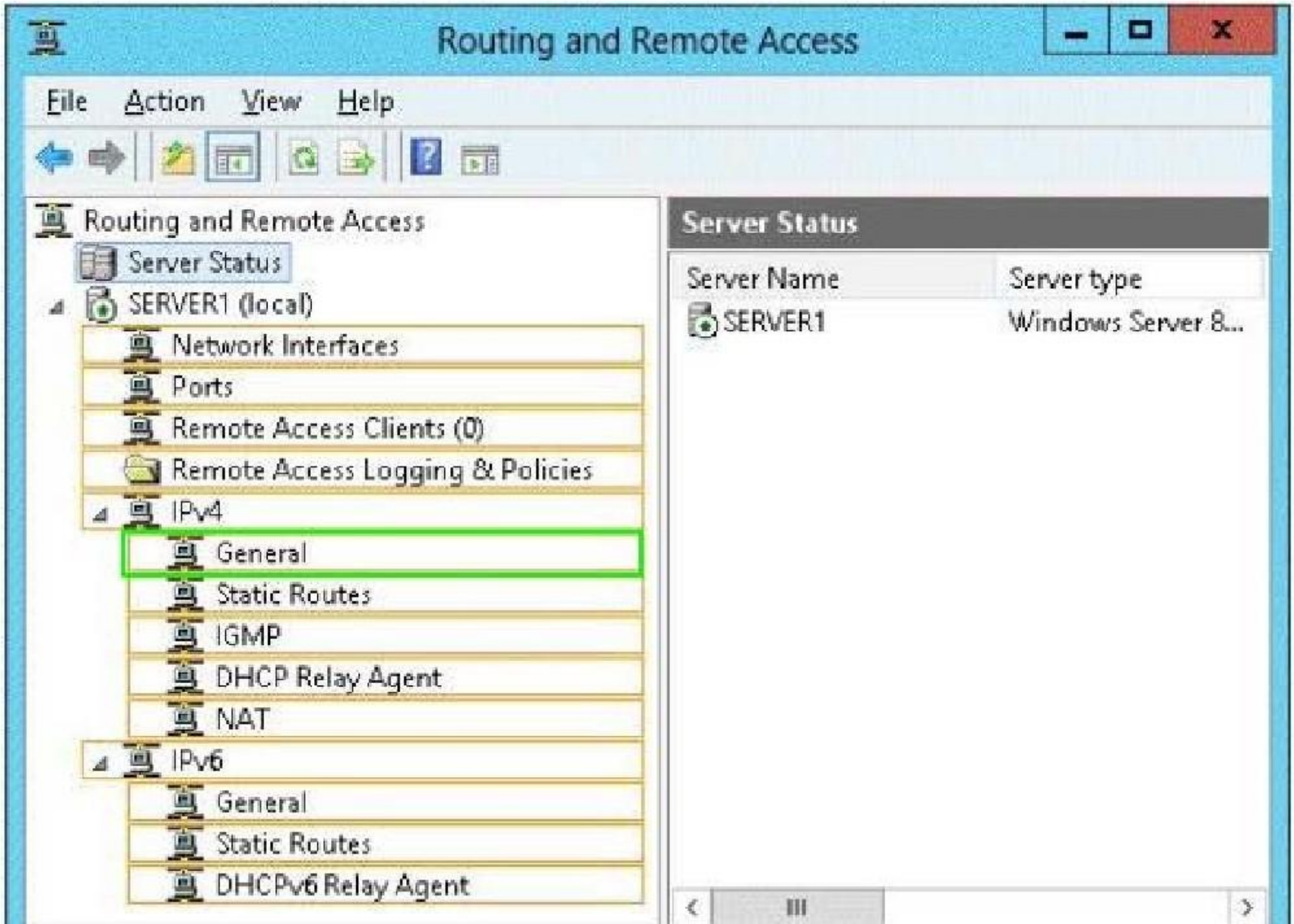

Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
SERVER1 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
Static Routes
IGMP
DHCP Relay Agent
NAT
IPv6
General
Static Routes
DHCPv6 Relay Agent
Server Status
Server Name
Server type
SERVER1
Windows Server 8...

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
SERVER1 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
Static Routes
IGMP
DHCP Relay Agent
NAT
IPv6
General
Static Routes
DHCPv6 Relay Agent
Server Status
Server Name
Server type
SERVER1
Windows Server 8...

QUESTION 214
Your network contains an Active Directory domain named contoso.com.

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

An administrator modifies the start of authority (SOA) record for the adatum.com zone.

After the modification, you discover that when you add or modify DNS records in the adatum.com zone, the changes are not transferred to the DNS servers that host secondary copies of the adatum.com zone.

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

What should you modify in the SOA record for the adatum.com zone?

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

adatum.com Properties

Name Servers | WINS | Zone Transfers

General | Start of Authority (SOA)

Serial number:

251 | Increment

Primary server:

server1.contoso.com. | Browse...

Responsible person:

hostmaster.contoso.com. | Browse...

Refresh interval:	15	minutes
Retry interval:	10	minutes
Expires after:	1	days
Minimum (default) TTL:	1	hours

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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

adatum.com Properties

Name Servers | WINS | Zone Transfers

General | Start of Authority (SOA)

Serial number:

251 Increment

Primary server:

server1.contoso.com. Browse...

Responsible person:

hostmaster.contoso.com. Browse...

Refresh interval:	15	minutes
Retry interval:	10	minutes
Expires after:	1	days
Minimum (default) TTL:	1	hours

QUESTION 215
Your network contains an Active Directory domain named contoso.com. The domain controllers in the domain are configured as shown in the following table.

Domain controller name	Operating system	Operation master role
DC1	Windows Server 2008	PDC emulator Infrastructure master RID master
DC2	Windows Server 2008 R2	Schema master Domain naming master

You deploy a new domain controller named DC3 that runs Windows Server 2012.

You discover that you cannot create Password Settings objects (PSOs) by using Active Directory Administrative Center.

You need to ensure that you can create PSOs from Active Directory Administrative Center.

What should you do?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Step 1: Create a PSO

Applies To: **Windows Server 2008**, Windows Server 2008 R2

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

QUESTION 216
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012. The domain contains 200 Group Policy objects (GPOs) and 100 WMI filters.

An administrator named Admin1 must be able to create new WMI filters and edit all of the existing WMI filters from the Group Policy Management Console (GPMC).

You need to delegate the required permissions to Admin1. The solution must minimize the number of permissions assigned to Admin1. What should you do?

A. From Group Policy Management, assign Full control to Admin1 for the WMI Filters container.
B. From Active Directory Users and Computers, add Admin1 to the Domain Admins group.
C. From Group Policy Management, assign Creator Owner to Admin1 for the WMI Filters container.
D. From Active Directory Users and Computers, add Admin1 to the WinRMRemoteWMIUsers__group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012. 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. Domain local groups
B. Computers
C. Universal groups
D. Global groups
E. Users

Correct Answer: DE

Section: (none)
Explanation

Explanation/Reference:
Explanation: Fine-grained password policies apply only to user objects (or inetOrgPerson objects if they are used instead of user objects) and global security groups.
Reference: AD DS: Fine-Grained Password Policies

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

QUESTION 218
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1 that runs Windows Server 2012.

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. Environment
D. Data Sources

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
Your network contains an Active Directory domain named contoso.com. The domain contains a file server named Server1 that runs Windows Server 2012. Server1 has a share named Share1.

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

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

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

What should you install on Server2?

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

Correct Answer: B
Section: (none)
Explanation

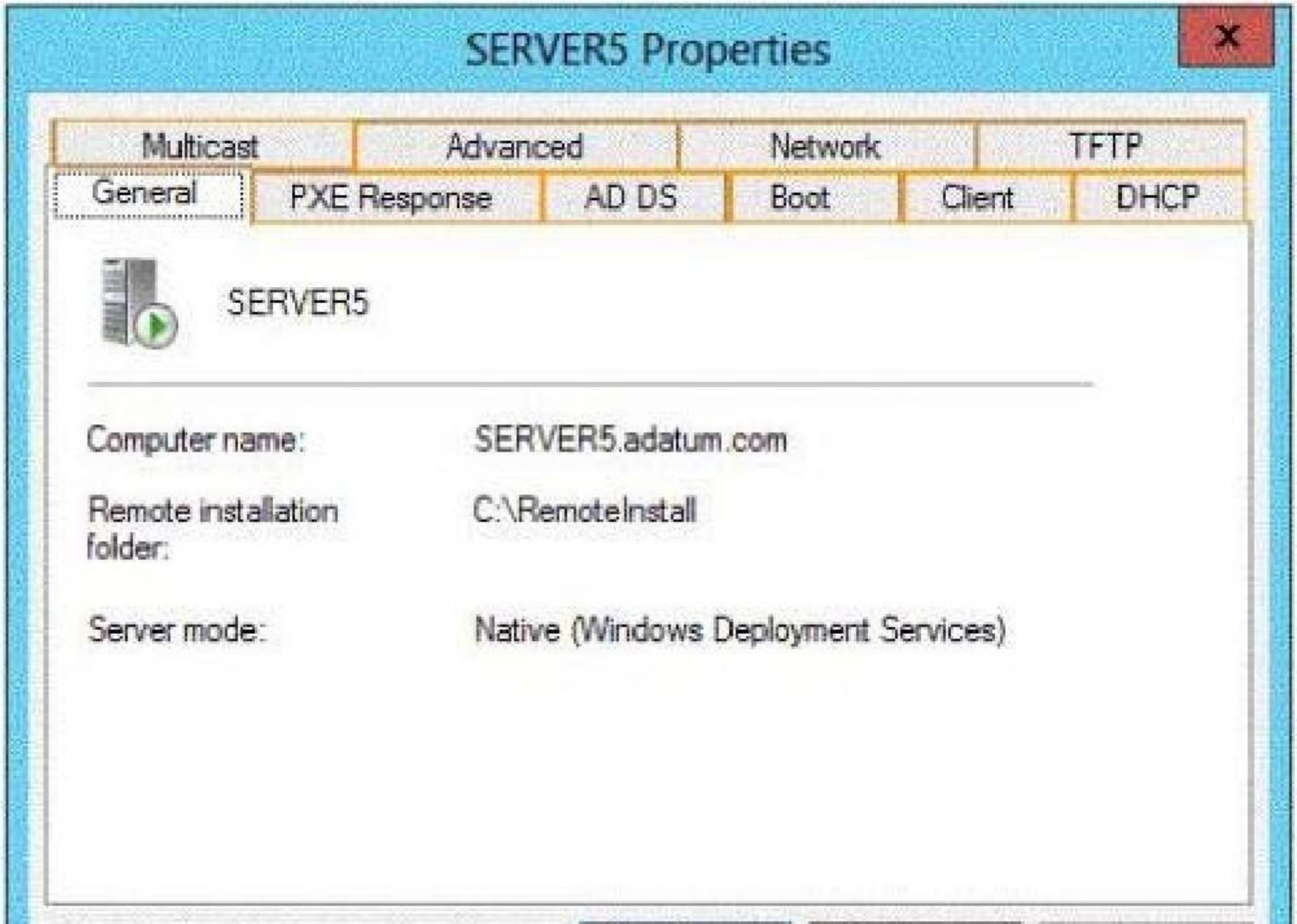
Explanation/Reference:

QUESTION 220
You have a server named Server5 that runs Windows Server 2012. Servers has the Windows Deployment Services server role installed.

Server5 contains several custom images of Windows 8.

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

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

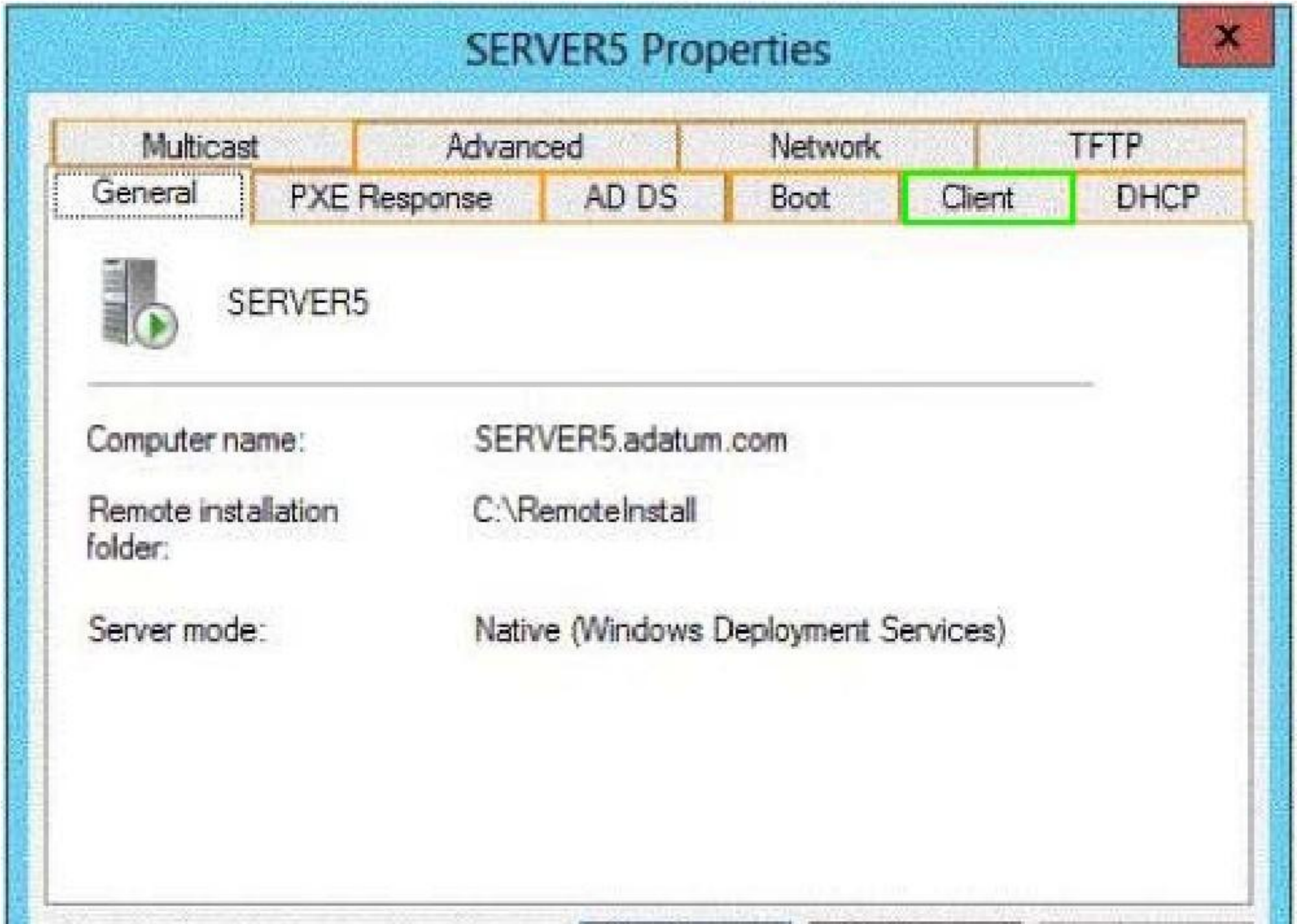

SERVER5 Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
SERVER5
Computer name:
SERVER5.adatum.com
Remote installation folder:
C:\RemoteInstall
Server mode:
Native (Windows Deployment Services)

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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


SERVER5 Properties
Multicast
Advanced
Network
TFTP
General
PXE Response
AD DS
Boot
Client
DHCP
SERVER5
Computer name:
SERVER5.adatum.com
Remote installation folder:
C:\RemoteInstall
Server mode:
Native (Windows Deployment Services)

QUESTION 221
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

The domain contains two organizational units (OUs) named OU1 and OU2 in the root of the domain.

Two Group Policy objects (GPOs) named GPO1 and GPO2 are created. GPO1 is linked to OU1. GPO2 is linked to OU2.

OU1 contains a client computer named Computer1. OU2 contains a user named User1.

You need to ensure that the GPOs applied to Computer1 are applied to User1 when User1 logs on.

What should you configure?

A. Block Inheritance
B. The GPO Status
C. The Enforced setting
D. GPO links

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: A GPO can be associated (linked) to one or more Active Directory containers, such as a site, domain, or organizational unit. Multiple containers can be linked to the same GPO, and a single container can have more than one GPO linked to it. If multiple GPOs are linked to one container, you can prioritize the order in which GPOs are applied.
Linking GPOs to Active Directory containers enables an administrator to implement Group Policy settings for a broad or narrow portion of the organization, as required.

QUESTION 222
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

The domain contains two organizational units (OUs) named OU1 and OU2 in the root of the domain.

Two Group Policy objects (GPOs) named GPO1 and GPO2 are created. GPO1 is linked to OU1. GPO2 is linked to OU2.

OU1 contains a client computer named Computer1. OU2 contains a user named User1.

You need to ensure that the GPOs applied to Computer1 are applied to User1 when User1 logs on.

What should you configure?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: A GPO can be associated (linked) to one or more Active Directory containers, such as a site, domain, or organizational unit. Multiple containers can be linked to the same GPO, and a single container can have more than one GPO linked to it. If multiple GPOs are linked to one container, you can prioritize the order in which GPOs are applied.
Linking GPOs to Active Directory containers enables an administrator to implement Group Policy settings for a broad or narrow portion of the organization, as required.

QUESTION 223
Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012.

Administrators use client computers that run Windows 8 to perform all management tasks.

A central store is configured on a domain controller named DC1.

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

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

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

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

What should you do?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 and has the Network Policy Server role service installed.

You need to enable trace logging for Network Policy Server (NPS) on Server1.

Which tool should you use?

A. the Network Policy Server console
B. the Server Manager console
C. the tracert.exe command
D. the netsh.exe command

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

To create tracing log files on a server running NPS

1. Open a command line as an administrator.
2. Type **netsh ras set tr * en**.
3. Reproduce the scenario that you are troubleshooting.
4. Type **netsh ras set tr * dis**.
5. Close the command prompt window.

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

QUESTION 225
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 and has the DNS Server server role installed.

Server1 is configured to delete automatically the DNS records of client computers that are no longer on the network. A technician confirms that the DNS records are deleted automatically from the contoso.com zone.

You discover that the contoso.com zone has many DNS records for servers that were on the network in the past, but have not connected to the network for a long time.

You need to set the time stamp for all of the DNS records in the contoso.com zone.
What should you do?

A. From DNS Manager, modify the Advanced settings from the properties of Server1.
B. From Windows PowerShell, run the Set-DnsServerResourceRecordAging cmdlet.
C. From DNS Manager, modify the Zone Aging/Scavenging Properties.
D. From Windows PowerShell, run the Set-DnsServerZoneAging cmdlet.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
You have a server named Server1 that runs Windows Server 2012.

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. an event trace data collector
D. a performance counter data collector

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
Your network contains an Active Directory domain named contoso.com. The domain contains three member servers named Server1, Server2, and Server3. All servers run Windows Server 2012 and have the Windows Server Update Services (WSUS) server role installed.

Server1 and Server2 are configured as replica servers that use Server3 as an upstream server. You remove Server3 from the network.

You need to ensure that WSUS on Server2 retrieves updates from Server1.

The solution must ensure that Server1 and Server2 have the latest updates from Microsoft.

Which command should you run on each server? To answer, select the appropriate command to run on each server in the answer area.

Server1

set-wsusserversynchronization –syncfrommu
set-wsusserversynchronization –useservername server1
set-wsusserversynchronization –useservername server2
wsusutil.exe movecontent \\server1\c$
wsusutil.exe movecontent \\server2\c$

Server2

set-wsusserversynchronization –syncfrommu
set-wsusserversynchronization –useservername server1
set-wsusserversynchronization –useservername server2
wsusutil.exe movecontent \\server1\c$
wsusutil.exe movecontent \\server2\c$

A.

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

B.

C.

D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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

Server1

- set-wsusserversynchronization –syncfrommu
- set-wsusserversynchronization –useservername server1
- set-wsusserversynchronization –useservername server2
- wsusutil.exe movecontent \\server1\c$
- wsusutil.exe movecontent \\server2\c$

Server2

- set-wsusserversynchronization –syncfrommu
- set-wsusserversynchronization –useservername server1
- set-wsusserversynchronization –useservername server2
- wsusutil.exe movecontent \\server1\c$
- wsusutil.exe movecontent \\server2\c$

QUESTION 228

Your network contains an Active Directory domain named contoso.com. Network Access Protection (NAP) is deployed to the domain.

You need to create NAP event trace log files on a client computer.

What should you run?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

To create NAP event trace log files on a client computer

1. Open a command line as an administrator.
2. Type **logman start QAgentRt -p {b0278a28-76f1-4e15-b1df-14b209a12613} 0xFFFFFFFF 9 -o %systemroot%\tracing\nap\QAgentRt.etl –ets**.

   Note

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

3. Reproduce the scenario that you are troubleshooting.
4. Type **logman stop QAgentRt -ets**.
5. Close the command prompt window.

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

QUESTION 229
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 and has the Network Policy Server role service installed.

An administrator creates a RADIUS client template named Template1.

You create a RADIUS client named Client1 by using Template1.

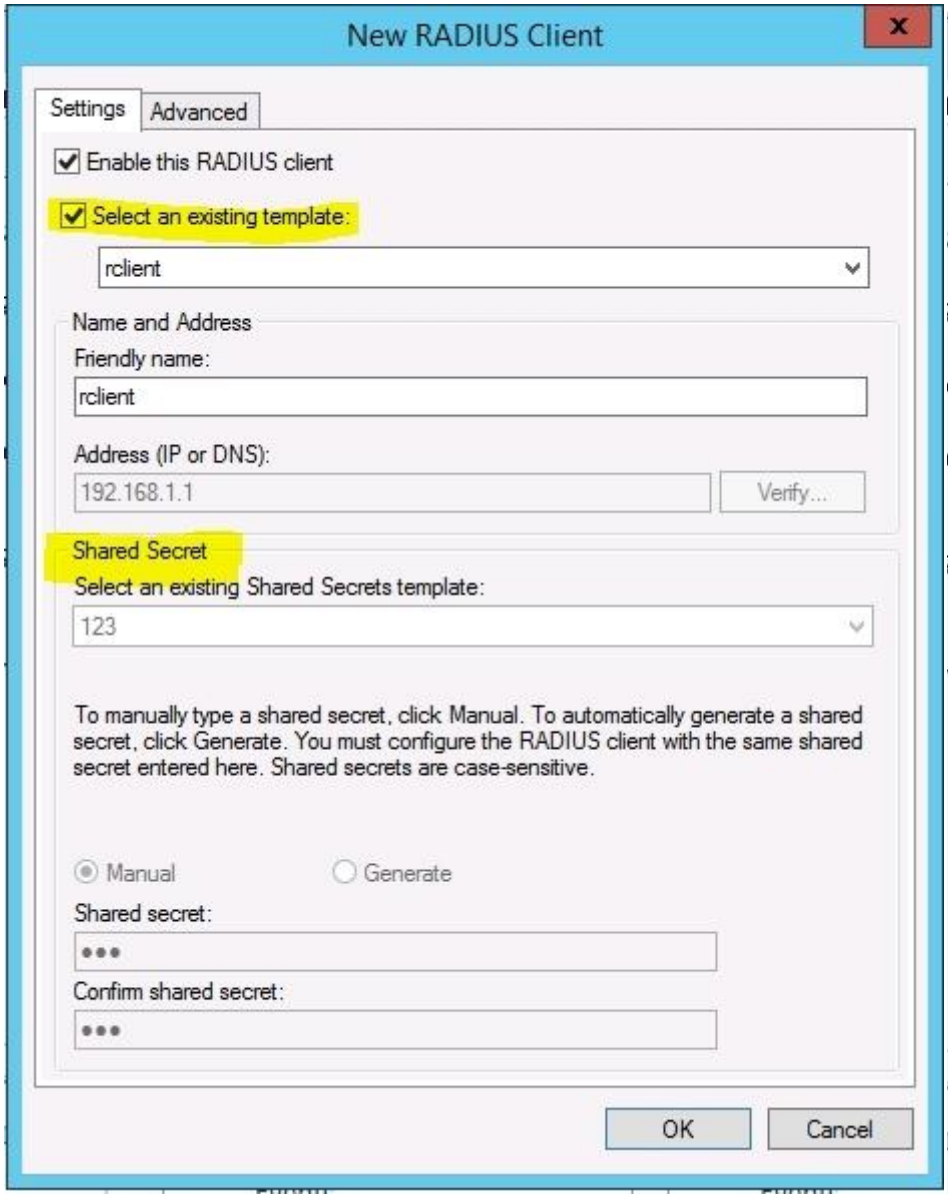
You need to modify the shared secret for Client1.

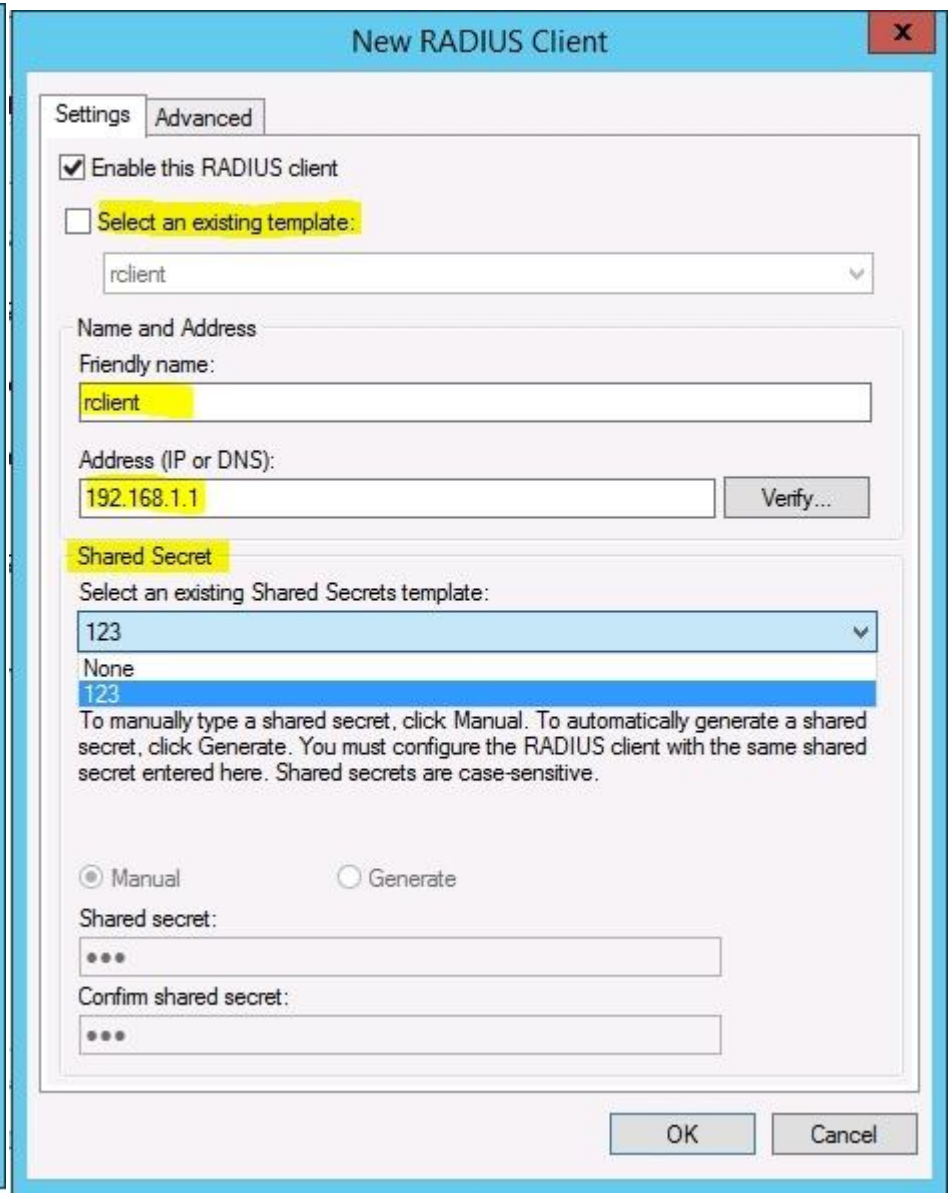
What should you do first?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:





QUESTION 230

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.

For Server2, you are configuring constrained delegation to a third-party service named Service1 on Server1.

When you attempt to add Service1 from Server1 to the delegation setting of Server2, you discover that Service1 is not listed in the Available services list.

You need to ensure that you can add Service1 for constrained delegation.

What should you do first?

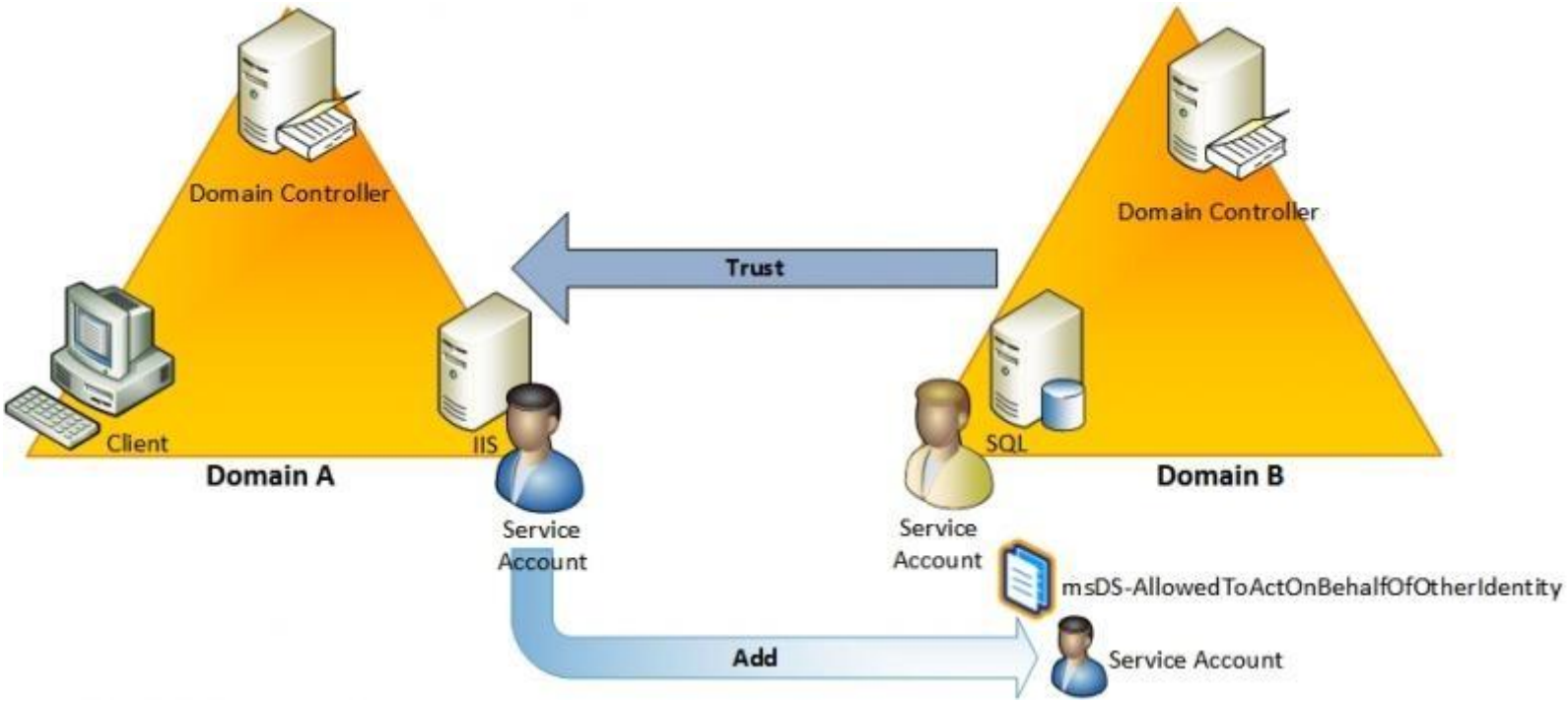
A. From the Services console, modify the properties of Service1.
B. From ADSI Edit, create a serviceConnectionPoint (SCP) object.
C. From a command prompt, run the setspn.exe command.
D. From Active Directory Users and Computers, enable the Advanced Features option.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
What Is Constrained Delegation?
Constrained delegation lets you limit the back-end services for which a front-end service can request tickets on behalf of another user.

Kerberos constrained delegation has been a part of the OS since Windows Server 2003. It requires you to configure an allow list of service principal names (SPNs) on user or computer objects in Active Directory (AD). You add the list of SPNs that represent the back-end services to which a front-end service is allowed to request tickets on behalf of the user to the ms-DS-Allowed-To-Delegate-To attribute of the principal under which the application or service on the front-end server runs.

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



http://windowsitpro.com/security/how-windows-server-2012-eases-pain-kerberos-constrained-delegation-part-1
http://technet.microsoft.com/en-us/library/cc720385%28v=ws.10%29.aspx

QUESTION 231
You have a file server named Server1 that runs Windows Server 2012. Server1 has the File Server Resource Manager role service installed.

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

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

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

What should you configure on Task1?

A. Create a custom action.

B. Configure a file screen.
C. Create a classification rule.
D. Create a condition.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
Your network contains two DNS servers named Server1 and Server2 that run Windows Server 2012. Server1 hosts a primary zone for contoso.com. Server2 hosts a secondary zone forcontoso.com.

You need to ensure that Server2 replicates changes to the contoso.com zone every five minutes.

Which setting should you modify in the start of authority (SOA) record?

A. Retry interval
B. Minimum (default) TTL
C. Expires after
D. Refresh interval

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

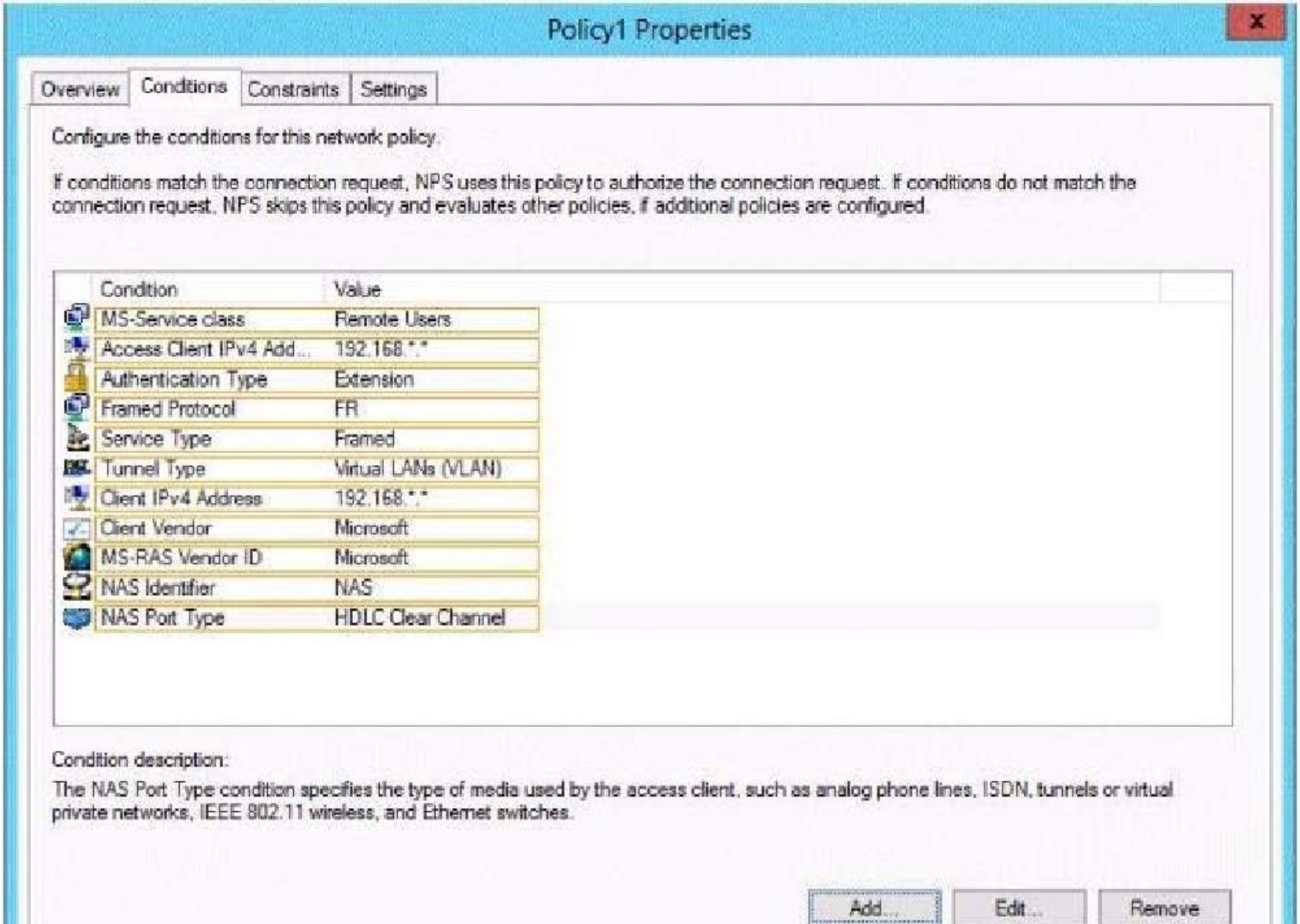
QUESTION 233
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2012 and has the Network Policy Server role service installed.

An administrator creates a Network Policy Server (NPS) network policy named Policy1.

You need to ensure that Policy1 applies to L2TP connections only.

Which condition should you modify? To answer, select the appropriate object in the answer area.

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

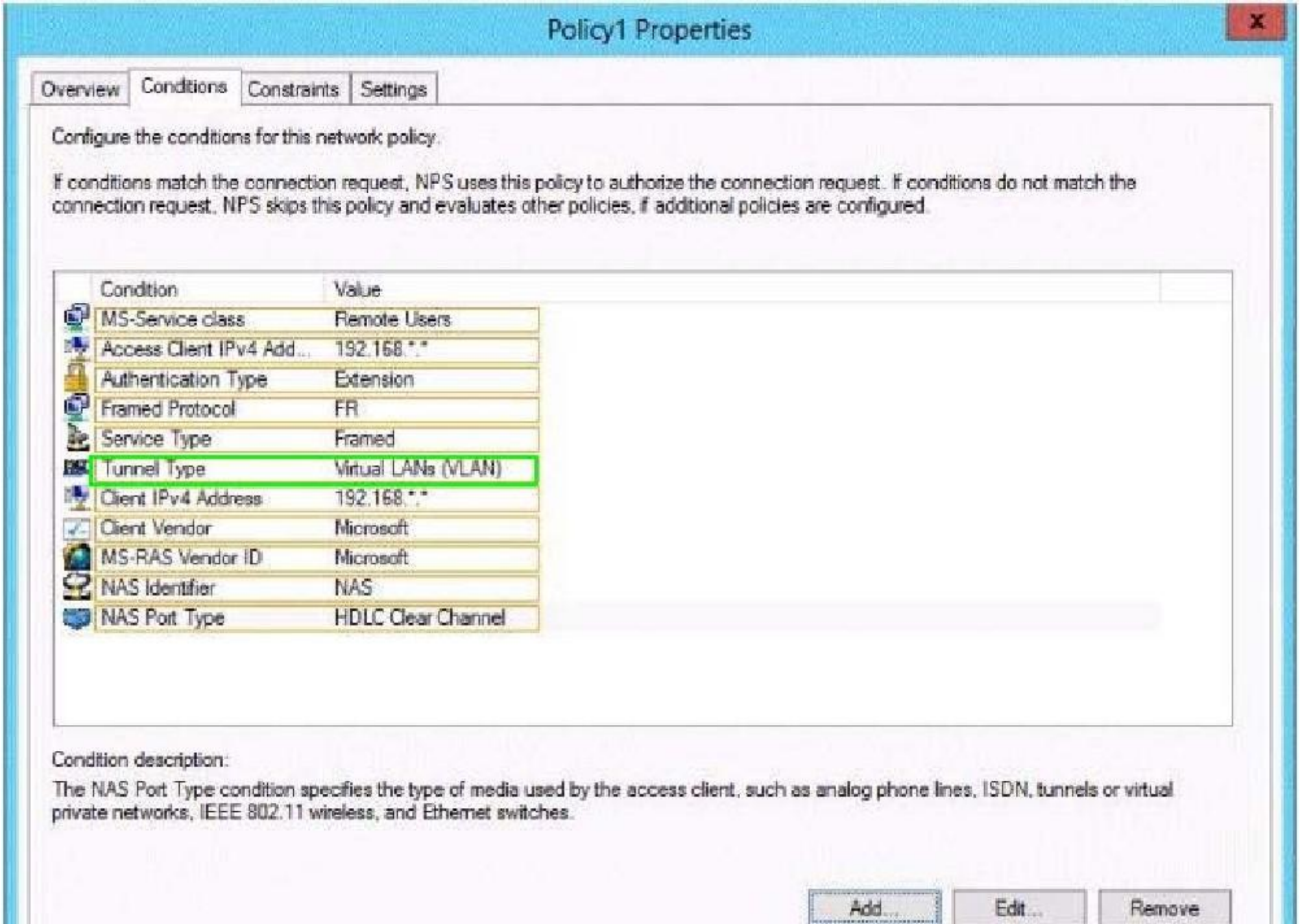

Policy1 Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
MS-Service class
Remote Users
Access Client IPv4 Add...
192.168.*.*
Authentication Type
Extension
Framed Protocol
FR
Service Type
Framed
Tunnel Type
Virtual LANs (VLAN)
Client IPv4 Address
192.168.*.*
Client Vendor
Microsoft
MS-RAS Vendor ID
Microsoft
NAS Identifier
NAS
NAS Port Type
HDLC Clear Channel
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.
Add...
Edit...
Remove

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

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


Policy1 Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
MS-Service class
Remote Users
Access Client IPv4 Add...
192.168.*.*
Authentication Type
Extension
Framed Protocol
FR
Service Type
Framed
Tunnel Type
Virtual LANs (VLAN)
Client IPv4 Address
192.168.*.*
Client Vendor
Microsoft
MS-RAS Vendor ID
Microsoft
NAS Identifier
NAS
NAS Port Type
HDLC Clear Channel
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.
Add...
Edit...
Remove

QUESTION 234
Your network contains two servers named Server1 and Server 2. Both servers run Windows Server 2012 and have the DNS Server server role installed.

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

You plan to create a standard primary zone for ad.contoso.com on Server2.

You need to ensure that Server1 forwards all queries for ad.contoso.com to Server2.

What should you do from Server1?

A. Create a trust anchor named Server2.
B. Create a conditional forward that points to Server2.
C. Create a zone delegation that points to Server2.
D. Add Server2 as a name server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
You have a DNS server named DN51 that runs Windows Server 2012.

On DNS1, you create a standard primary DNS zone named adatum.com.

You need to change the frequency that secondary name servers will replicate the zone from DNS1.

Which type of DNS record should you modify?

A. start of authority (SOA)
B. name server (NS)
C. service location (SRV)
D. host information (HINFO)

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 236
how can you manage your virtual vms via hyper v ?

A. task manager
B. via hyper advisor
C. operation manager
D. performance logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

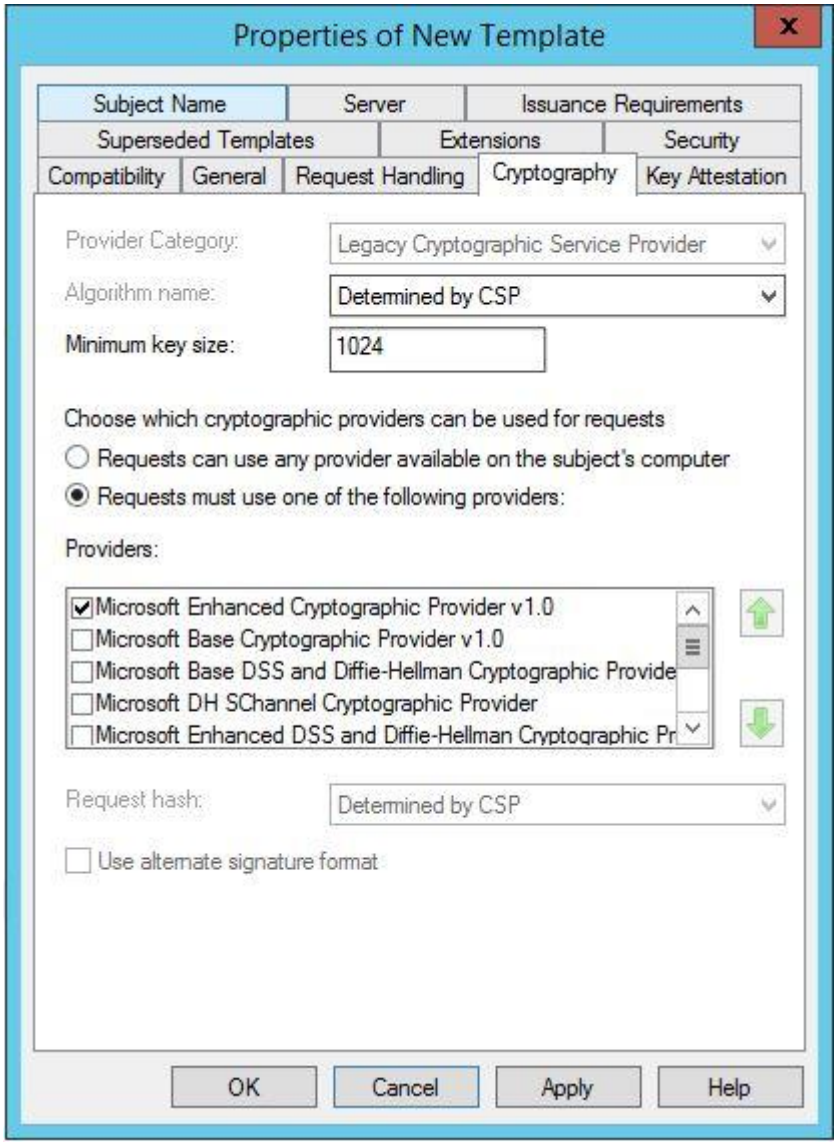
QUESTION 237
Your network contains an Active Directory domain named contoso.com.

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

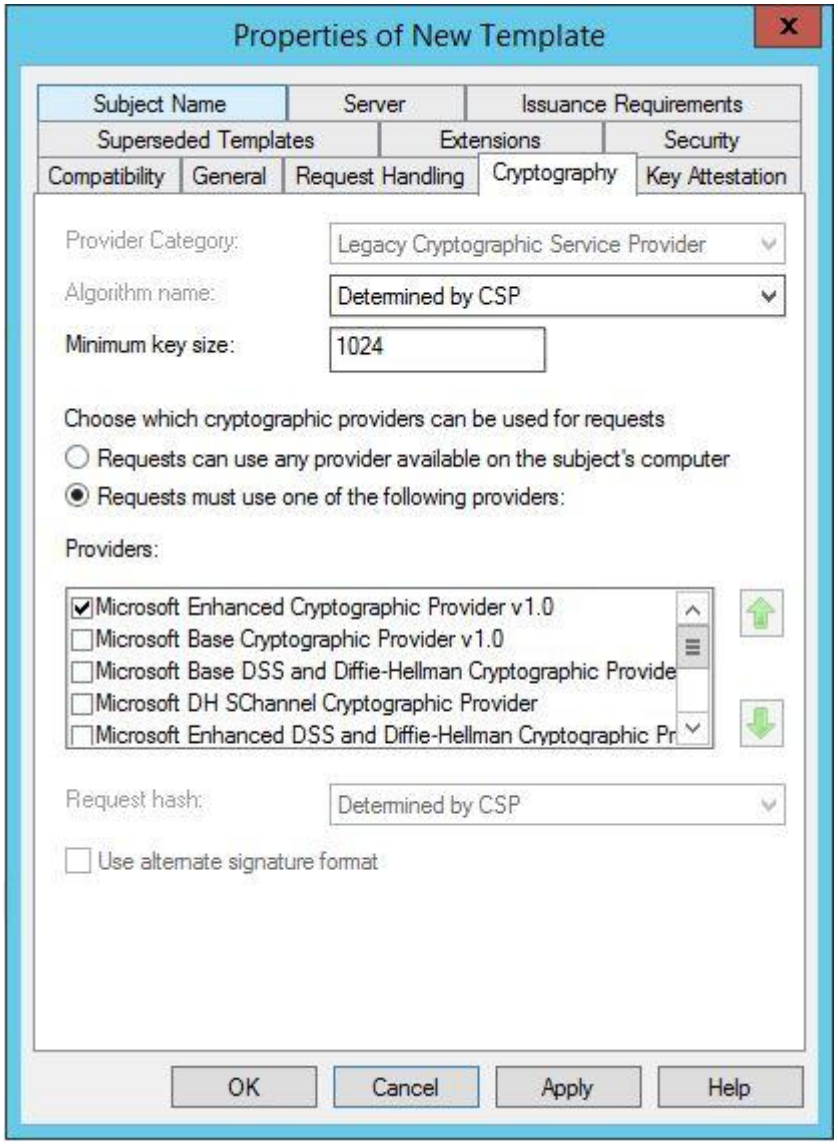
Which Cryptography setting of the certificate template should you modify?

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

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Create a certificate template for Network Unlock, which the Active Directory CA can use to create and issue the Network Unlock certificates.

New features: Network Unlock

Another new feature in the Windows 8 and Server 2012 version of BitLocker is network unlock. This feature is aimed at enterprise environments, specifically at systems that belong to a Windows domain. What it does is automatically unlock BitLocker-protected drives when the computer is rebooted if it is connected to the corporate network (this must be a wired connection, not a wi-fi or remote connection).

This avoids the problem of users forgetting their PINs or USB keys, when they're connected to the trusted network (the assumption being that if they are physically on premises with Ethernet plugged in, they are probably the authorized users). It also makes it easier to roll out patches and other updates to unattended desktops that are BitLocker-protected. Of course this is an optional configuration; for better security, organizations can still require that the PIN be entered (and/or USB key inserted) to access the protected drives even when on the corporate network.
Network unlock prerequisites

There are some prerequisites before you can implement network unlock. The BitLocker-protected system must be using UEFI firmware (not legacy BIOS) and it needs to have a DHCP driver in the firmware. The network must have a Windows Server 2012 server operating in the WDS (Windows Deployment Services) role and also a DHCP server that is separate from the WDS server (and separate from the domain controller). Group policy must be configured for network unlock, and the network unlock feature itself must be installed on the Windows Server 2012 server. You do this through Server Manager or with PowerShell; the feature name is BitLocker Network Unlock.

Network unlock uses public key cryptography and a network key that is stored on the system drive. It and a session key that uses 256 bit AES are stored together. The key is encrypted with a 2048 bit RSA public key.
How network unlock works

The client computer's boot manager detects the network unlock key protector. Key protectors are the means by which BitLocker keys are protected, such as a password or PIN, a key file, a smart card, certificate, etc. When the client detects this protector, it uses DHCP (hence the requirement for a DHCP drive in UEFI) to get an IPv4 IP address. Then it sends out a DHCP request with the encrypted network key and session key.

The server has to have a **2048 bit** RSA key pair and the clients need to have the public key. The certificate is deployed through the Group Policy Editor on the domain controller. The WDS server decrypts the request with the RSA private key. Then it sends the network key back, encrypted with the session key (also using DHCP).

What happens if the WDS server isn't available or doesn't return the proper key? In that case, the user will be prompted to use the protector that it's configured to use when not on the corporate network (e.g., TPM + PIN). The user will be able to unlock the BitLocker-protected drive in the standard way.

6. Select the **Cryptography** tab. Set the **Minimum key size** to 2048. (Any Microsoft cryptographic provider that supports RSA can be used for this template, but for simplicity an
Provider.)

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

QUESTION 238
Your network contains an Active Directory forest named contoso.com. All servers run Windows Server 2012.

You need to create a custom Active Directory application partition.

Which tool should you use?

A. Dsadd
B. Dsmod
C. Netdom
D. Dnscmd

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
DnsCmd ServerName /CreateDirectoryPartition FQDN of partition

http://wiki.answers.com/Q/How_do_you_create_a_new_application_partition