DUMPSARENA

Administering Windows Server 2012

Microsoft 70-411

Version Demo

Total Demo Questions: 15

Total Premium Questions: 305

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	96
Topic 2, Volume B	209
Total	305

QUESTION NO: 1

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

You have a desktop computer that has the following configuration:

- Computer name: Computer1
- Operating system: Windows 8
- MAC address: 20-CF-30-65-D0-87
- GUID: 979708BF-C04B-4525-9FE0-C4150BB6C618

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

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

A. 20CF3065D0870000000000000000000

B. 979708BFC04B45259FE0C4150BB6C618

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

D. 000000000000000000020CF306SD087

E. 00000000-0000-0000-0000-C41S0BB6C618

ANSWER: C D

Explanation:

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

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

* Example: Remove a device by using its ID from a specified domain This command removes the pre-staged device that has the specified ID. Thecmdlet searches the domain named TSQA.contoso.com for the device.

Windows PowerShell

PS C:\> Remove-WdsClient -DeviceID "5a7a1def-2e1f-4a7b-a792-ae5275b6ef92" -Domain -DomainName "TSQA.contoso.com"

QUESTION NO: 2

Your network contains an Active Directory domain named adatum.com. The domain has a certification authority (CA) named CA1.

All servers run Windows Server 2012 R2. All client computers run Windows 10.

You need to add a data recovery agent for the Encryption File System (EFS) to the domain.

What should you do?

A. From the Default Domain Controllers Policy, select Add Data Recovery Agent.

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 the Default Domain Policy, select Create Data Recovery Agent.

ANSWER: C

Explanation:

References: https://msdn.microsoft.com/library/cc875821.aspx#EJAA

QUESTION NO: 3

Your network contains two DNS servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 hosts a primary zone for contoso.com. Server2 hosts a secondary zone for contoso.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. Expires after

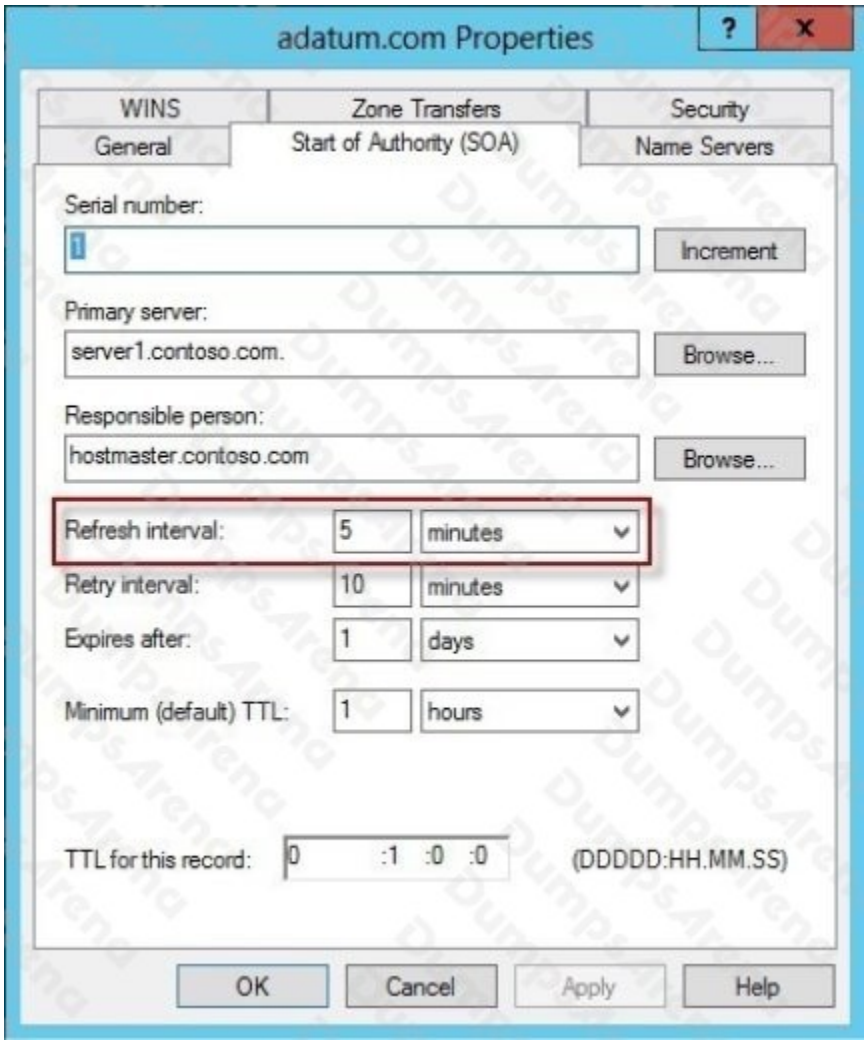
C. Minimum (default) TTL

D. Refresh interval

ANSWER: D

Explanation:

By default, the refresh interval for each zone is set to 15 minutes. The refresh interval is used to determine how often other DNS servers that load and host the zone must attempt to renew the zone.



QUESTION NO: 4

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

The network contains two subnets named Subnet1 and Subnet2. Server1 has a DHCP scope for each subnet.

You need to ensure that noncompliant computers on Subnet1 receive different network policies than noncompliant computers on Subnet2.

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

A. The NAP-Capable Computers conditions

B. The NAS Port Type constraints

C. The Health Policies conditions

D. The MS-Service Class conditions

E. The Called Station ID constraints

ANSWER: C D

Explanation:

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

If policies are filtered by DHCP scope, then MS-Service Class is configured in policy conditions.

QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

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

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

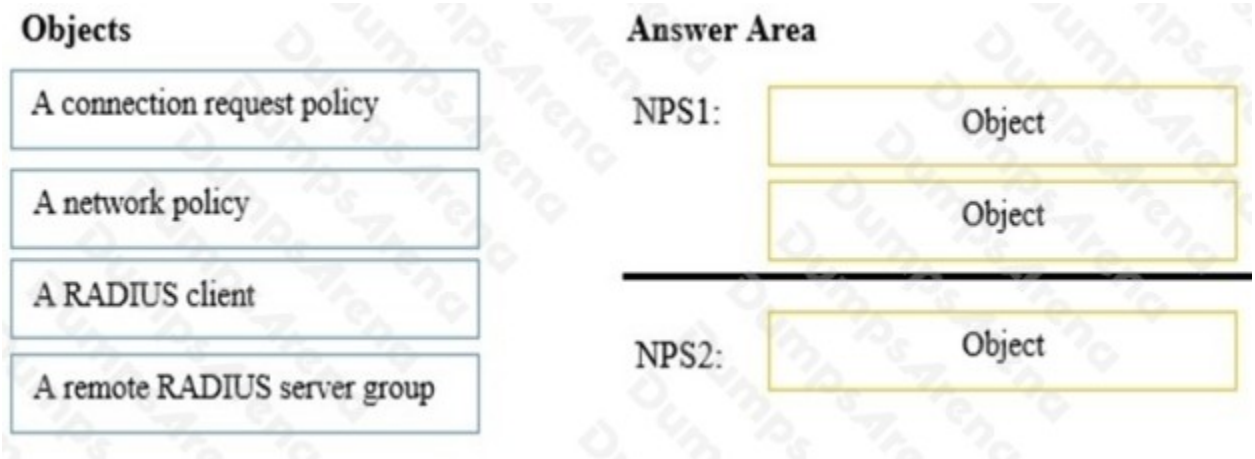
You plan to grant users from adatum.com VPN access to your network.

You need to authenticate the users from adatum.com on VPN1.

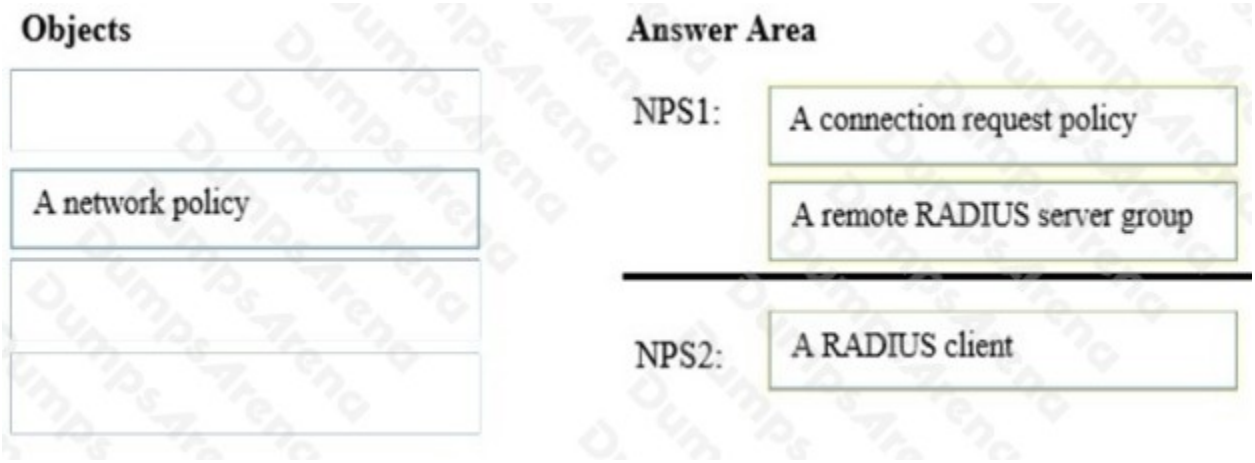
What should you create on each NPS server?

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

Select and Place:



ANSWER:



QUESTION NO: 6

You have a server that runs Windows Server 2012 R2.

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

You plan to apply several updates to Windows2012.vhd.

You need to mount Windows2012.vhd to D:\Mount.

Which tool should you use?

A. Server Manager

B. Device Manager

C. Mountvol

D. Dism

ANSWER: D

Explanation:

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

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

QUESTION NO: 7

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

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

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

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

A. The client identifier

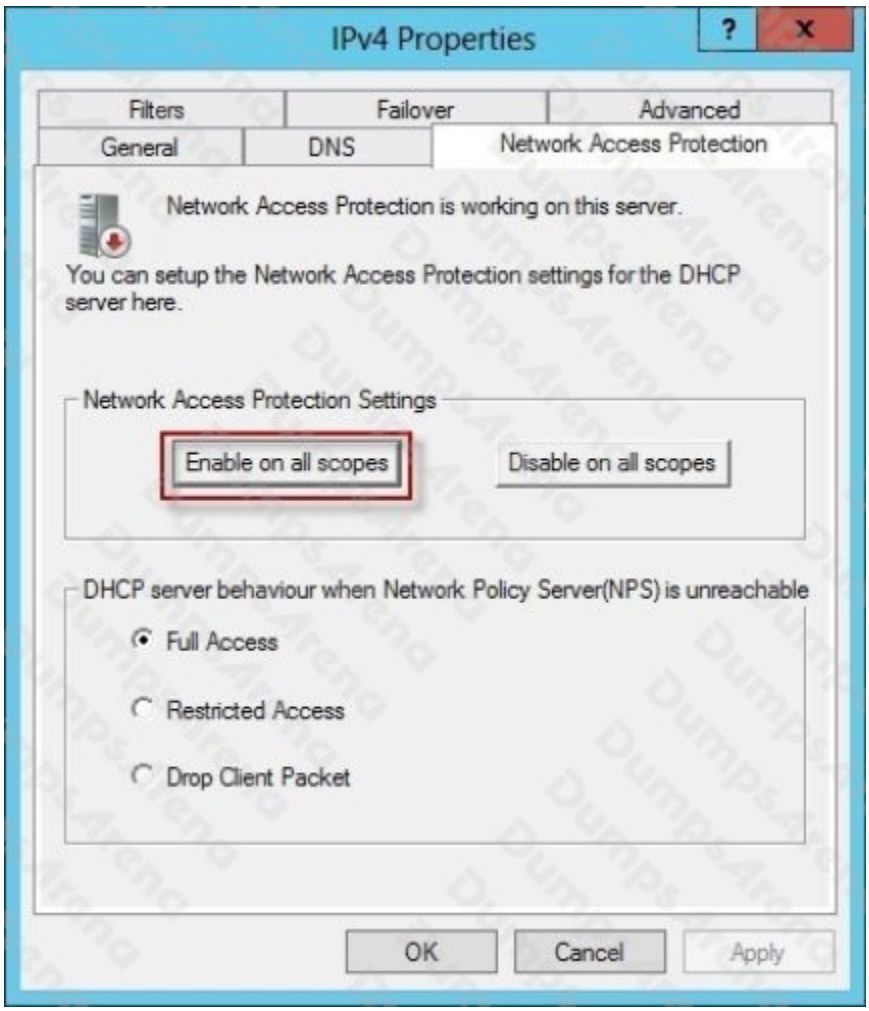
B. The user class

C. The vendor class

D. The relay agent information

ANSWER: B

Explanation:



To configure a NAP-enabled DHCP server

- On the DHCP server, click Start, click Run, in Open, type dhcpmgmt. smc, and then press ENTER.
- In the DHCP console, open \IPv4.
- Right-click the name of the DHCP scope that you will use for NAP client computers, and then click Properties.
- On the Network Access Protection tab, under Network Access Protection Settings, choose Enable for this scope, verify that Use default Network Access Protection profile is selected, and then click OK.
- In the DHCP console tree, under the DHCP scope that you have selected, right-click Scope Options, and then click Configure Options.
- On the Advanced tab, verify that Default User Class is selected next to User class.
- Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by compliant NAP client computers, and then click Add.
- Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each router to be used by compliant NAP client computers, and then click Add.
- Select the 015 DNS Domain Name check box, and in String value, under Data entry, type your organization's domain name (for example, woodgrovebank. local), and then click Apply. This domain is a full-access network assigned to compliant NAP clients. 10.On the Advanced tab, next to User class, choose Default Network Access Protection Class. 11.Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by noncompliant NAP client computers, and then click Add. This can be the same default gateway that is used by compliant NAP clients. 12.Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each DNS server to be used by noncompliant NAP client computers, and then click Add. These can be the same DNS servers used by compliant NAP clients. 13.Select the 015 DNS Domain Name check box, and in String value, under Data entry, type a name to identify the restricted domain (for example, restricted. Woodgrovebank. local), and then click OK. This domain is a restricted-access network assigned to noncompliant NAP clients.
- Click OK to close the Scope Options dialog box. - Close the DHCP console.

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

QUESTION NO: 8

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 requests to a remote RADIUS server group named Group1.

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

How should you configure Group1?

A. Change the Weight of Server4 to 10.

B. Change the Weight of Server2 and Server3 to 10.

C. Change the Priority of Server2 and Server3 to 10.

D. Change the Priority of Server4 to 10.

ANSWER: D

Explanation:

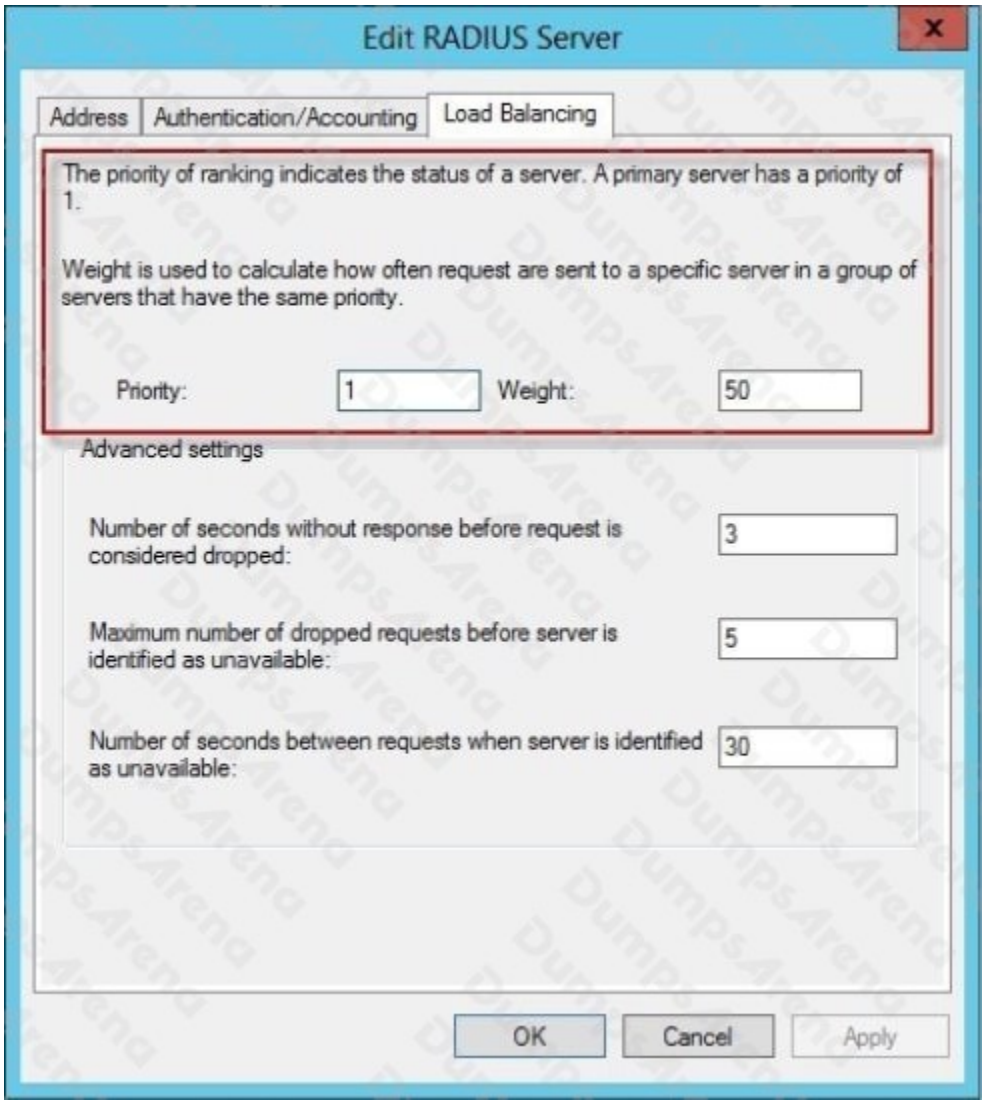
During the NPS proxy configuration process, you can create remote RADIUS server groups and then add RADIUS servers to each group. To configure load balancing, you must have more than one RADIUS server per remote RADIUS server group. While adding group members, or after creating a RADIUS server as a group member, you can access the Add RADIUS server dialog box to configure the following items on the Load Balancing tab:

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

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

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

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



References: http://technet.microsoft.com/en-us/library/dd197433(WS.10).aspx

QUESTION NO: 9

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

You install the Remote Access server role on 10 servers.

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

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

A. Configure each Remote Access server to use the Routing and Remote Access service (RRAS) to authenticate connection requests.

B. On NPS1, create a remote RADIUS server group. Add all of the Remote Access servers to the remote RADIUS server group.

C. On NPS1, create a new connection request policy and add a Tunnel-Type and a Service-Type condition.

D. Configure each Remote Access server to use a RADIUS server named NPS1.

E. On NPS1, create a RADIUS client template and use the template to create RADIUS clients.

ANSWER: C D

Explanation:

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

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

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

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

QUESTION NO: 10

Your network contains two Active Directory forests named contoso.com and adatum.com. The contoso.com forest contains a server named

Server1.contoso.com. The adatum.com forest contains a server named server2. adatum.com. Both servers have the Network Policy Server role service installed.

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

You plan to configure Server3 as an authentication provider for several VPN servers.

You need to ensure that RADIUS requests received by Server3 for a specific VPN server are always forwarded to Server1.contoso.com.

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

Choose two.)

A. Remediation server groups

B. Remote RADIUS server groups

C. Connection request policies

D. Network policies

E. Connection authorization policies

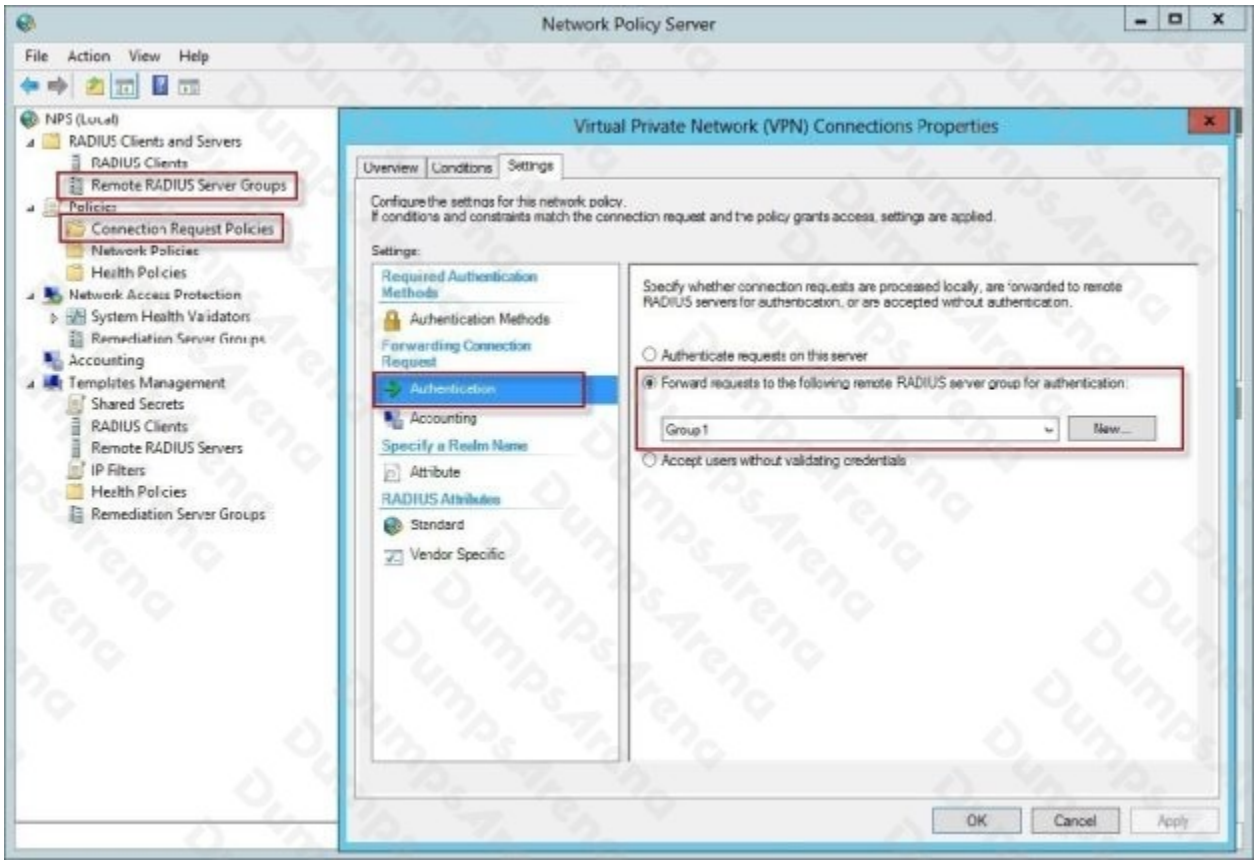
ANSWER: B C

Explanation:

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

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

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



References:

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

QUESTION NO: 11

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

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

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

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

A. Shortcuts

B. Network Shares

C. Environment

D. Folders

E. Files

ANSWER: D E

Explanation:

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

QUESTION NO: 12 - (HOTSPOT)

HOTSPOT

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.

Hot Area:

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

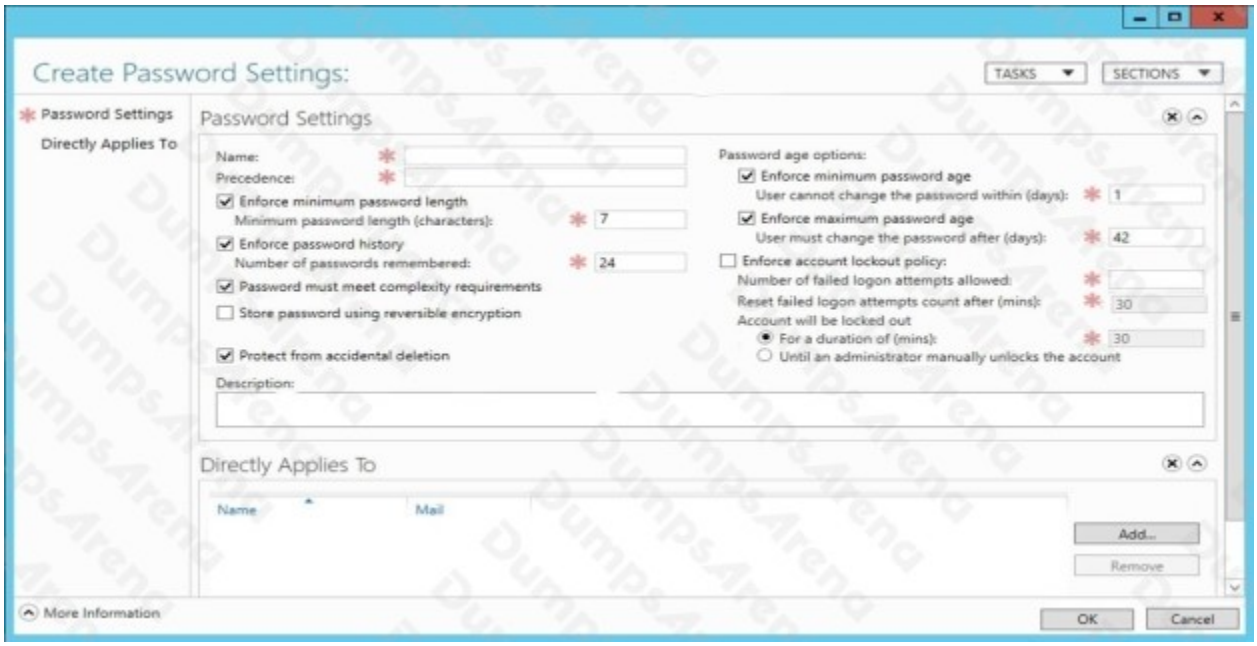
ANSWER:

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

Explanation:

Note:

* Password Setting Object (PSO) is another name for Fine Grain Password Policies. * Here you can see all the settings that go into a PSO.



QUESTION NO: 13

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

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

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

Active Directory Recycle Bin is enabled.

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

You need to restore the membership of Group1.

What should you do?

A. Recover the items by using Active Directory Recycle Bin.

B. Modify the Recycled attribute of Group1.

C. Perform tombstone reanimation.

D. Perform an authoritative restore.

E. Perform a non-authoritative restore.

F. Modify the isDeleted attribute of Group1.

G. Apply a virtual machine snapshot to DC2.

ANSWER: D

Explanation:

Because removing user accounts from an Active Directory group will not send them to the Active Directory Recycle Bin, performing an authoritative restore is the best option.

QUESTION NO: 14 - (DRAG DROP)

DRAG DROP

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

You deploy a new domain controller that runs Windows Server 2012 R2.

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

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

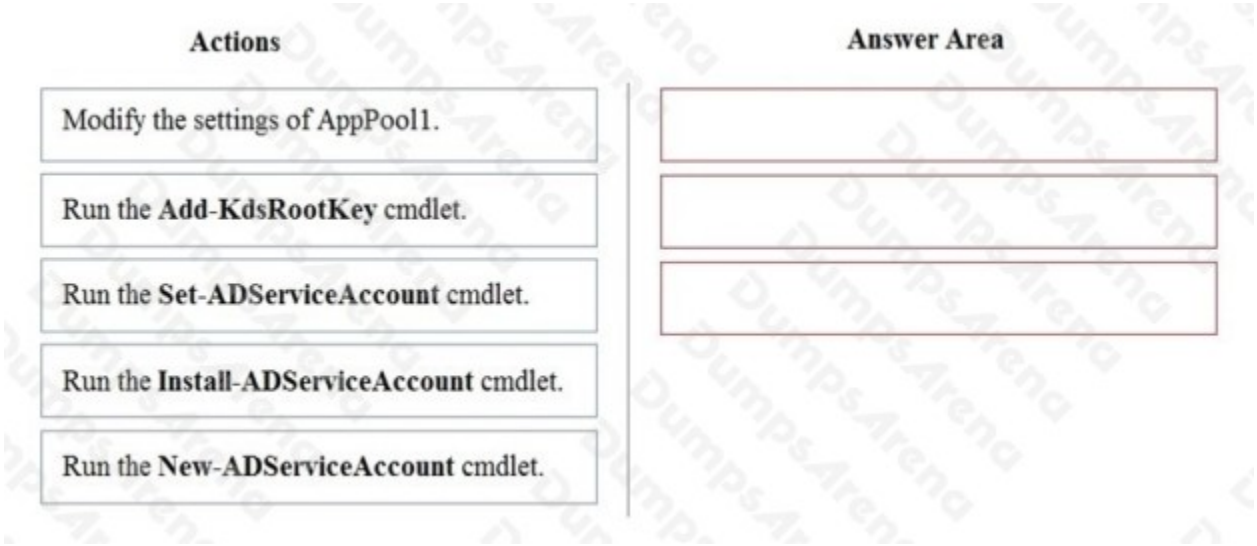
Server1 and Server2 host a load-balanced application pool named AppPool1.

You need to ensure that AppPool1 uses a group Managed Service Account as its identity.

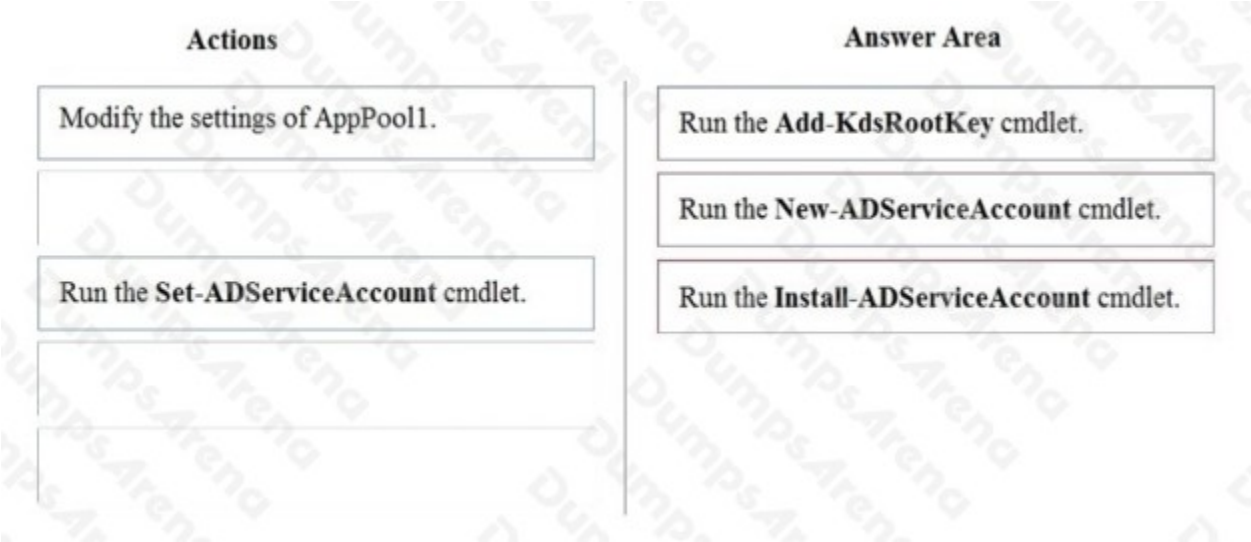
Which three actions should you perform in sequence?

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:



ANSWER:



Explanation:

References: https://blogs.technet.microsoft.com/askpfeplat/2012/12/16/windows-server-2012-group-managed-service-accounts/

QUESTION NO: 15 - (HOTSPOT)

HOTSPOT

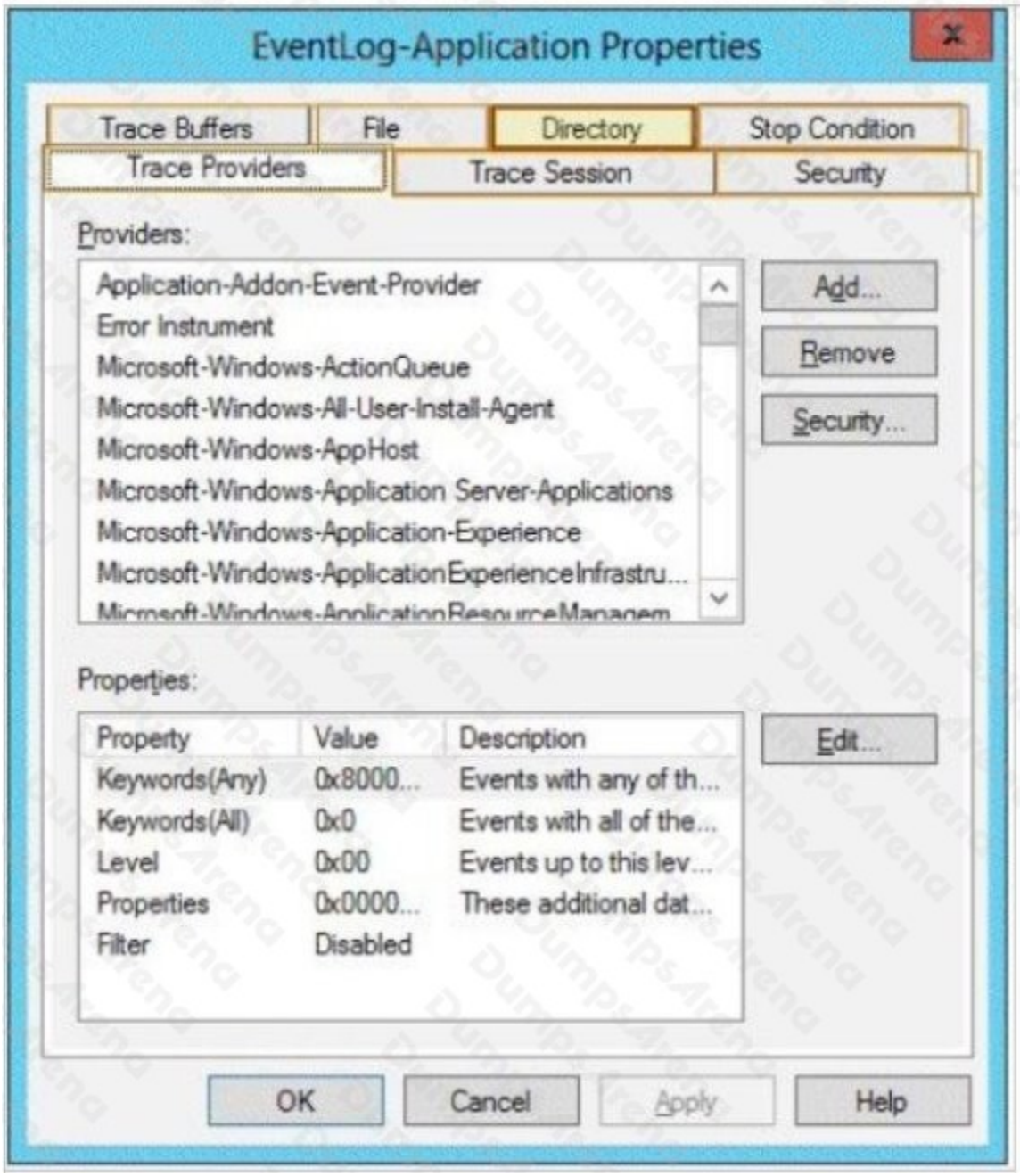
Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 runs Windows Server 2012 R2.

You enable the EventLog-Application event trace session.

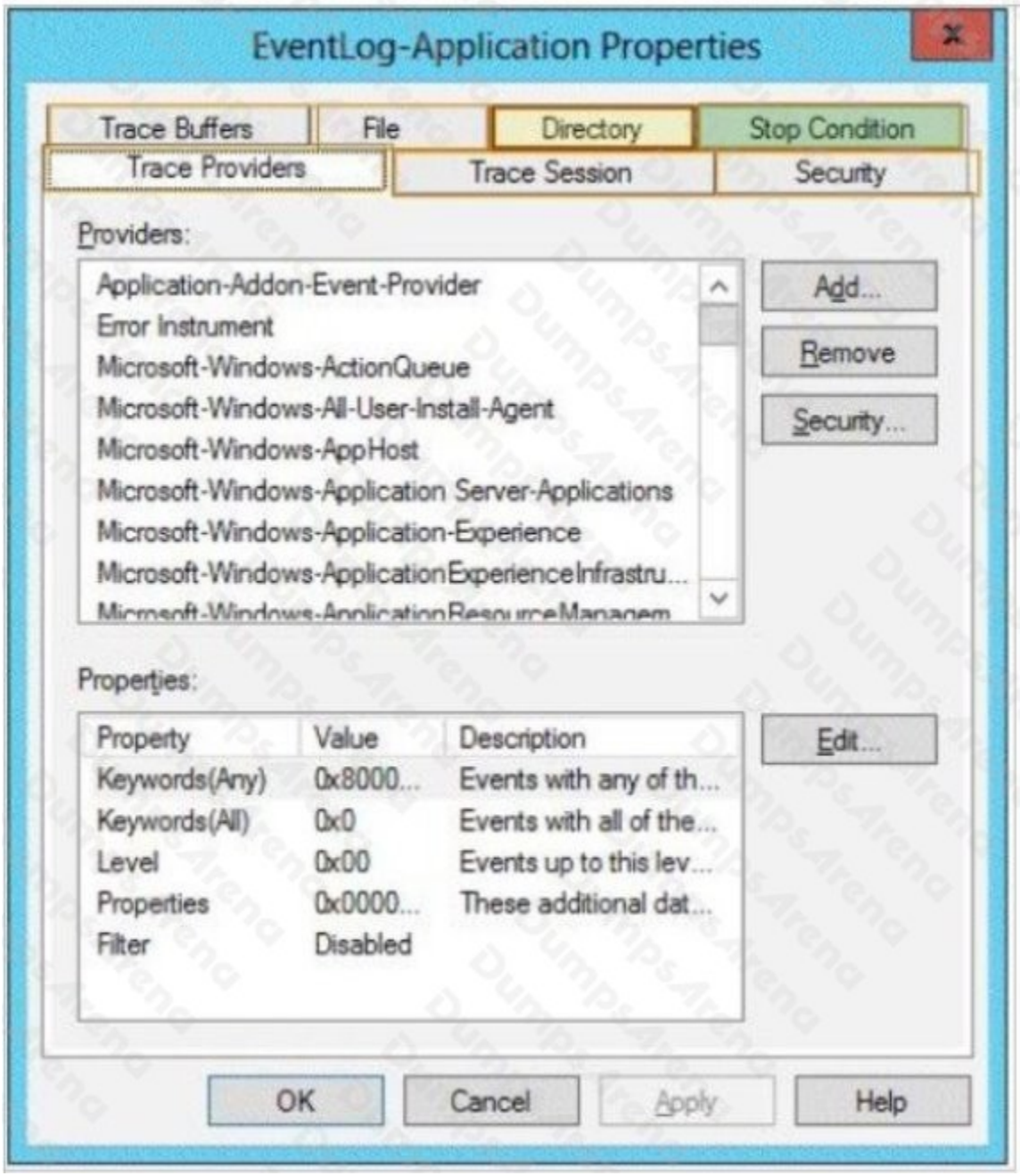
You need to set the maximum size of the log file used by the trace session to 10 MB.

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

Hot Area:

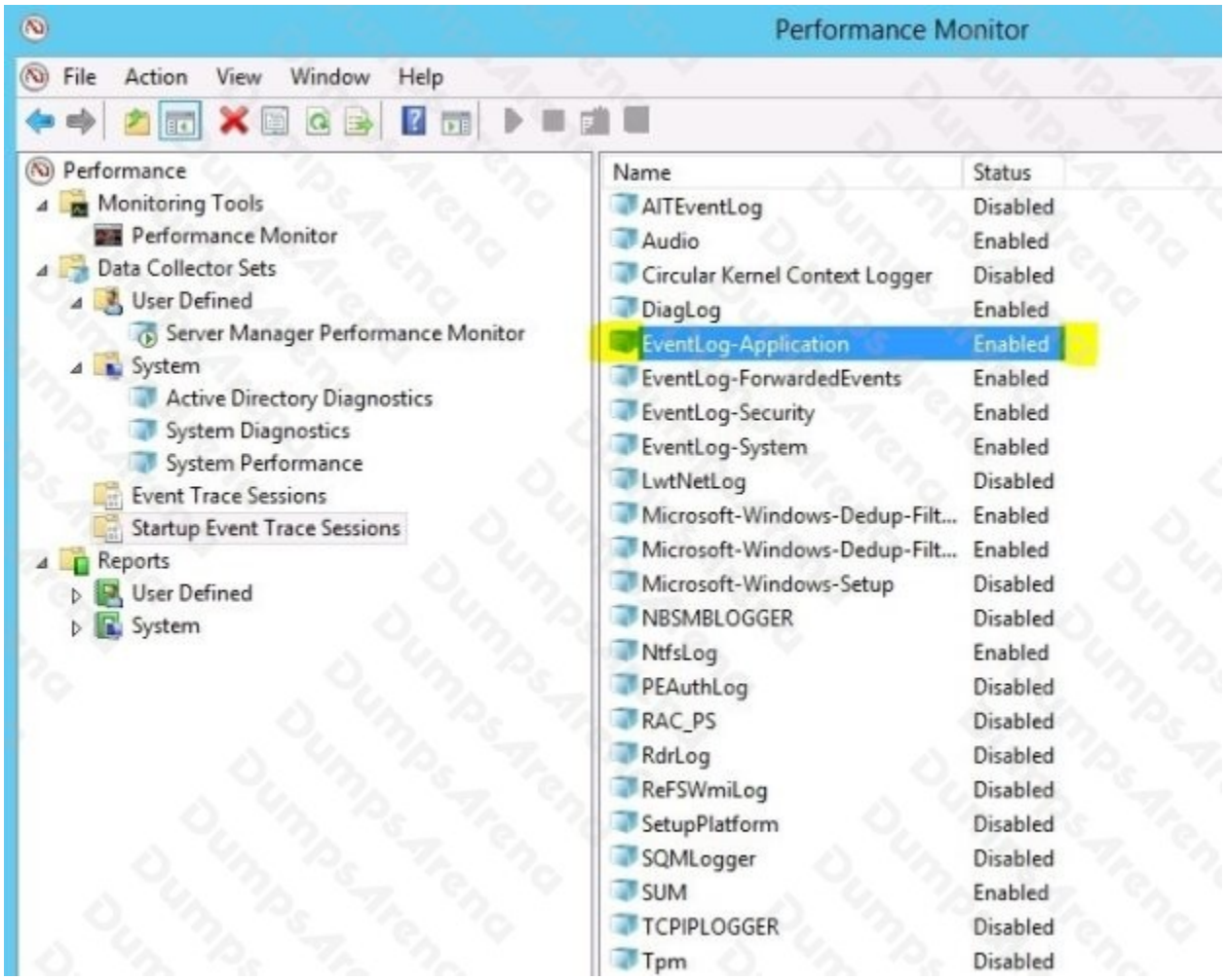

EventLog-Application Properties
Trace Buffers
File
Directory
Stop Condition
Trace Providers
Trace Session
Security
Providers:
Application-Addon-Event-Provider
Error Instrument
Microsoft-Windows-ActionQueue
Microsoft-Windows-All-User-Install-Agent
Microsoft-Windows-AppHost
Microsoft-Windows-Application Server-Applications
Microsoft-Windows-Application-Experience
Microsoft-Windows-ApplicationExperienceInfrastru...
Add...
Remove
Security...
Properties:
Property
Value
Description
Keywords(Any)
0x8000...
Events with any of th...
Keywords(All)
0x0
Events with all of the...
Level
0x00
Events up to this lev...
Properties
0x0000...
These additional dat...
Filter
Disabled
Edit...
OK
Cancel
Apply
Help

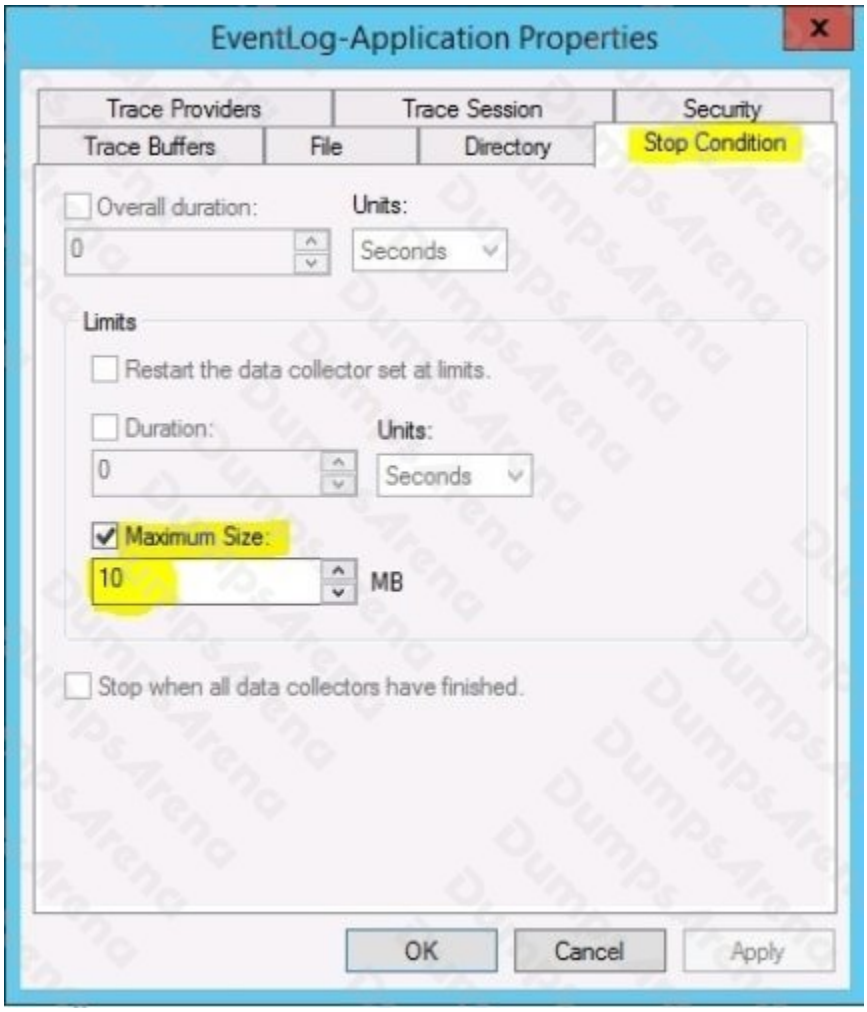
ANSWER:



Explanation:

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


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



References: http://technet.microsoft.com/en-us/magazine/ff458614.aspx