Exam Number/Code: 70-411

Exam Name: Administering Windows Server 2012

Version: Demo

QUESTION: 1
DRAG DROP - (Topic 0)

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

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

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

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

What should you create on each NPS server?

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

Objects	Answer Area
a connection request policy	NPS1: Object
a network policy	Object
a RADIUS client	NPS2: Object
a remote RADIUS server group	

Answer:

Objects	Answer Area
a connection request policy	NPS1: a connection request policy
a network policy	a remote RADIUS server group
a RADIUS client	NPS2: a RADIUS client
a remote RADIUS server group	

QUESTION: 2
HOTSPOT - (Topic 0)

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

User name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

What should you identify?

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

Answer Area

User1: [▼]

User2: [▼]

User3: [▼]

Answer Area

User1: [dropdown]
- Policy1
- Policy2
- Policy3

User2: [dropdown]
- Policy1
- Policy2
- Policy3

User3: [dropdown]
- Policy1
- Policy2
- Policy3

Answer:

Answer Area

User1: [dropdown]
- Policy1
- **Policy2**
- Policy3

User2: [dropdown]
- **Policy1**
- Policy2
- Policy3

User3: [dropdown]
- **Policy1**
- Policy2
- Policy3

QUESTION: 3
 - (Topic 0)
Your network contains an Active Directory domain named contoso.com. The domain
contains a server named Server1 that runs Windows Server 2012 R2.

Server1 has the following role services installed:

DirectAccess and VPN (RRAS)

Network Policy Server

Remote users have client computers that run either Windows XP, Windows 7, or Windows 8.
You need to ensure that only the client computers that run Windows 7 or Windows 8 can establish VPN connections to Server1.

What should you configure on Server1?

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

Answer: A

Explanation:
If you want to configure the Operating System condition, click Operating System, and then click Add. In Operating System Properties, click Add, and then specify the operating system settings that are required to match the policy. The Operating System condition specifies the operating system (operating system version or service pack number), role (client or server), and architecture (x86, x64, or ia64) required for the computer configuration to match the policy.
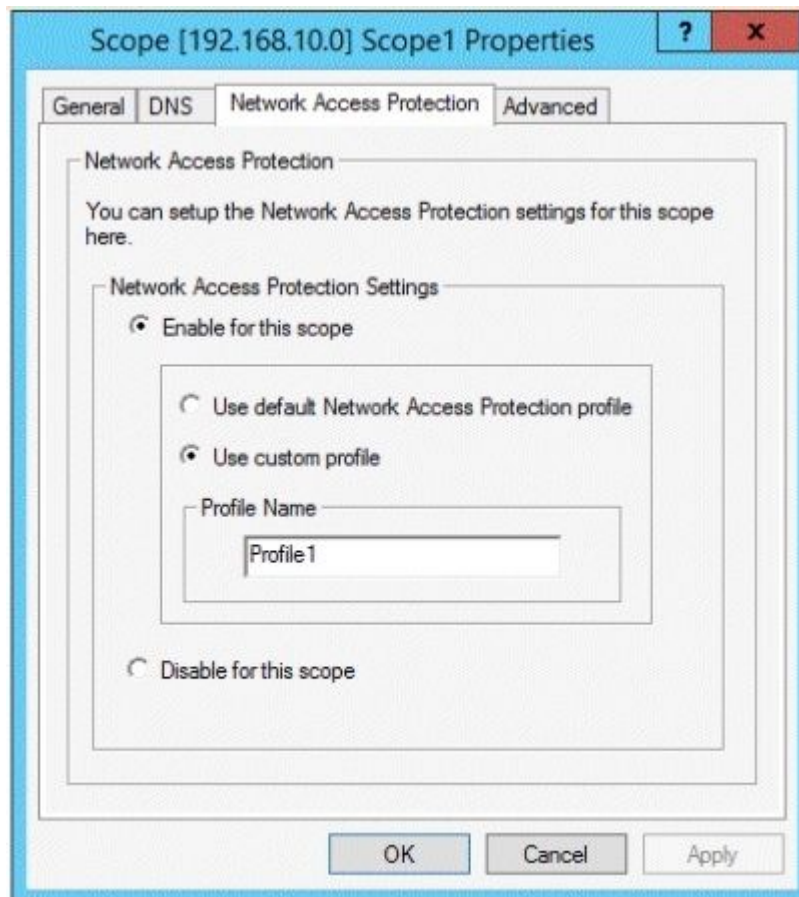
QUESTION: 4
HOTSPOT - (Topic 0)

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

You are configuring Network Access Protection (NAP) to use DHCP enforcement.

You configure a DHCP scope as shown in the exhibit. (Click the Exhibit button.)

Scope [192.168.10.0] Scope1 Properties

General | DNS | Network Access Protection | Advanced

Network Access Protection

You can setup the Network Access Protection settings for this scope here.

Network Access Protection Settings

(•) Enable for this scope

( ) Use default Network Access Protection profile

(•) Use custom profile

Profile Name

Profile1

( ) Disable for this scope

[OK] [Cancel] [Apply]

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

What should you configure on each server?

To answer, select the appropriate options for each server in the answer area.

Answer Area

Server1: [_____ ▼]

Server2: [_____ ▼]

Answer Area

Server1:
- Health Policies
- Identity-Type
- MS-Service Class
- Service-Type

Server2:
- filters
- a policy
- scope options
- server options
- a User class
- a Vendor class

Answer:

Answer Area

Server1:
- **Health Policies**
- Identity-Type
- MS-Service Class
- Service-Type

Server2:
- filters
- a policy
- scope options
- **server options**
- a User class
- a Vendor class

QUESTION: 5
 - (Topic 0)

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.
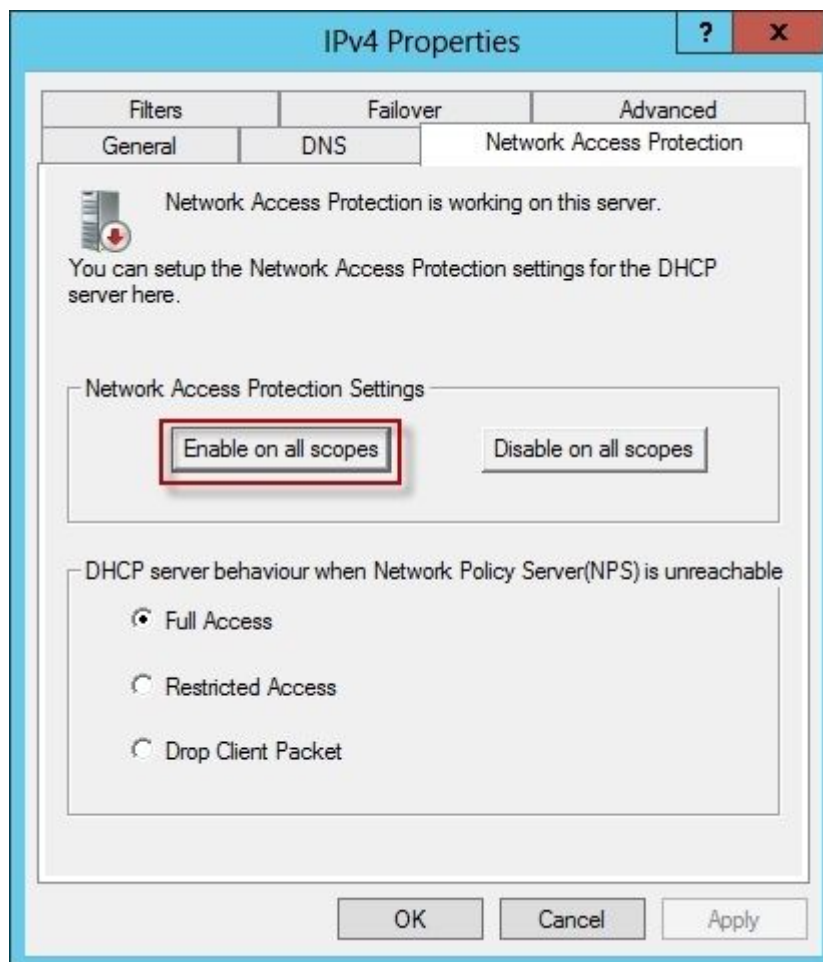
www.certasap.com original question and answer

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 <servername>\IPv4.

Right-click the name of the DHCP scope that you will use for NAP client computers, and then click Properties.

On the Network Access Protection tab, under Network Access Protection Settings, choose Enable for this scope, verify that Use default Network Access Protection profile is selected, and then click OK.

In the DHCP console tree, under the DHCP scope that you have selected, right- click Scope Options, and then click Configure Options. On the Advanced tab, verify that Default User Class is selected next to User class.

Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by compliant NAP client computers, and then click Add.

Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each router to be used by compliant NAP client computers, and then click Add.

Select the 015 DNS Domain Name check box, and in String value, under Data entry, type your organization's domain name (for example, woodgrovebank. local), and then click Apply. This domain is a full-access network assigned to compliant NAP clients.

On the Advanced tab, next to User class, choose Default Network Access Protection Class.

Select the 003 Router check box, and in IP Address, under Data entry, type the IP address for the default gateway used by noncompliant NAP client computers, and then click Add. This can be the same default gateway that is used by compliant NAP clients.

Select the 006 DNS Servers check box, and in IP Address, under Data entry, type the IP address for each DNS server to be used by noncompliant NAP client computers, and then click Add. These can be the same DNS servers used by compliant NAP clients.

Select the 015 DNS Domain Name check box, and in String value, under Data entry, type a name to identify the restricted domain (for example, restricted. Woodgrovebank. local), and then click OK. This domain is a restricted-access network assigned to noncompliant NAP clients.

Click OK to close the Scope Options dialog box.

Close the DHCP console.

QUESTION: 6
HOTSPOT - (Topic 0)

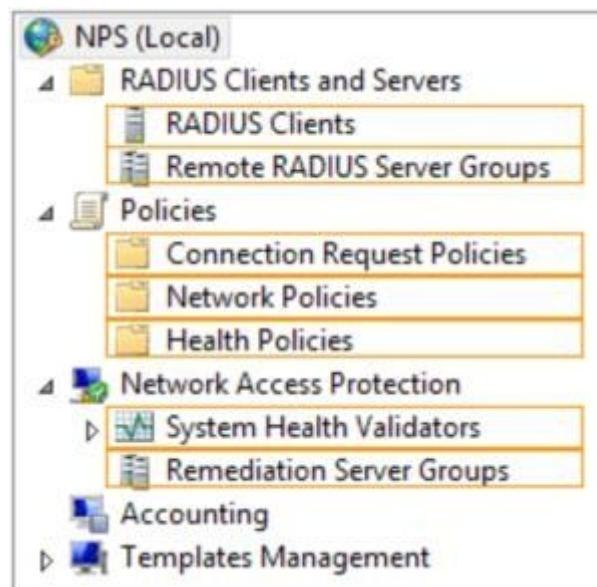Your network contains a RADIUS server named Server1.

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

You need to ensure that all accounting requests for Server2 are forwarded to Server1.
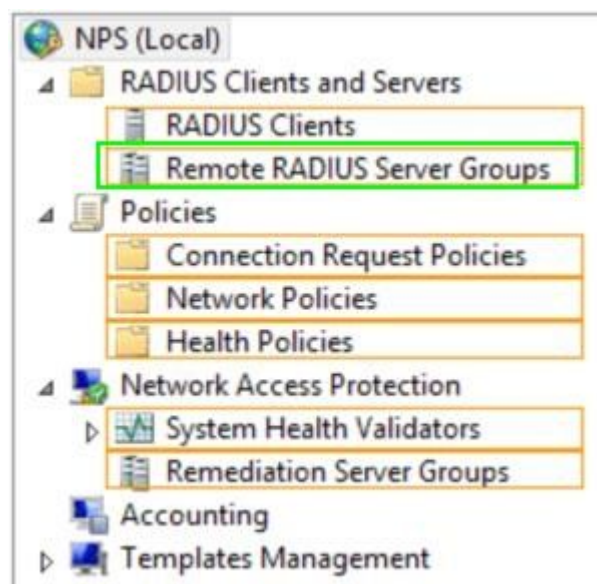
On Server2, you configure a Connection Request Policy.

What else should you configure on Server2?

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

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
  - Remediation Server Groups
- Accounting
- Templates Management

Answer:

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
  - Remediation Server Groups
- Accounting
- Templates Management

QUESTION: 7
 - (Topic 0)

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

An administrator creates a RADIUS client template named Template1.

You create a RADIUS client named Client1 by using Template 1.

You need to modify the shared secret for Client1.

What should you do first?

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

Answer: D

Explanation:
Clear checkmark for Select an existing template in the new client wizard.

In New RADIUS Client, in Shared secret, do one of the following:
Bullet Ensure that Manual is selected, and then in Shared secret, type the strong
password that is also entered on the RADIUS client. Retype the shared secret in Confirm
shared secret.

New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

☑ Select an existing template:

Template1 ▼

Name and Address

Friendly name:

Client1

Address (IP or DNS):

192.168.1.1   Verify...

Shared Secret

Select an existing Shared Secrets template:

None ▼

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

◉ Manual   ○ Generate

Shared secret:

•••

Confirm shared secret:

•••

OK   Cancel

New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

☐ Select an existing template:

Template1 ▾

Name and Address

Friendly name:

Client1

Address (IP or DNS):

192.168.1.1   Verify...

Shared Secret

Select an existing Shared Secrets template:

None ▾

None
123

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

◉ Manual   ○ Generate

Shared secret:

•••

Confirm shared secret:

•••

OK   Cancel

QUESTION: 8
 - (Topic 0)

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

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

Server1 provides VPN access to external users.

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

What should you run?

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

Answer: C

Explanation:
Add-RemoteAccessRadius
Adds a new external RADIUS server for VPN authentication, accounting for DirectAccess (DA) and VPN, or one-time password (OTP) authentication for DA.
AccountingOnOffMsg<String>
Indicates the enabled state for sending of accounting on or off messages. The acceptable values for this parameter are:
Enabled.
Disabled. This is the default value.
This parameter is applicable only when the RADIUS server is being added for Remote Access accounting.

QUESTION: 9
- (Topic 0)

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

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

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

How should you configure Group1?

A. Change the Weight of Server4 to 10.

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

Answer: D

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

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

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

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

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

QUESTION: 10
DRAG DROP - (Topic 0)

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

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

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

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

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

The Authenticated Users group is assigned the default permissions to all of the GPOs.

There are no site-level GPOs.

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

Which three GPOs should you identify in sequence?

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

Actions	Answer Area
GPO5	
GPO3	
GPO2	
GPO1	
GPO4	

Answer:

Actions	Answer Area
GPO5	GPO2
GPO3	GPO4
GPO2	GPO5
GPO1	
GPO4	