

**Microsoft 70-642**



**70-642 TS: Windows Server 2008 Network  
Infrastructure, Configuring  
Practice Test  
Version**

**QUESTION NO: 1**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com which uses Internet Protocol version 6 (IPv6)

CertKiller.com currently has their headquarters located in Miami containing 25 subnets.

During the course of the business day you receive instruction from CertKiller.com to install a server named CERTKILLER-SR01 on the network. CertKiller.com wants you to configure CERTKILLER-SR01 to communicate with all client computers on all the IPv6 subnets.

What should you do?

- A. You should consider having the IPv6 address fe80::2c0:d11f:fec8:3124/64 configured for CERTKILLER-SR01.
- B. You should consider having the IPv6 address fd00:: 2c0:d11f:fec8:3124/8 configured for CERTKILLER-SR01.
- C. You should consider having the IPv6 address 0000::2c0:d11f:fec8:3124/64 configured for CERTKILLER-SR01.
- D. You should consider having the IPv6 address ff80::2c0:d11f:fec8:3124/64 configured for CERTKILLER-SR01.

**Answer: B**

**QUESTION NO: 2**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

The CertKiller.com network currently has three departments and CertKiller.com plans to add a fourth in the future. During the course of the day you receive instruction from CertKiller.com to assign a subnet for the departments using the global address prefix 3FFA:FF2B:4D:B000::/41 assigned to you.

What should you do?

- A. You should consider having the IPv6 address 3FFA:FF2B:4D:C000::/43 for the added department.
- B. You should consider having the IPv6 address 3FFA:FF2B:4D:F000::/45 for the added department.
- C. You should consider having the IPv6 address 3FFA:FF2B:4D:C800::/43 for the added department.

D. You should consider having the IPv6 address 3FFA:FF2B:4D:B400::/43 for the added department.

**Answer: C**

**Explanation:**

The option 3FFA:FF2B:4D: C800: :/ 43 is correct. The subnetting in IPv6 is performed by determining the number of bits used for subnetting and the itemization of the new subnetted address prefixes.

Usually the number of bits for subnetting is  $s$ , where  $2^s$  = number of subnets to be created. In this scenario  $2^s = 4$  and therefore  $s=2$ .

Then the itemizations of the new subnetted address prefixes are done. In this scenario, the correct subnetted address prefix is 3FFA:FF2B:4D :C800 ::/43. So option A is the correct answer.

**QUESTION NO: 3**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as the Dynamic Host Configuration Protocol (DHCP) server. During the course of the day you receive instruction from CertKiller.com to ensure that no IP address of configuration settings are automatically assigned to DHCP clients on a subnet which does not make use of DHCPv6 provided by CERTKILLER-SR01.

What should you do?

- A. You should consider having the Managed Address Configuration to 0 and Other Stateful Configuration flag set to 1.
- B. You should consider having the Managed Address Configuration to 1 and Other Stateful Configuration flag set to 0.
- C. You should consider having both the Managed Address Configuration and Other Stateful Configuration flag set to 0.
- D. You should consider having both the Managed Address Configuration and Other Stateful Configuration flag set to 1.

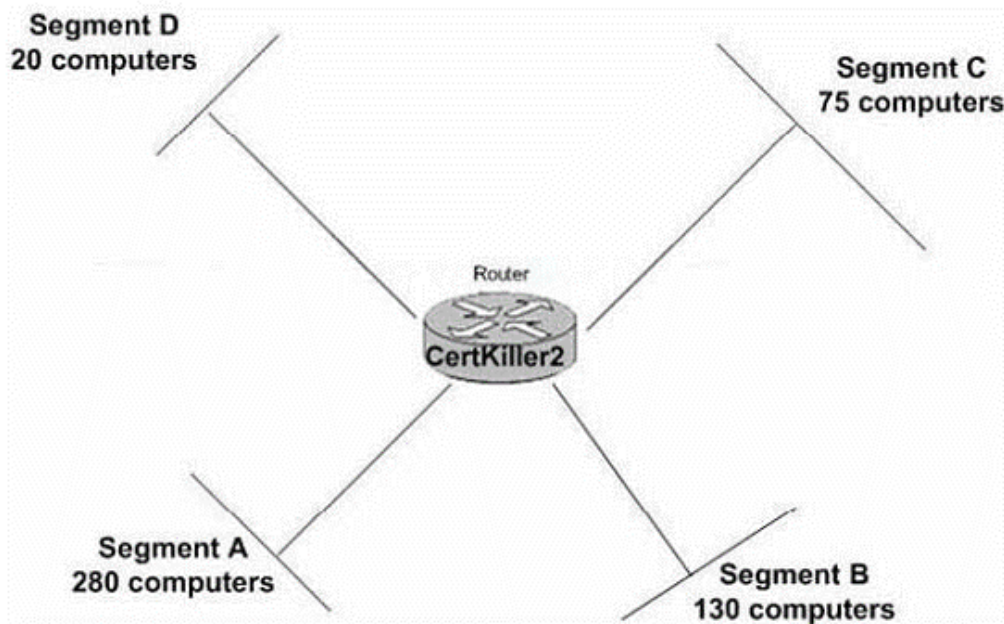
**Answer: C**

**Explanation:**

This setting will ensure that the host will receive neither an IP address nor any additional configuration information.

**QUESTION NO: 4**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. A portion of the CertKiller.com network is shown in the exhibit below:



CertKiller.com has recently decided to make use of IPv4 addressing using the network range 129.108.10.0/21. During the course of the day you receive instruction from CertKiller.com to have the network range segmented into four segments as shown in the exhibit.

What should you do?

- A. You should consider assigning the network ranges as shown below  
Segment A 129.108.10.0/22, Segment B 129.108.10.128/23, Segment C 129.108.10.0/192 and Segment D 129.108.10.224/25
- B. You should consider assigning the network ranges as shown below  
Segment A 129.108.10.128/22, Segment B 129.108.10.192/23, Segment C 129.108.10.224/24 and Segment D 129.108.10.0/26
- C. You should consider assigning the network ranges as shown below  
Segment A 129.108.10.109/22, Segment B 129.108.10.0/23, Segment C 129.108.10.0/24 and Segment D 129.108.10.109/25
- D. You should consider assigning the network ranges as shown below  
Segment A 129.108.10.0/22, Segment B 129.108.10.0/23, Segment C 129.108.10.0/24 and Segment D 129.108.10.128/26

**Answer: D**

**QUESTION NO: 5**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 as the network DNS server. During the course of the day you receive instruction from CertKiller.com to deploy two servers to the network configured as DHCP servers.

The CertKiller.com network users recently started reporting that they are unable to log onto the domain after you changed the IP address of CERTKILLER-SR01. CertKiller.com wants you to ensure that the network users are able to log onto the domain.

What should you do?

- A. You should consider having the DHCP scope option 006 DNS name Servers reconfigured with the new IP addresses of CERTKILLER-SR01.
- B. You should consider having the network settings for workstations configured to Disable NetBIOS over TCP/IP.
- C. You should consider having the Netlogon service restarted on CERTKILLER-SR01.
- D. You should consider having the ipconfig/registerdns command run at the command prompt of CERTKILLER-SR01.

**Answer: A**

**Explanation:**

To ensure that the users are able to log on to the domain, you should reconfigure the DHCP scope option 006 DNS name Server with the new DNS servers IP addresses.

**QUESTION NO: 6**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day you receive information from CertKiller.com about eight IPv6 segmented address prefixes shown below:

- A. 3FFE:FFFF:0:C000::/54
- B. 3FFE:FFFF:0:C400::/54
- C. 3FFE:FFFF:0:C800::/54
- D. 3FFE:FFFF:0:CC00::/54
- E. 3FFE:FFFF:0:D400::/54
- F. 3FFE:FFFF:0:D400::/54
- G. 3FFE:FFFF:0:D800::/54
- H. 3FFE:FFFF:0:DC00::/54

CertKiller.com wants you to determine what the original prefix length for the global address prefix 3FFE:FFFF:0:C000:: would be?

- A. The original prefix length for the global address would be 3FFE:FFFF:0:C000::/52.
- B. The original prefix length for the global address would be 3FFE:FFFF:0:C000::/54
- C. The original prefix length for the global address would be 3FFE:FFFF:0:C000::/51.
- D. The original prefix length for the global address would be 3FFE:FFFF:0:C000::/53.

**Answer: C**

**Explanation:**

The original prefix length for the global address prefix 3FFE :FFFF:0:C000 :: is 51. The eight Ipv6 subnetted address prefixes are the result of 3 bit subnetting of the global address prefix 3FFE:FFFF:0:C000::/51. To perform 3-bit subnetting of the global address prefix 3FFE :FFFF:0:C000 ::/51 we use the following calculations:

Hexadecimal value of the subnet ID being subnetted, F = 0xC000

Subnetting bits, s = 3

**QUESTION NO: 7**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com has recently deployed a computer named CERTKILLER-SR01 to the IPv6 network with 25 segments. CertKiller.com wants you to ensure that CERTKILLER-SR01 is able to communicate with all client computers on all segments.

What should you do?

- A. You should consider having the IPv6 address ff80::2b0: d0ff:fee9:4143/64 assigned to CERTKILLER-SR01.

- B. You should consider having the IPv6 address 0000::2b0: d0ff:fee9:4143/64 assigned to CERTKILLER-SR01.
- C. You should consider having the IPv6 address fd00::2b0:d0ff:fee9:4143/8 assigned to CERTKILLER-SR01.
- D. You should consider having the IPv6 address fe80::2b0: d0ff:fee9:4143/64 assigned to CERTKILLER-SR01.

**Answer: C**

**Explanation:**

To ensure that the server communicates with systems on all segments of the IPV6 network, you need to configure the IPV6 address as fd00: :2b0:d0ff:fee9:4143 /8 because this address is the local unicast address type and is not routed on the Internet. It is generally filtered inbound.

Reference : IPv6 Unicast Address Information

<http://www.netcraftsmen.net/welcher/papers/ipv6part02.html>

**QUESTION NO: 8**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day CertKiller.com opens a branch office in Toronto which initially has fifty client computers. CertKiller.com wants you to determine which IP addressing scheme should be used at the branch office.

What should you do?

- A. You should consider having the 192.10.100.0/29 IP addressing scheme used at the Toronto office.
- B. You should consider having the 192.10.100.0./31 IP addressing scheme used at the Toronto office.
- C. You should consider having the 192.10.100.0/26 IP addressing scheme used at the Toronto office.
- D. You should consider having the 192.10.100.0/30 IP addressing scheme used at the Toronto office.

**Answer: C**

**Explanation:**



To configure an appropriate IP addressing scheme in the network, you should use 192.10.100.0/26. In this scenario, 50 computers have to be configured in a network. Network address is calculated as follows:

Class A networks has a default subnet mask of 255.0.0.0 and use 0-127 as their first octet  
Class B networks has a default subnet mask of 255.255.0.0 and it can use 128-191 as their first octet  
Class C networks has a default subnet mask of 255.255.255.0 and it can use 192-223 as their first octet

You need to configure the network address to accommodate at least 50 hosts per subnet. To calculate the number of host bits, use the formula:  $2^n - 2$  where  $n = 32$  bits. To configure 50 hosts, you need 192.10.100/26 network address which has maximum 62 hosts per subnet. The formula to calculate the hosts per subnet is:

$$32 - 26 = 6$$

$$2^6 - 2 = 62$$

So according to this calculation, network address 192.10.100/26 will be able to accommodate 50 hosts per subnet. We have deducted 6 bits from the total of 32 bits.

#### QUESTION NO: 9

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com.

CertKiller.com currently has their headquarters located in Miami containing network servers that are installed with Microsoft Windows Server 2008. The client computers on the CertKiller.com network run either Microsoft Windows Vista, Windows XP Professional (SP2) or Windows 2000 Professional.

During the course of the business day you receive instruction from CertKiller.com to install a server named CERTKILLER-SR01 to run IPv6 addressing on the network. CertKiller.com wants you to configure all client computers to communicate with CERTKILLER-SR01.

What should you do?

- A. You should consider having the Windows 2000 Professional computers upgraded with Service Pack 4.
- B. You should consider having the Active Directory Client extension (DSCClient.exe) installed on all the client computers.
- C. You should consider having all client computers installed with the IPv6.exe tool.
- D. You should consider having the Windows 2000 Professional computers upgraded to Windows XP SP2.



**Answer: D**

**Explanation:**

:

To ensure that all computers can use the IPv6 protocol, you need to upgrade the Windows 2000 Professional computers to Windows XP SP2. IPv6 protocol is far superior to IPv4 protocol in terms of security, complexity, and quality of service (QoS). Therefore, all the new operating systems started using IPv6 protocol. The older operating systems such as Windows 2000 professional does not support Ipv6 therefore this needs to be upgraded to either Windows XP or Windows Vista.

You can now get versions of Windows that fully support most aspects of IPv6 (namely Windows XP and Windows Server 2003) and you will soon be able to get versions of Windows that not only fully support IPv6 but also provide enhanced performance for IPv6 networking.

Reference : IPv6 Support in Microsoft Windows/ Windows 2000

[http://www.windowsnetworking.com/articles\\_tutorials/IPv6-Support-Microsoft-Windows.html](http://www.windowsnetworking.com/articles_tutorials/IPv6-Support-Microsoft-Windows.html)

**QUESTION NO: 10**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami and branch offices located in Toronto and Philadelphia. The branch offices currently make use of IPv4 and IPv6 protocol and are secured by a firewall configured to perform symmetric Network Address Translation (NAT). During the course of the day you receive instruction from CertKiller.com to configure the firewall in such a way as to allow peer-to-peer communications between Miami and Toronto and Philadelphia.

What should you do?

- A. You should consider having the firewall configured with a link local IPv6 address on the internal interface.
- B. You should consider having the symmetric NAT changed to dynamic NAT on the firewall.
- C. You should consider having the use of Teredo configured in the firewall.
- D. You should consider having the firewall configured with a global IPv6 address on the external interface.

**Answer: C**

**Explanation:**

To allow peer-to-peer communication between all branch offices where each location is protected by a firewall that performs symmetric NAT, you need to configure the firewall to allow the use of Teredo.

Teredo is an IPv6 transition technology that provides address assignment and host-to-host automatic tunneling for unicast IPv6 traffic when IPv6/IPv4 hosts are located behind one or multiple IPv4 network address translators (NATs).

Teredo in Windows Vista and Windows Server 2008 will work if one of the peers is behind a symmetric NAT and the other is behind a cone or restricted NAT.

Reference : Teredo Overview

[http://technet.microsoft.com/en-us/library/bb457011\(TechNet.10\).aspx](http://technet.microsoft.com/en-us/library/bb457011(TechNet.10).aspx)

### QUESTION NO: 11

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day CertKiller.com decided to deploy a computer named CERTKILLER-SR01 to the network using the IPv6 address 172.16.45.9/21. CertKiller.com wants you to test communication at the command prompt to a server that is making use of the 172.16.40.18/21 IP address.

What should you do?

- A. You should consider having the ping command run with the Site-local address of the server.
- B. You should consider having the ping 172.16.40.9::: command run.
- C. You should consider having the ping ::9.40.18.172 command run.
- D. You should consider having the ping command run with the Link-local address of the server.

**Answer: D**

**Explanation:**

:

To test IPv6 communication to a server, you need to type ping followed by the Link-local address of the server. Link-local addresses are network addresses which are intended only for use in a local data link layer network, and not for routing beyond that network.

Link-local addresses are often used for network address autoconfiguration where no external source of network addressing information is available.

Windows Vista, Windows Server 2008, Windows XP with SP1 or later, and Windows Server 2003 include an IPv6-enabled version of the Ping.exe tool.

Reference : Test an IPv6 configuration by using the ping command

<http://technet2.microsoft.com/windowsserver/en/library/8478cc0b-1613-431b-8130-529735d2945b1033.msp?mfr=true>

Reference : link-local address

<http://www.answers.com/topic/link-local-address-1?cat=technology>

## QUESTION NO: 12

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day CertKiller.com deployed a computer named CERTKILLER-SR21 which is configured with the Network Access Policy server role. CertKiller.com wants you to have the tunnel interface and the IPv6 Loopback interface as the only connections running IPv6.

What should you do?

- A. You should consider having the netsh ras ipv4 set command run.
- B. You should consider having the Internet Protocol Version 6 (TCP/IPv6) checkbox from the Local Area Connection Properties window cleared.
- C. You should consider having the netsh internal interface ipv6 delete command run.
- D. You should consider having the IPv6 protocol removed with the ipv6.exe tool.

**Answer: B**

### Explanation:

To disable IPv6 for all connections except for the tunnel interface and the IPv6 Loopback interface, you need to uncheck Internet Protocol Version 6 (TCP/IPv6) from the Local Area Connection Properties window.

This is because unlike Windows XP and Windows Server 2003, IPv6 in Windows Vista and Windows Server 2008 cannot be uninstalled. However, you can disable IPv6 in Windows Vista and Windows Server 2008 by doing one of the following: In the Network Connections folder, obtain properties on all of your connections and adapters and clear the check box next to the Internet Protocol version 6 (TCP/IPv6) components in the list.

This method disables IPv6 on your LAN interfaces and connections, but does not disable IPv6 on tunnel interfaces or the IPv6 loopback interface.

Reference : IPv6 for Microsoft Windows: Frequently Asked Questions

<http://www.microsoft.com/technet/network/ipv6/ipv6faq.msp>

### QUESTION NO: 13

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com has recently decided to make use of the IPv6 addressing scheme for the network using the range 131.107.x.x/6. with mask 255.255.224.0. CertKiller.com wants you to determine the number of valid IP addresses per range would be?

- A. The range 131.107.x.x/6 with mask 255.255.224.0 would have 254 valid IP addresses per range.
- B. The range 131.107.x.x/6 with mask 255.255.224.0 would have 2046 valid IP addresses per range.
- C. The range 131.107.x.x/6 with mask 255.255.224.0 would have 8190 valid IP addresses per range.
- D. The range 131.107.x.x/6 with mask 255.255.224.0 would have 1022 valid IP addresses per range.

**Answer: C**

#### Explanation:

With an address block of 172.16.0.0/22, you should be able to support 1022 hosts.

#### Incorrect Answers:

- A: If you are hosting 254 hosts, you should have an address block of 131.107.0.0 with a subnet mask of 255.255.255.0 or an address block of 172.20.43.0/24.
- B: If you are hosting 2046 hosts, you should have an address block of 10.4.32.0/21.
- D: If you are hosting 126 hosts, you should have an address block of 192.168.1.32 with a subnet mask of 255.255.255.128 or an address block of 10.12.200.128/25.

### QUESTION NO: 14

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

The CertKiller.com network currently contains six computers using the address space

172.16.1.0./29 using central computing services. During the course of the day CertKiller.com plans adding an additional ten computers to the network. CertKiller.com wants you to have the network expanded appropriately.

What should you do?

- A. You should consider having the network expanded to a /27 address block.
- B. You should consider having the network expanded to a /28 address block.
- C. You should consider having the network expanded to a /26 address block.
- D. You should consider having the network left as is since a /29 address block accommodates the growth.

**Answer: A**

**Explanation:**

The CertKiller.com written company policy states that the network should be granted address space as it needs. You need to expand the network to a /27 address block. This will support 32 addresses and 30 computers.

**Incorrect Answers:**

- B: If you expand the network to a /28 address block, you will support 16 addresses and 14 computers. This will not comply with CertKiller.com written company policy. You need an address block that will support the computers at CertKiller.com.
- C: If you expand the network to a /26 address block, you will support 64 addresses and 62 computers. This will not comply with CertKiller.com written company policy.
- D: If you expand the network to a /29 address block, you will support 8 addresses and 6 computers. This will not comply with CertKiller.com written company policy. You need an address block that will support the computers at CertKiller.com.

**QUESTION NO: 15**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day CertKiller.com deployed a computer named CERTKILLER-SR21 to be connected to the IPv6 Intranet. CertKiller.com wants you to configure CERTKILLER-SR21 with an appropriate IPV6 address type.

What should you do?

- A. You should consider having CERTKILLER-SR21 configured with a link-local address.

- B. You should consider having CERTKILLER-SR21 configured with a unique local address.
- C. You should consider having CERTKILLER-SR21 configured with a global address.
- D. You should consider having CERTKILLER-SR21 configured with a site-local address.

**Answer: B**

**Explanation:**

You should use a unique local address. These addresses are the same as the private addresses in the IPv4. These addresses are used on the subnets of private networks and are not accessible on the public Internet.

**Incorrect Answers:**

A: You should not use a link-local address. The link-local address is the same as the APIPA addresses. These addresses are nonroutable and it is only used on a local subnet.

C: You should not use a Global address. The Global addresses are the same as the public addresses which are used by IPv4.

D: You should not use a site-local address. Although it is a private address, it has been set on a path towards obsolescence. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.74, 75, 77

**QUESTION NO: 16**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day CertKiller.com decided to have a test IPv6 network created within the current network using three subnets in the test network.

What should you do?

- A. You should consider having the test network configured with Global addresses.
- B. You should consider having the test network configured with Link-local addresses.
- C. You should consider having the test network configured with unique local addresses.
- D. You should consider having the test network configured with Site-local addresses.

**Answer: C**

**Explanation:**

The unique local address is the best option. These addresses are the same as the private addresses in the IPv4 however; it is used on the subnets of private networks and is not accessible on the public Internet.

**Incorrect Answers:**

A: You should not use a Global address in the test environment. The Global addresses are the same as the public addresses which are used by IPv4.

B: You should not use a link-local address in the test environment. The link-local address is the same as the APIPA addresses. These addresses are nonroutable and it is only used on a local subnet.

D: The site-local address is a private address. It will be useless to use it in a test environment because the site-local address has been set on a path towards obsolescence. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.74, 75, 77

**QUESTION NO: 17**

You are the newly appointed enterprise administrator at CertKiller.com. The corporate network of the company consists of a single Active Directory domain. All workstations are members of the Active Directory domain. All servers on the network are configured to run Windows Server 2008.

The company makes use of private networks to access resources on the Internet and other public networks. CertKiller.com currently makes use of IPv4. You are in the process of up a communication server for the company.

Due to company growth CertKiller.com requires additional globally public IPv4 addresses to accommodate clients accessing the Internet. You need to determine a method that is not complicated as well as cost effective.

What should you do?

- A. You should consider enabling NAT technology on the workstations on the network.
- B. You should consider converting the current setup to accommodate IPv6 as it is supported by Windows Server 2008.
- C. You should consider deploying a Proxy server.
- D. None of the above.

**Answer: A**

**Explanation:**

Your best option in this scenario would be to enable the NAT technology on the computers on the network. NAT was designed to be the solution for SOHO networking situations that encompasses IPv4.

**Incorrect Answers:**

B: This option can be feasible with Windows Server 2008. The transition is very complicated and not cost effective. Reference: Syngress - The Real MCTS-MCITP 70-649 Prep Kit - Independent



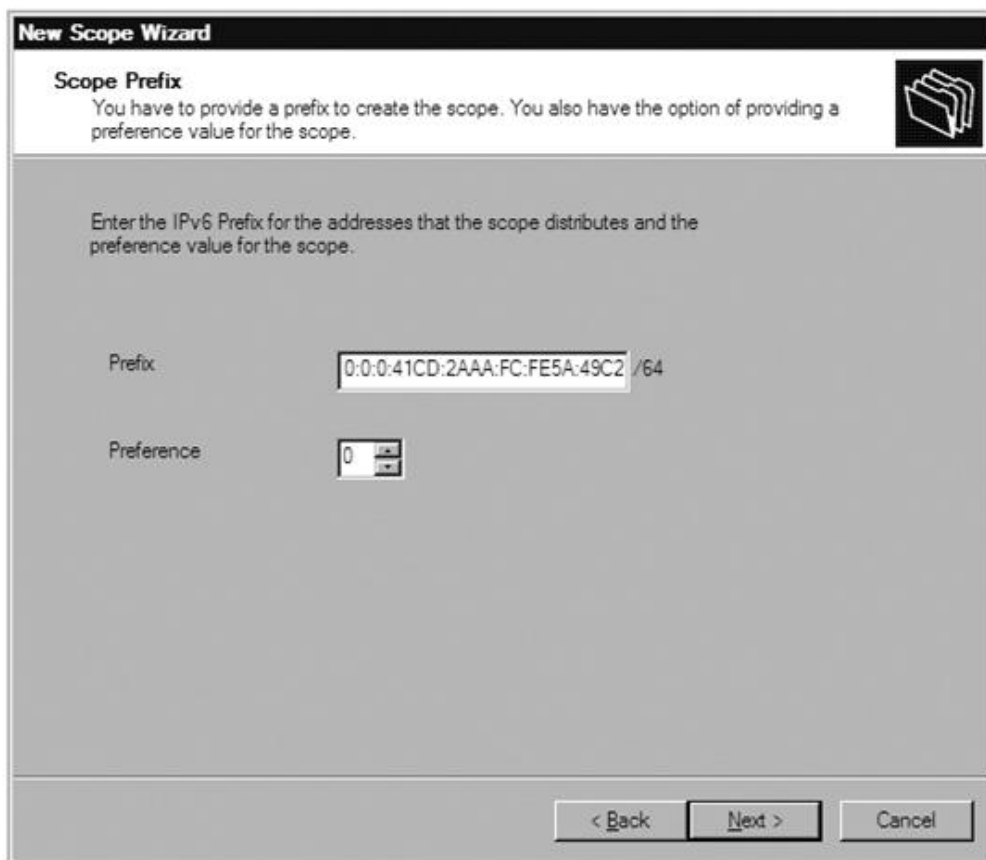
and Complete Self-Paced Solutions

C: Setting up a Proxy server is much harder than that of NAT.

### QUESTION NO: 18

You are an enterprise administrator for CertKiller.com. The company runs Windows Server 2008 on all the servers on the network.

The company network contains a Windows Server 2008 DHCP Server role. You open the server role and view the scope settings of a user. The diagram below displays the scope settings:



The image shows a screenshot of the 'New Scope Wizard' window in Windows Server 2008. The title bar says 'New Scope Wizard'. The main heading is 'Scope Prefix'. Below the heading, it says: 'You have to provide a prefix to create the scope. You also have the option of providing a preference value for the scope.' There is a folder icon in the top right corner. The main area contains the instruction: 'Enter the IPv6 Prefix for the addresses that the scope distributes and the preference value for the scope.' There are two input fields: 'Prefix' and 'Preference'. The 'Prefix' field contains the text '0:0:0:41CD:2AAA:FC:FE5A:49C2 /64'. The 'Preference' field contains the value '0'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Determine the statements that are true based on the data displayed in the diagram? (Choose all that apply.)

- A. The Prefix Value in the diagram is too long. It should contain fewer digits.
- B. The Preference Value in the diagram is incorrect. You need to set it to 1 for all addresses that make use of the /64 option.
- C. The Prefix Value as well as the Preference Value in the diagram is correct.
- D. The Prefix Value in the diagram is incorrect. The value cannot start with 0:0:0:.

**Answer: A,D**

**Explanation:**

The Prefix Value should contain the prefix for the addresses the scope distributes. /64 signify that 64 bits are used for the network address. In IPv6 every number will represent 16. /64 will signify that the prefix has to be 4 digits.

**Incorrect Answers:**

B: You are able to set the Preference Value to 0. The Preference Value identifies the preferred order in which the addresses will be distributed to the host. A 0 Preference will be handed out prior to the Preference 1 address.

C: The Prefix Value is incorrect. Reference: Syngress - The Real MCTS-MCITP 70-649 Prep Kit - Independent and Complete Self-Paced Solutions

**QUESTION NO: 19**

You are an enterprise administrator for CertKiller.com. The company runs Windows Server 2008 on all the servers on the network.

A manager in the development department wants to make use of IPv6. You thus decide to create a test IPv6 network in the company. The test network has to encompass three subnets. Determine the IPv6 address type you require?

- A. Link-local addresses.
- B. Site-local addresses.
- C. Global addresses.
- D. Unique local addresses.

**Answer: D**

**Explanation:**

You will require unique local addresses in this scenario. These addresses resemble the private address ranges in IPv4. It is also used for private routing within the organization.

**Incorrect Answers:**

A: Link local addresses are not routable. It will thus not result in the subnets intercommunicating.

B: It is a way to provide routing within a private network. It has however been deprecated.

C: You make use of global addresses when you want the network to connect to the public IPv6 network. Reference: Syngress - The Real MCTS-MCITP 70-649 Prep Kit - Independent and Complete Self-Paced Solutions

**QUESTION NO: 20**

You are the newly appointed enterprise administrator at CertKiller.com. The corporate network of the company consists of a single Active Directory domain. All workstations are members of the Active Directory domain. All servers on the network are configured to run Windows Server 2008.

You are responsible for managing a Windows Server 2008 workstation named CERTKILLER-SR01. You receive an instruction from the CIO to connect CERTKILLER-SR01 to the Ipv6 Internet. In order to execute the instruction an IPv6 address is required. You need to identify the appropriate IPv6 address that is required in this scenario.

What should you do?

- A. You need to make use of a unique address.
- B. You need to make use of a site-local address.
- C. You need to make use of a link-local address.
- D. You need to make use of a global address.

**Answer: D**

**Explanation:**

Your best option in this scenario would be to make use of a global address. Global addresses are routable addresses. You make use of global addresses when you want the network to connect to the public IPv6 network. You can also make use of a global address when you want a static IPv6 address to which computers are able to connect across the IPv6 Internet.

**Incorrect Answers:**

- A: Unique local addresses are routable. You cannot be used on a public network.
  - B: The site-local address is a version of the unique local address. However, it is being phased out.
  - C: Link local addresses are not routable. You cannot be used on a public network.
- Reference:  
Syngress - The Real MCTS-MCITP 70-649 Prep Kit - Independent and Complete Self-Paced Solutions Part 2, Configure Dynamic Host Configuration Protocol (20 Questions)

**QUESTION NO: 21**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com recently deployed a computer named CERTKILLER-SR21 as the network DHCP server.

During the course of the day the network clients started reporting that the client computers are not receiving IP addresses from CERTKILLER-SR21 but receive the IP range 169.168.x.x. You have later discovered that CERTKILLER-SR21 has stopped and the settings were configured properly. CertKiller.com wants you to ensure that CERTKILLER-SR21 is not stopped allowing client computers to obtain proper IP addresses from CERTKILLER-SR21.

What should you do?

- A. You should consider having CERTKILLER-SR21 restarted.
- B. You should consider having CERTKILLER-SR21 authorized to assign IP addresses to client computers.
- C. You should consider having CERTKILLER-SR21 reconfigured to assign IP addresses to all client computers using DNS settings.
- D. You should consider having the DHCP server service restarted on CERTKILLER-SR21.
- E. You should consider having a scope configured on CERTKILLER-SR21.

**Answer: B**

**Explanation:**

To make sure that the CKDHCP server is not stopped, you should authorize the DHCP server to assign IP addresses to client computers. DHCP assigns IP addresses, Default gateway and DNS servers to the DHCP-enabled clients. To ensure that the client machines receive their IP addresses and all related configuration, you should authorize the DHCP server. In fact you should authorize the DHCP server as soon as you install it. The easiest way to do this is to install DHCP server on a machine that is running as a domain controller. The server is automatically authorized when you add the DHCP server for the first time.

**QUESTION NO: 22**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com has recently planed the deployment of a computer named CERTKILLER-SR01 configured with the DHCP service providing client computers with IP addressing information automatically. CertKiller.com wants you to have CERTKILLER-SR01 installed with the DHCP service whilst ensuring it is automatically authorized.

What should you do?

- A. You should consider having CERTKILLER-SR01 configured as a domain controller before installing DHCP.
- B. You should consider having CERTKILLER-SR01 configured as a member server and create a scope to access the domain controller.
- C. You should consider having CERTKILLER-SR01 configured as a stand-alone server before installing DHCP.
- D. You should consider having CERTKILLER-SR01 configured as a member of the domain before installing DHCP.

**Answer: A**

**Explanation:**

The correct option is A. you should install the DHCP server on a domain controller. The DHCP server dynamically allocates IP addresses and other related configurations to DHCP-enabled clients. You have to authorize the DHCP server to ensure that the DHCP is able to assign IP addresses to client computers. A DHCP server that is not authorized in your enterprise will not be able to function properly and will be stopped. But when you install the DHCP server on a computer that runs as a domain controller, the server is automatically authorized when you add the server to the DHCP console for the first time.

**QUESTION NO: 23**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as the Dynamic Host Configuration Protocol (DHCP) server. During the course of the day you receive instruction from CertKiller.com to ensure that no IP address of configuration settings are automatically assigned to DHCP clients on a subnet which does not make use of DHCPv6 provided by CERTKILLER-SR01.

What should you do?

- A. You should consider having the Managed Address Configuration to 1 and Other Stateful Configuration flag set to 0
- B. You should consider having the both Managed Address Configuration to 0 and Other Stateful Configuration flag set to 1
- C. You should consider having both the both Managed Address Configuration and Other Stateful Configuration flag set to 1.
- D. You should consider having both the Managed Address Configuration and Other Stateful Configuration flag set to 0.

**Answer: D**

**Explanation:**

To ensure that neither IP address nor other configuration settings are automatically allocated to DHCP clients on a subnet that does not use DHCPv6 from CertKillerDHCP1, you need to set both Managed Address Configuration and Other Stateful Configuration flag to 0. The combination of both M and O flags set to 0 corresponds to a network without a DHCPv6 infrastructure.

Reference : The Cable Guy the DHCPv6 Protocol

<http://technet.microsoft.com/en-us/magazine/cc162485.aspx>

**QUESTION NO: 24**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 as the network DNS server. During the course of the day you receive instruction from CertKiller.com to deploy two servers to the network configured as DHCP servers.

The CertKiller.com network users recently started reporting that they are unable to log onto the domain after you changed the IP address of CERTKILLER-SR01. CertKiller.com wants you to ensure that the network users are able to log onto the domain.

What should you do?

- A. You should consider having ipconfig/registerdns command run at the command prompt of the DHCP servers.
- B. You should consider having the network settings for workstations configured to Disable NetBIOS over TCP/IP.
- C. You should consider having the Netlogon service restarted on the DHCP servers.
- D. You should consider having the DHCP scope option 006 DNS - Servers reconfigured with the new IP address of CERTKILLER-SR01.

**Answer: D**

**Explanation:**

To ensure that users are able to log on to the domain, you need to reconfigure the DHCP scope option 006 DNS - Servers with the IP addresses of new DNS servers because this option allows you to define IP addresses for one or more DNS servers to be used by the DHCP clients.

Reference: Using Dynamic Host Configuration Protocol / Setting DHCP Options

[http://www.intranetjournal.com/articles/200004/im\\_dhcp.html](http://www.intranetjournal.com/articles/200004/im_dhcp.html)

**QUESTION NO: 25**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server

2008 and the client computers run Microsoft Windows Vista.

CertKiller.com recently deployed a server named CERTKILLER-SR01 which has the DHCP Server role installed and CERTKILLER-WS01 client computer. The configuration of the deployed computers is shown in the table below:

During the course of the day a network user named Rory Allen complains that CERTKILLER-WS01 is not receiving IP addressing information from CERTKILLER-SR01. You have later opened Microsoft Network Monitor 3.0 on CERTKILLER-SR01 and enabled the P-mode. CertKiller.com wants you to capture only DHCP server related traffic between CERTKILLER-SR01 and CERTKILLER-WS01.

What should you do?

- A. You should consider using the IPv4.Address == 169.253.98.22 && DHCP to build a filter in Network Monitor.
- B. You should consider using the Ethernet. Address == 0x00103A4D5423 && DHCP to build a filter in Network Monitor.
- C. You should consider using the IPv4.Address == 169.253.98.22 && DHCP to build a filter in Network Monitor.
- D. You should consider using the IPv4.Address == 192.168.1.109 && DHCP to build a filter in Network Monitor.

**Answer: C**

**Explanation:**

:

In order to capture traffic between two hosts that are on the same hub or logical VLAN (layer 2) the computer running NM would configure a filter that looks for traffic from the other host only and then in addition you can further filter by protocol. Therefore you would actually look to build the filter

"IPv4.Address == 192.168.1.109 && DHCP"

If you use the 169.253.98.22 && DHCP, then all DHCP traffic going to the DHCP server will be displayed and it will be very difficult to separate out traffic for the individual host.

## QUESTION NO: 26

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest containing a single domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.



CertKiller.com recently deployed a computer named CERTKILLER-SR01 which has the DHCP Server role installed. CERTKILLER-SR01 provides IP addresses for 20 client computers. CertKiller.com has grown in its capacity and had to add an additional DHCP server named CERTKILLER-SR02 to accommodate all the new client computers. The CertKiller.com CIO has been assigned a new client computer named CERTKILLER-WS21. CertKiller.com wants you to ensure that CERTKILLER-WS21 receives its client reservation from CERTKILLER-SR02.

What should you do?

- A. You should consider having the DHCP reservation for CERTKILLER-WS21 added to CERTKILLER-SR02.
- B. You should consider having CERTKILLER-SR01 and CERTKILLER-SR02 added to the RAS and IAS Servers group.
- C. You should consider having the netsh add helper command run on CERTKILLER-WS21.
- D. You should consider having the ipconfig /renew command run on CERTKILLER-WS21.

**Answer: A**

**Explanation:**

:

A reservation is a specific IP addresses that is tied to a certain device through its MAC address. By adding a reservation, you ensure that a machine always receives the same IP address from the DHCP server.

In the above scenario you need to simply add the DHCP reservation for CertKillerPTC1 to the second DHCP server also, so that the same reservation is available on the other DHCP server also.

Reference : Configure a DHCP server in Windows Server 2008

<http://www.zdnetindia.com/index.php?action=articleDescription&prodid=18616>

Reference : DHCP Reservations and Exclusions

<http://www.windowsnetworking.com/kbase/WindowsTips/Windows2003/AdminTips/Network/DHCP/ReservationsandExclusions.html>

## QUESTION NO: 27

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com recently deployed four servers configured with the DNS role and assigned a static IP address. During the course of the day CertKiller.com instruct you to install an additional server named CERTKILLER-SR01 configured as the DHCP server. CertKiller.com wants you to prevent CERTKILLER-SR01 from assigning the IP addresses of the DNS servers to the client computers.

What should you do?

- A. You should consider having CERTKILLER-SR01 configured with an exclusion which contains the IP addresses of the four DNS servers.
- B. You should consider having CERTKILLER-SR01 configured with a new scope for the DNS servers.
- C. You should consider having CERTKILLER-SR01 configured with an exclusion which contains the IP address of CERTKILLER-SR01.
- D. You should consider having the 005 Name Servers scope option configured on CERTKILLER-SR01.

**Answer: A**

**Explanation:**

To prevent CERTKILLER-SR01 from assigning the addresses of the DNS servers to DHCP clients, you need to configure an exclusion that contains the IP addresses of the four DNS servers. An exclusion is an address or range of addresses taken from a DHCP scope that the DHCP server is not allowed to hand out.

Reference : DHCP Reservations and Exclusions

<http://www.windowsnetworking.com/kbase/WindowsTips/Windows2003/AdminTips/Network/DHCP/ReservationsandExclusions.html>

**QUESTION NO: 28**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as the DHCP server. During the course of the business day you receive instruction from CertKiller.com to have the size of the DHCP database on CERTKILLER-SR01 reduced.

What should you do?

- A. You should consider having the database reconciled using the DHCP snap-in.
- B. You should consider having the `jetpack.exe dhcp.mdb temp.mdb` command run from the folder that holds the DHCP database.
- C. You should consider enabling the File is ready for archiving attribute from the properties of `dhcp.mdb` file.
- D. You should consider enabling the Compress contents to save disk space attribute from the properties of `dhcp.mdb` file.

**Answer: B**

**Explanation:**

To reduce the size of the DHCP database, you need to use `jetpack dhcp.mdb temp.mdb` command. (The file `temp.mdb` is used as a temporary database during the compacting operation.) After the database is compacted, the message: 'Jetpack completed successfully' appears.

Reference : Section B: Migrate scopes and settings to the Management Server Prepare your DHCP server environment and export your DHCP server configuration  
<http://technet.microsoft.com/en-us/library/cc463365.aspx>

**QUESTION NO: 29**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami and branch office located in Toronto.

The offices are connected through a WAN link. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com has decided to deploy a DHCP server named CERTKILLER-SR01 to the network for assigning IPv4 address at the Miami office whilst the Toronto office users use static IP addresses and are located on another subnet. CertKiller.com wants you to have the portable computers configured to access resources located at both offices.

What should you do?

- A. You should consider having each of the portable computers configured with an alternate configuration containing a static IP address in the range used at the Miami office.
- B. You should consider having each of the portable computers configured with an alternate configuration that contains a static IP address in the range used at the Toronto office.
- C. You should consider having the address assigned by CERTKILLER-SR01 configured as a static IP address on each of the portable computers.
- D. You should consider having each of the portable computers configured to use a static IPv4 address in the range used at the Toronto office.

**Answer: B**

**Explanation:**

To ensure that the portable computers can connect to network resources at the head office and the branch office, you should configure each portable computer using an alternate configuration that contains a static IP address in the range used at the branch office.

Alternate Configuration functionality can be used to establish multiple-network connectivity. This feature specifies that TCP/IP uses an alternative configuration if a DHCP server is not found. The Alternate Configuration functionality is useful in situations where you use the computer on more than one network, where one of those networks does not have a DHCP server and you do not want to use an automatic private Internet protocol (IP) addressing configuration.

You can use the Alternate Configuration functionality if you use a mobile computer at your office and at your home. When you are in the office, the computer uses a DHCP-allocated TCP/IP configuration. When you are at home (where you do not have access to a DHCP server), the computer automatically uses the alternative configuration. Similarly you can configure alternate configuration that contains a static IP address in the range used at the branch office to connect portable computers to the network resources at the main office and the branch office

Reference : How to use the Alternate Configuration feature for multiple network connectivity in Windows XP

<http://support.microsoft.com/kb/283676>

**QUESTION NO: 30**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com recently deployed two servers to the network named CERTKILLER-SR01 and CERTKILLER-SR02 respectively. CERTKILLER-SR01 is used as the DHCP server and CERTKILLER-SR02 is used as the application server. CertKiller.com is currently configured with a single scope. CertKiller.com wants you to ensure that CERTKILLER-SR02 always receives the same IP address and DNS settings as well as WINS settings from CERTKILLER-SR01.

What should you do?

- A. You should consider adding an exclusion range in the DHCP scope on CERTKILLER-SR01.
- B. You should consider having CERTKILLER-SR01 configured with a multicast scope.

- C. You should consider adding an additional static IP address on CERTKILLER-SR01 for CERTKILLER-SR02.
- D. You should consider adding a DHCP reservation in the DHCP scope on CERTKILLER-SR01.

**Answer: D**

**Explanation:**

To ensure that CERTKILLER-SR02 always receives the same IP address. CERTKILLER-SR02 must receive its DNS settings and its WINS settings from CERTKILLER-SR01, you need to create a DHCP reservation in the DHCP scope.

A reservation is a specific IP addresses that is tied to a certain device through its MAC address. By adding a reservation, you ensure that a machine always receives the same IP address from CERTKILLER-SR01.

Reference : Configure a DHCP server in Windows Server 2008

<http://www.zdnetindia.com/index.php?action=articleDescription&prodid=18616>

Reference : DHCP Reservations and Exclusions

<http://www.windowsnetworking.com/kbase/WindowsTips/Windows2003/AdminTips/Network/DHCP/ReservationsandExclusions.html>

**QUESTION NO: 31**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com which has the functional level of the domain set at Windows Server 2003. CertKiller.com currently has their headquarters located in Miami.

CertKiller.com has recently deployed a server to the network named CERTKILLER-SR01 configured as a member server running the DHCP service. During the course of the day you receive instruction from CertKiller.com to start the DHCP service and it fails. CertKiller.com wants you to ensure that the DHCP service starts on CERTKILLER-SR01.

What should you do?

- A. You should consider having CERTKILLER-SR01 rebooted.
- B. You should consider having the scope activated on CERTKILLER-SR01.
- C. You should consider having CERTKILLER-SR01 configured with a scope to assign IP addresses.
- D. You should consider having CERTKILLER-SR01 authorized in the Active Directory domain to assign IP addresses.

**Answer: D**

**Explanation:**

To ensure that the DHCP service starts, you need to authorize CertKillerDHCP1 in the Active Directory domain. This procedure is needed because you are running a DHCP server on a member server.

Reference : Authorize a DHCP server in Active Directory

<http://technet2.microsoft.com/windowsserver/en/library/9f713d6c-d7e5-42a0-87f7-43dbf86a17301033.mspx?mfr=true>

**QUESTION NO: 32**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

The client computers on the subnet in the Toronto office is configured to make use of IP addresses in the 169.254.x.x range. During the course of the business day you receive complaints from the Toronto office users about being unable to access shared resources in the Miami office. CertKiller.com wants you to address the access issues experienced by the users in the Toronto office.

What should you do?

- A. You should consider having a DHCP broadcast agent configured on a member server in the Miami office.
- B. You should consider having a DHCP relay agent configured on a member server in the Toronto office.
- C. You should consider having the Resource Relay Address DHCP server option included in the Miami office server IP address range.
- D. You should consider having the Resource Location Servers DHCP server option included in the Miami office server IP address range.

**Answer: B**

**Explanation:**

To ensure that computers can connect to shared resources in both the head office and the branch office, you need to configure a DHCP relay agent on a member server in the branch office. The computers in the branch office have IP addresses in the range of 169.254.x.x because the clients were not able to contact a DHCP server and obtain an IP address lease. This is because the

DHCP server may be unavailable to the branch office computers, which are on the other LAN. A DHCP server can provide IP addresses to client computers on other LANs only if a DHCP relay agent is available.

Reference : Chapter 5: Implementing the Dynamic Host Configuration Protocolcontinued / DHCP Servers Do Not Provide IP Addresses

<http://www.microsoft.com/mspress/books/sampchap/6371a.aspx>

### QUESTION NO: 33

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com recently deployed a server to the network named CERTKILLER-SR01 configured as the DHCP server.

During the course of the business week you discovered that CERTKILLER-SR01 has failed. You later received instruction from CertKiller.com to restore the DHCP database using the recent backup. CertKiller.com wants you to ensure that the DHCP clients will not receive IP addresses currently in use on the network.

What should you do?

- A. You should consider having the Conflict Detection value set to 0.
- B. You should consider having the Conflict Detection value set to 1.
- C. You should consider having the Conflict Detection value set to 2.
- D. You should consider having the DHCP server option set to 15.

**Answer: B,C**

#### **Explanation:**

To prevent DHCP clients from receiving IP addresses that are currently in use on the network, you need to set the Conflict Detection value to 1 or 2. By default, "Conflict detection attempts" is set to 0, which means that DHCP server should not check the addresses that it is assigning to its clients.

When this value is increased to the value of 1 or 2, this would enable the DHCP server to check once or twice to determine whether the address is in use before giving it to a client

Reference : How can I enable conflict detection on my DHCP server?

<http://windowsitpro.com/article/articleid/47133/how-can-i-enable-conflict-detection-on-my-dhcp-server.html>



**QUESTION NO: 34**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com recently deployed a server to the network named CERTKILLER-SR01 configured as a DHCP server which has two local area network connections named King Area 1 and King Area 2 respectively. During the course of the day you receive instruction from CertKiller.com to prevent CERTKILLER-SR01 from responding to DHCP client requests on King Area 2 whilst allowing non-DHCP client requests on King Area 2.

What should you do?

- A. You should consider having a new multicast scope added using the DHCP snap-in.
- B. You should consider having the bindings modified to associate only King Area 1 with the DHCP service using the DHCP snap-in.
- C. You should consider having the metric value set to 1 in the properties of the King Area 2 network connection.
- D. You should consider having the metric value set to 1 in the properties of the King Area 1 network connection.

**Answer: B**

**Explanation:**

To prevent the CertKillerDHCP1 from responding to DHCP client requests on LAN2 while allowing it to continue to respond to non-DHCP client requests on LAN2, you need to modify the bindings to associate only LAN1 with the DHCP service from the DHCP snap-in.

The Change Server Connection Bindings option in DHCP Snap-in allows you to view the connections through which the DHCP server is providing addresses. If you have multiple network adapters in a DHCP server, can configure DHCP for only selected interfaces. You can click the Bindings button to view and configure the binding on your computer.

Reference : Implementing, Managing, and Troubleshooting DHCP/ DHCP Server Common Commands

<http://www.informit.com/articles/article.aspx?p=684650&seqNum=5>

**QUESTION NO: 35**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com has recently deployed a server named CERTKILLER-SR01 which runs the DHCP service for the newly created 172.14.28.0/22 subnet. During the course of the day you discover that none of the DHCP clients are able to communicate outside the local subnet when the IP address of the computer on the network is specified.

You have later discovered some network clients have statically assigned IP address and are able to communicate outside the local subnet. CertKiller.com wants you to configure CERTKILLER-SR01 to ensure that the DHCP clients are able to communicate outside the local subnet.

What should you do?

- A. You should consider having the 006 DNS Servers option configured.
- B. You should consider having the 003 Router option configured.
- C. You should consider having the 044 WINS/NBNS Servers option configured.
- D. You should consider having the 015 Domain Name option configured.

**Answer: B**

**Explanation:**

The 003 Router option will allow DHCP client computers to communicate outside the local subnet.

**Incorrect Answers:**

- A: The 006 DNS Servers option is used for DNS name servers whereby the DHCP clients can resolve domain name queries.
- C: The 044 WINS/NBNS Servers option is used for primary and secondary WINS servers.
- D: You should not use the 015 Domain Name option. This actually specifies the domain name that the DHCP clients should use. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp. 221

**QUESTION NO: 36**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01.msft as the DHCP server with the IP address 192.168.0.5 and DNS server address of 192.168.1.0. During the course of the day you create a scope range of 192.168.1.0/24 for network client computers.

The network users on a local subnet recently reported that they are not receiving IP leases from CERTKILLER-SR01.msft but receive they receive the APIPA range 169.254.0.0/16. CertKiller.com wants you to configure CERTKILLER-SR01.msft to successfully lease the scope range created on the local subnet.

What should you do?

- A. You should consider having the DHCP client service enabled on CERTKILLER-SR01.msft.
- B. You should consider having the client computers configured as DHCP clients.
- C. You should consider having the Ipconfig /registerdns command run on CERTKILLER-SR01.msft.
- D. You should consider having CERTKILLER-SR01.msft redeployed after changing its IP address to match the range it is trying to distribute.

**Answer: D**

**Explanation:**

You should redeploy CertKillerDHCP1.msft after changing the address of the server. CertKillerDHCP1.msft is configured with a static IP address of 192.168.0.5/24. This will let CertKillerDHCP1.msft to lease addresses in that range. So you need to redeploy CertKillerDHCP1.msft after changing the address of the server.

**Incorrect Answers:**

- A: CertKillerDHCP1.msft is not acting as a DHCP client. So it does not need those services.
- B: The client computers already have an address in the APIPA range. So they are already set up as DHCP clients.
- C: If you run the Ipconfig /registerdns on CertKillerDHCP1.msft, it will allow other computers to connect to it by stating CertKillerDHCP1.msft. Although the computer now can connect to the server, it does not mean that the DHCP will work properly.

**QUESTION NO: 37**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com has recently deployed a server named CERTKILLER-SR01 configured with the DHCP service on the network to lease IP addresses using the range 172.14.1.0/24. CertKiller.com has additionally added a member server to the subnet configured as a DNS server using the static IP address 172.14.1.100. During the course of the day you receive instruction from CertKiller.com to have a scope created on CERTKILLER-SR01 which will not conflict of the member DNS servers

IP address.

What should you do?

- A. You should consider having a reservation created to assign the address 172.14.1.100 to the member DNS server.
- B. You should consider having the 006 DNS Servers option used to assign the client computers the member DNS servers address.
- C. You should consider having an exclusion for the 172.14.1.100 address created.
- D. You should consider having two scopes configured which avoids the 172.14.1.100 address.

**Answer: C**

**Explanation:**

You should create an exclusion for the 172.14.1.100 address. When it is created CertKillerDHCP1 will not lease the address. Furthermore the DNS server will keep its static configuration.

**Incorrect Answers:**

- A: You cannot create reservation to assign the address 172.14.1.100 to the member DNS server. A DNS server should have a static address.
- B: Assigning the 006 DNS Servers option, will not stop the conflict of the scope leasing.
- D: You cannot create two scopes to avoid the 172.14.1.100 address. One contiguous address range can only run on one scope.

**QUESTION NO: 38**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami.

The CertKiller.com network servers run Microsoft Windows Server 2008 Core and the client computers run Microsoft Windows Vista. During the course of the business day CertKiller.com deployed a server to the network named CERTKILLER-SR01 which has the DHCP server role installed. CertKiller.com wants you to have the member server configured as the DHCP server.

What should you do?

- A. You should consider having the `sc config dhcpserver start= auto` command run.
- B. You should consider having the `start /w ocsetup DHCPServer` command run.
- C. You should consider having the `servermanagercmd -install dhcp` command run.
- D. You should consider having the `net start DHCPServer` command run.

**Answer: B**

**Explanation:**

Because CertKiller.com is using a Microsoft Windows Server 2008 Core, you can install a DNS role on CertKillerServer1 by running the following command: `start /w ocsetup DNS-Server-Corer-Role`.

**Incorrect Answers:**

A: The `sc config dhcpserver start= auto` command is then used to automatically start the DHCP Service server for configuration.

C: The `servermanagercmd -install dhcp` command will not work on a Server Core installation.

D: You cannot configure a member server as a DHCP server with the `net start DHCPService` command. You can only use this command to start this service for the first time when you used the `start /w ocsetup DHCPService` command. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp. 126, 221, 245

**QUESTION NO: 39**

You are employed as the network administrator at CertKiller.com. All servers on the network are configured to run Windows Server 2008.

You are assigned a DHCP server named CERTKILLER-SR01. You setup a new subnet using CERTKILLER-SR01. You receive numerous complaints from users stating that they are unable to log onto the network when they are locally connected. You receive an instruction from the CIO to resolve the matter urgently. You decide to check the DHCP settings in order to resolve the queries.

What should you do?

- A. Your best option would be to check the scope settings of CERTKILLER-SR01.
- B. Your best option would be to check the exclusions on CERTKILLER-SR01.
- C. Your best option would be to check the subnet mask of the default gateway on CERTKILLER-SR01.
- D. Your best option would be to check the lease duration of CERTKILLER-SR01.

**Answer: D****Explanation:**

Your best option in this scenario would be to check the lease duration of CERTKILLER-SR01. When only mobile users complain that they are unable to log on you need to limit the search relating to mobile users. Long lease IP addresses results in it being not available to mobile users. Mobile users that are issued with an IP address when they connect can keep it if they disconnect for an extended period of time. When others log on and try to get an IP configuration setting no IP addresses will be available to assign to them. It is thus best to have a short lease duration

especially when there are numerous mobile users on the network.

**Incorrect Answers:**

A: There is not a problem with the scope settings. The scenario states that certain users are unable to get a connection when they are locally connected.

B: Exclusions do not impact mobile users. Checking the exclusions on CERTKILLER-SR01 is thus incorrect.

C: If an error occurred with the subnet mask of the default gateway settings all users on the company network will experience problems logging onto the network. Reference:

Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 40**

You work as a network administrator at CertKiller.com. You are in the process of installing Windows Server 2008. CertKiller.com has its headquarters in Paris and a branch office in London. There are both desktop and laptop workstations in operation at CertKiller.com.

You receive an instruction from the CIO to install Windows Server 2008 on a computer named CERTKILLER-SR09 located at the London office. You install the DHCP role on CERTKILLER-SR09. You need to accomplish this without causing any downtime. You thus need to determine the appropriate scope settings that will achieve this.

What should you do?

- A. You should consider removing the network connection of CERTKILLER-SR09 prior to installing DHCP.
- B. You should consider adding an additional DHCP server on the network.
- C. You should consider configuring CERTKILLER-SR09 as a DHCP relay agent since only one DHCP server is allowed on a network.
- D. You should consider authorizing CERTKILLER-SR09 in Active Directory prior to executing the DHCP role.

**Answer: D**

**Explanation:**

Your best option in this scenario would be to authorize CERTKILLER-SR09 in Active Directory prior to executing the DHCP role. The DHCP server role can be installed without activating the server. CERTKILLER-SR09 needs to be authorized via Active Directory before it will be allowed to function as a DHCP server on the CertKiller.com network.

**Incorrect Answers:**

A: You are able to install the DHCP role on a server that is attached to the network. The default setting is that the role can be installed and not be activated. Once the role is activated you need to authorize it in the Active Directory.

B: This option is incorrect. A new DHCP server can take down the network if the scope settings are wrong.

C: This option is incorrect. You are allowed more than one DHCP server on the network. DHCP relay agents are routers and switches designed to forward DHCP traffic. Reference:

Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008 Part 3, Configure routing (17 Questions)

#### QUESTION NO: 41

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently has the Toronto office connected to the Miami office.

During the course of the day you receive instruction from CertKiller.com to temporarily connect the Toronto office to the Miami office corporate network by adding a route directing traffic to the network 192.61.0.0 subnet mask 255.255.255.0. CertKiller.com additionally wants you to ensure that the next hop in the IP routing table being 192.33.0.1.

What should you do?

- A. You should consider having the route -4 192.61.0.0 subnet mask: 255.255.255.0 192.33.0.1 command run.
- B. You should consider having the route add 192.61.0.0 subnet mask: 255.255.255.0 192.33.0.1 metric 45 command run.
- C. You should consider having the route add 192.61.0.0 subnet mask: 255.255.255.0 192.33.0.1 command run.
- D. You should consider having the route -p add 192.61.0.0 subnet mask: 255.255.255.0 192.33.0.1 command run.

**Answer: C**

#### Explanation:

To add a route in the IP routing table, you should use 192.61.0.0 subnet mask: 255.255.255.0 192.33.0.1 command. The destination server address is 192.61.0.0 with a subnet mask of 255.255.255.0 along with the next hop address of 192.33.0.1.

Basically the route command is used to change or view the entries in the local routing table. The full command syntax for this specific task is

route [-f] [-p] [ Command [ Destination ] [mask Netmask] [ Gateway ] [metric Metric] ] [if Interface ]



The -f parameter issues a command to the Windows to clear all gateway entries in the routing table. The -p command is used to make a specific route persistent. When the server is rebooted, all routes configured through the route command are erased from the IP routing table. If you use the -p parameter, the route command instructs Windows to retain and keep the route in the IP routing table even if the server is rebooted.

**Incorrect Answers:**

A: These options are invalid in this scenario. If you use only the -p parameter along with this route commands. The command will not be executed because you haven't cleared the gateway entries in the IP routing table. Similarly if you use only -f, this route entry will be erased if the server is rebooted.

B: These options are invalid in this scenario. If you use only the -p parameter along with this route commands. The command will not be executed because you haven't cleared the gateway entries in the IP routing table. Similarly if you use only -f, this route entry will be erased if the server is rebooted.

D: These options are invalid in this scenario. If you use only the -p parameter along with this route commands. The command will not be executed because you haven't cleared the gateway entries in the IP routing table. Similarly if you use only -f, this route entry will be erased if the server is rebooted.

**QUESTION NO: 42**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day you receive complaints from the network users in the Miami office about not being able to access resources located in the Toronto office. You later decided to make use of the route print command and discover an incorrect entry 192.23.0.0 255.255.255.0 in the routing table. CertKiller.com wants you to restore connectivity between the offices.

What should you do?

A. You should consider having the wrong entry deleted from the routing table by using route delete 192.23.0.0 255.255.255.0 command.

B. You should consider having the incorrect entry deleted from the routing table by using route \*224\* command.

C. You should consider having the wrong entry, 10.23.0.0 255.255.0.0 deleted in the routing table by using the route -p command.

D. You should consider having all entries in the routing table deleted by using route -delete on each entry.

**Answer: A**

**Explanation:**

To restore the connectivity between the main office and the branch office network, you should first delete the wrong entry from the routing table using the route -delete 192.23.0.0 255.255.255.0. After deleting the entry, you can use the route -add command to add the correct entry.

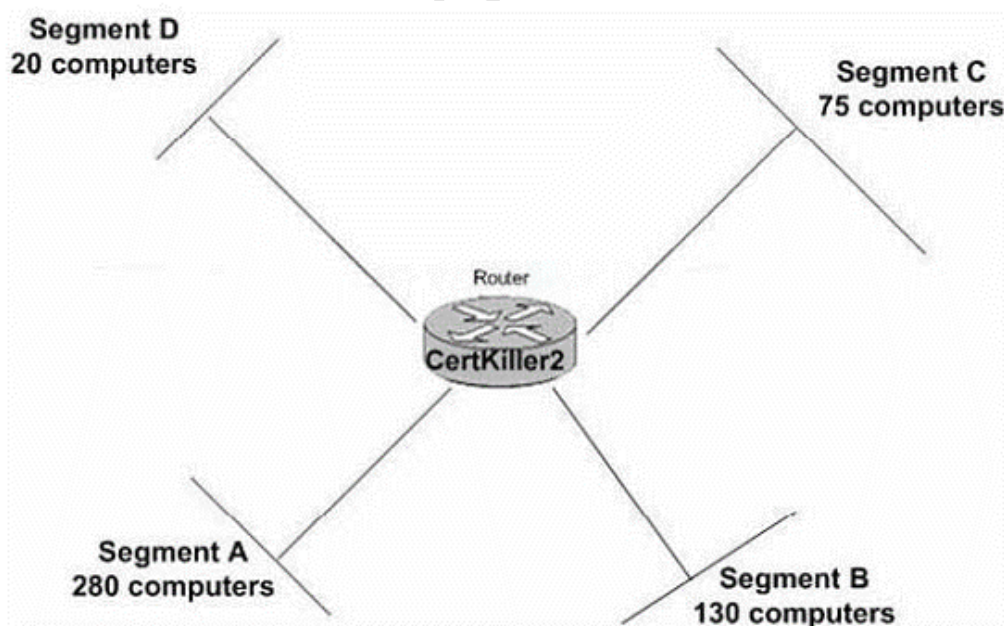
Basically the route command is used to change or view the entries in the local routing table. The full command syntax for this specific task is

```
route [-f] [-p] [ Command [ Destination ] [mask Netmask ] [ Gateway ] [metric Metric ]] [if Interface ]]
```

The -f parameter issues a command to the Windows to clear all gateway entries in the routing table. The -p command is used to make a specific route persistent. When the server is rebooted, all routes configured through the route command are erased from the IP routing table. If you use the -p parameter, the route command instructs Windows to retain and keep the route in the IP routing table even if the server is rebooted.

**QUESTION NO: 43**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. A portion of the CertKiller.com network is shown in the exhibit below:



CertKiller.com has recently decided to make use of IPv4 addressing using the network range 129.108.10.0/21. During the course of the day you receive instruction from CertKiller.com to have the network range segmented into four segments as shown in the exhibit and to ensure that all client computers in all the segments are supported.

What should you do?

A. You should consider assigning the network ranges as shown below

Segment A 129.108.10.0/22, Segment B 129.108.10.128/23, Segment C 129.108.10.0/192 and Segment D 129.108.10.224/25

B. You should consider assigning the network ranges as shown below

Segment A 129.108.10.128/22, Segment B 129.108.10.192/23, Segment C 129.108.10.224/24 and Segment D 129.108.10.0/26

C. You should consider assigning the network ranges as shown below

Segment A 129.108.10.109/22, Segment B 129.108.10.0/23, Segment C 129.108.10.0/24 and Segment D 129.108.10.109/25

D. You should consider assigning the network ranges as shown below

Segment A 129.108.10.0/22, Segment B 129.108.10.0/23, Segment C 129.108.10.0/24 and Segment D 129.108.10.128/26

E. You should consider assigning the network ranges as shown below

Segment A: 129.108.10.0/22, Segment B: 129.108.10.0/23, Segment C: 129.108.10.0/24, Segment D: 129.108.10.128/24

**Answer: E**

**Explanation:**

:

To ensure that your solution must support all computers in each segment, you need to configure Segment A: 129.108.10.0/22, Segment B: 129.108.10.0/23, Segment C: 129.108.10.0/24, Segment D: 129.108.10.128/24

This is because 129.108.10.0/21 can have maximum 2048 computers. / 22 means that a subnet can have 1024 computers, /23 means that a subnet can have 512 computers, and /24 means that a subnet can have 254 computers.

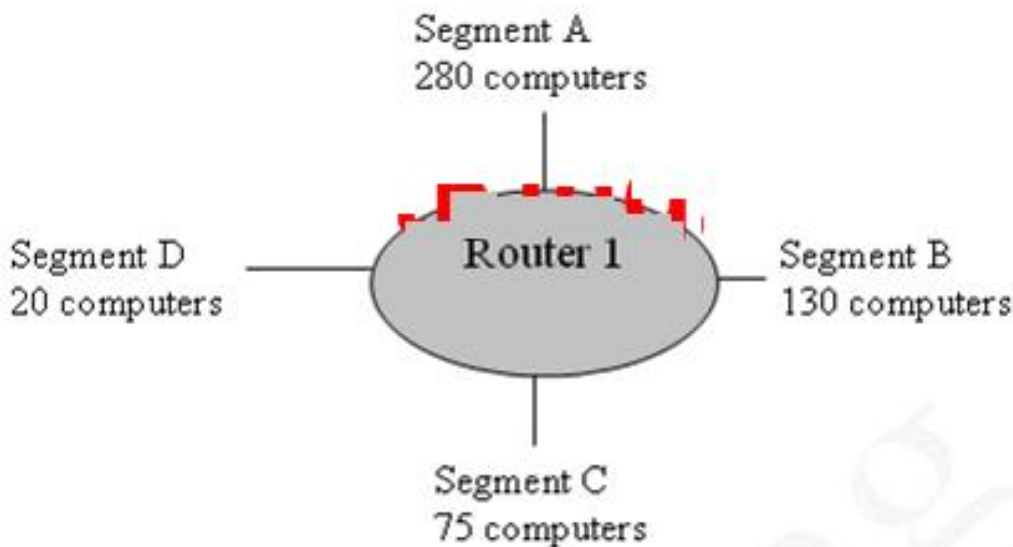
Because there are two networks with /24 subnet, 512 computer can be configured for /24 subnet. The sum of above three gives the required number of computers in the subnet.

Reference : Subnetwork

<http://en.wikipedia.org/wiki/Subnetwork>

**QUESTION NO: 44**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day CertKiller.com designed the plans for a public network which uses the IPv4 range 131.107.40.0/22 as shown below:



CertKiller.com wants you to configure subnets for the segments of the public network to support computers in all segments.

What should you do?

A. You should consider assigning the network ranges as shown below:

Segment A: 131.107.40.0/25

Segment B: 131.107.42.128/26

Segment C: 131.107.45.192/27

Segment D: 131.107.45.224/30

B. You should consider assigning the network ranges as shown below:

Segment A: 131.107.40.128/23

Segment B: 131.107.45.0/24

Segment C: 131.107.46.0/25

Segment D: 131.107.46.128/27

C. You should consider assigning the network ranges as shown below:

Segment A: 131.107.40.0/23

Segment B: 131.107.44.0/24

Segment C: 131.107.45.0/25

Segment D: 131.107.45.128/27

D. You should consider assigning the network ranges as shown below:

Segment A: 131.107.40.0/23

Segment B: 131.107.44.0/24

Segment C: 131.107.45.128/25

Segment D: 131.107.45.0/27

**Answer: C**

**Explanation:**

To ensure that your solution must support all computers in each segment, you need to configure

Segment A: 131.107.40.0/23, Segment B: 131.107.42.0/24, Segment C: 131.107.43.0/25,

Segment D: 131.107.43.128/27

Segment A: 131.107.40.0/23 can have 512 computer covering 300 computers.

Segment B: 131.107.42.0/24 can have 254 computers covering 125 computers

Segment C: 131.107.43.0/25 can have 192 covering 100 computers

Segment D: 131.107.43.128/27 can have 32 computers covering 15 nodes

The sum of above subnets gives the required number of computers in the subnet.

Reference : Subnetwork

<http://en.wikipedia.org/wiki/Subnetwork>

**QUESTION NO: 45**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com has recently deployed a new server in the domain named CERTKILLER-SR01 configured with the IP address: 192.168.45.186, Subnet mask: 255.255.255.192 and Default gateway 192.168.45.1. During the course of the day you receive complaints from remote subnet users are unable to connect to CERTKILLER-SR01. CertKiller.com wants you to ensure that the remote subnet users are able to access CERTKILLER-SR01.

What should you do?

- A. You should consider having the subnet mask changed to a 27-bit mask
- B. You should consider having the subnet mask changed to a 24-bit mask.
- C. You should consider having the IP address changed to 192.168.45.200.
- D. You should consider having the IP address changed to 192.168.45.129.

**Answer: B**

**Explanation:**

To ensure that all users are able to connect to the server, you need to change the subnet mask to a 24-bit mask. Because the subnet, 255.255.255.192 assigned to the server can have maximum of 32 hosts and because the subnet is in different network, the server cannot communicate to the gateway (192.168.46.1) assigned to it. To communicate with the gateway, the server should have in the same subnet and therefore the subnet of the server needs to be changed to 24bit, which can have 254 hosts.

Reference : Subnet Masks & Their Effect

<http://www.firewall.cx/ip-subnetting-mask-effect.php>

**QUESTION NO: 46**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com has recently deployed a router named KingRouting using the IP address 192.168.0.0 to connect the Miami office to the Internet.

CertKiller.com has additionally added a router named TestRouting using the IP address 192.168.64.0 to join the Miami office with a segment named KingSecured which has a network address of 192.168.4.0/26. During the course of the day you discover that a client computer which requires access to the KingSecured servers is unable to connect to the network using the current configuration. CertKiller.com wants you to add a persistent route for the KingSecured network to the routing table on the client computer.

What should you do?

- A. You should consider having the route add -p 192.168.4.0/22 192.168.4.1 command run.
- B. You should consider having the route add -p 192.168.64.10 mask 255.255.255.192 192.168.4.0 command run.
- C. You should consider having the route add -p 192.168.4.0/26 192.168.64.11 command run.
- D. You should consider having the route add -p 192.168.4.0 mask 255.255.255.192 192.168.64.1 command run.

**Answer: C****Explanation:**

To add a persistent route for the Private1 network to the routing table on CertKiller1, you need to add command Route add -p 10.128.4.0/26 10.128.64.11. This is because 10.128.4.0/26 is the IP subnet you desired to connect to and 10.128.64.11 is your IP gateway to the second subnet.



**QUESTION NO: 47**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com decided to make use of IPv4 addressing at both offices. During the course of the day you receive instruction from CertKiller.com to travel to Toronto office and deploy an additional server named CERTKILLER-SR02 which should be configured for Routing and Remote Access.

What should you do? (Choose two)

- A. You should consider having the netsh interface ipv4 enable command run on CERTKILLER-SR02.
- B. You should consider having CERTKILLER-SR02 configured with the Routing and Remote Access role.
- C. You should consider having the netsh ras ipv4 set access ALL command run on CERTKILLER-SR02.
- D. You should consider having the IPv4 Router Routing and Remote Access option enabled on CERTKILLER-SR02.

**Answer: B,D**

**Explanation:**

To configure routing on the server at the branch office, you need to first install the Routing and Remote Access role on the server and then enable the IPv4 Router Routing and Remote Access option on the server.

**Incorrect Answers:**

- A: You cannot use Network shell (netsh) is a command because it only allows you to configure and display the status of various network communications server roles and components after they are installed on computers running WindowsServer2008 and does not allow you to configure routing.
- C: You cannot use Network shell (netsh) is a command because it only allows you to configure and display the status of various network communications server roles and components after they are installed on computers running WindowsServer2008 and does not allow you to configure routing.



**QUESTION NO: 48**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently has their headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com recently decided to have the client computers located on a 192.168.1.0/24 segment configured with the default gateway 192.168.1.1.

During the course of the day you receive instruction from CertKiller.com to add an additional router for use with the 192.168.1.0/24 segment (Interface 192.168.15.1.2) and 192.168.2.0/24 segment (Interface 192.168.2.1). CertKiller.com wants you to configure the client computers on the 192.168.1.0/24 segment to make use of the second router connecting to the 192.168.2.0/24 segment.

What should you do?

- A. You should consider having the route add 192.168.1.2 MASK 255.255.255.0 192.168.2.0 command run.
- B. You should consider having the route add 192.168.1.1 MASK 255.255.255.0 192.168.2.0 command run.
- C. You should consider having the route add 192.168.2.0 MASK 255.255.255.0 192.168.1.1 command run.
- D. You should consider having the route add 192.168.2.0 MASK 255.255.255.0 192.168.1.2 command run.

**Answer: D**

**Explanation:**

If you are using the command in this way: route add 192.168.2.0 MASK 255.255.255.0 192.168.1.2, the client computer on the 192.168.1.0/24 subnet will use the second router when connecting to the 192.168.2.0/24 subnet.

**Incorrect Answers:**

- A: Run the route add 192.168.1.2 MASK 255.255.255.0 192.168.2.0 will not work. The parameters are reversed.
- B: Run the route add 192.168.1.1 MASK 255.255.255.0 192.168.2.0 will not work. The parameters are reversed and the wrong router is listed.
- C: If you run the route add 192.168.2.0 MASK 255.255.255.0 192.168.1.1, it will specify the wrong router. The default gateway is the router with the IP address of 192.168.1.1. This will result that the traffic will go to that router.

**QUESTION NO: 49**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day CertKiller.com decided to host an internal Web site which will be located on a remote network. CertKiller.com recently tested the Web site and has discovered that connectivity problems are occurring. CertKiller.com wants you to have the list of routers viewed which has packets traveling between the client and the server.

What should you do? (Choose two)

- A. You should consider having the PathPing command run.
- B. You should consider having the Ipconfig command run.
- C. You should consider having the Tracert command run.
- D. You should consider having the Ping command run.

**Answer: A,C**

**Explanation:**

You can use the Tracert command and the PathPing command. The Tracert command is used to trace a path to the network destination. The PathPing command is used to find the links that causes the intermittent connectivity problems.

**Incorrect Answers:**

- B: The Ipconfig command is used to display the current IP address, not to view or find routers that has a connectivity problem.
- D: The Ping command is used to test connectivity.

**QUESTION NO: 50**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured with two network interfaces connected to different subnets.

During the course of the day you decided to deploy additional routers to the first interface for providing access to different subnets. CertKiller.com recently requested that you configure CERTKILLER-SR01 to automatically identify the outers in addition to determining which remote subnets is available using each router.

What should you do?

- A. You should consider having OSPF enabled on the interface.
- B. You should consider having NAT enabled on the interface.
- C. You should consider having a static route added to the interface.
- D. You should consider having Rip enabled on the interface.

**Answer: D**

**Explanation:**

You should enable RIP on the interfaces. RIP will automatically detect remote networks and neighboring routers.

**Incorrect Answers:**

A: Windows Server 2008 does not support OSPF.

B: You should not enable NAT on the interface. NAT translate private IP addresses to public IP address for the use on the Internet.

C: A static route is used when many gateways are connected to the local network and some do not act as a default gateway. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.260, 265, 307, 603

**QUESTION NO: 51**

You work as a network administrator at CertKiller.com. All servers on the CertKiller.com network are configured to run Windows Server 2008.

You are in the process of troubleshooting a network system that contains a large amount of static routes. Whilst reviewing the data you detect that an error was made when the routes were entered into one of the gateways. You need to resolve this issue as soon as possible.

What should you do?

- A. You should not attempt anything as static routes auto correct themselves.
- B. You should perform a system reboot to clear the persistent routes.
- C. You should modify the static routes to dynamic routes.
- D. None of the above.

**Answer: A**

**Explanation:**

When changes are made to the network or a failure between the two statically defined nodes will cause traffic between the points to be rerouted. Any packets awaiting transport between affected paths will be forced to wait for repairs to the failure or an updated static route.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

### QUESTION NO: 52

You are employed as the network administrator at CertKiller.com. All servers on the CertKiller.com network are configured to run Windows Server 2008.

You receive an instruction from the CIO to setup a lab for a training class. To safeguard the network you decide to isolate this lab network from the rest of the environment. You need to determine the appropriate IP addressing method that will achieve this.

What should you identify?

- A. You should make use of Public network addressing.
- B. You should make use of Network Address Translation.
- C. You should make use of Subnet isolation via the subnet mask.
- D. You should make use of Private network addressing.

**Answer: C**

#### Explanation:

In this scenario your best option would be to use subnet isolation via the subnet mask. When a router or a switch is installed and you make use of a different subnet mask you will be able to isolate the subnet in the lab in order for local traffic not to be routed to the network.

#### Incorrect Answers:

- A: The public network addressing scheme is not appropriate for the lab environment.
  - B: You make use of network address translation when private IP addresses have to head out to the Internet. The scenario does not mention Internet connectivity and it does not solve the subnet isolation issue.
  - D: The CertKiller.com network may already be using private network addresses so with no other specifics the use of private network addressing is incorrect.
- Reference:  
Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

### QUESTION NO: 53

You are employed as the systems administrator at CertKiller.com. CertKiller.com has its headquarters in Stockholm where you are located.

You receive an instruction from the CIO to set up LAN. One of the prerequisites of CertKiller management is that you need to accomplish this using the Windows 2008 Server RRAS. In order to organize the appropriate signal flow between the devices you need to determine the correct

routing algorithms or protocols that need to be used.

What should you identify?

- A. You should consider using OSPF.
- B. You should consider using RIP2.
- C. You should consider using RIP.
- D. None of the above.

**Answer: B,C**

**Explanation:**

RIP and RIP2 is supported by Windows Server 2008.

**Incorrect Answers:**

A: OSPF is no longer supported in RRAS of Windows Server 2008. Reference: Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

#### QUESTION NO: 54

You are employed as the exchange administrator at CertKiller.com. You are responsible for managing the Exchange network for CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are in the process of configuring a routing table which is based on information gathered in order to optimize the network. During routine monitoring you detect that the IP destination 192.168.1.123 as well as the subnet mask of 255.255.255.0 needs to be deleted. You need to determine the appropriate command that will accomplish this.

What should you identify?

- A. You should use the route delete 192.\* command.
- B. You should use the route delete 192.168.1.123 mask 255.255.255.0 command.
- C. You should use the route add 192.168.1.123 mask 255.255.255.0 192.168.0.123 command.
- D. You should use the route change 192.168.1.123 mask 255.255.255.0 192.168.0.25 command.

**Answer: B**

**Explanation:**

Your best option in this scenario would be to make use of the route delete 192.168.1.123 mask 255.255.255.0 command. As soon as this command is run the aforementioned route will be deleted.

**Incorrect Answers:**

A: These commands will not accomplish this task.Reference:  
Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008  
C: These commands will not accomplish this task.Reference:  
Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008  
D: These commands will not accomplish this task.Reference:  
Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

#### QUESTION NO: 55

You work as a network administrator for CertKiller.com. You have deployed a file server on the corporate network on a server that runs Windows Server 2008.

You receive an instruction from the CIO to ensure that the LAN network is scalable as the organization grows. The LAN network will contain a vast amount of physical workstations. To accomplish the task you make use of a Distance Vector Routing protocol like RIP.

What will you deduce when you make use of RIP?

- A. You will discover that RIP is not usable for LAN configurations.
- B. You will discover that RIP does not understand VLSM.
- C. You will discover that RIP is not scalable for big networks.
- D. None of the above.

**Answer: C**

#### Explanation:

RIP is very limited. RIP stops routing loops from continuing for an indefinite time by implementing a limit on the amount of hops permitted in a path from the source to the destination. This results in the fact that RIP limits the size of the network that can be supported by the design.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

#### QUESTION NO: 56

You are an Enterprise administrator for CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. You have deployed a file server named CERTKILLER-SR03 on the corporate network. You configured a shared folder on CERTKILLER-SR03 to enable users to access shared files on CERTKILLER-SR03.

During the course of the day you received complaints from users stating their inability to access the shared files located on CERTKILLER-SR03. The TCP/IP properties for CERTKILLER-SR03 is

configured to obtain IP address automatically and the users' computers were configured with IP addresses and subnet masks. CertKiller.com wants you to ensure that all users are able to access the shared files located on TESTING-SR03.

What should you do?

- A. You should consider having the DNS server address configured on the CERTKILLER-SR03 TCP/IP properties.
- B. You should consider having the default gateway address configured on the CERTKILLER-SR03 TCP/IP properties.
- C. You should consider having a static IP address for CERTKILLER-SR03 configured on the CERTKILLER-SR03 TCP/IP properties.
- D. You should consider having the DNS suffix on the network interface added to the domain on the CERTKILLER-SR03 TCP/IP properties.

**Answer: C**

**Explanation:**

To ensure that users are able to access the shared files, you need to configure a static IP address on the file server because In order for both PC's to be able to communicate together, the Ethernet adapters will need to be configured with a static IP address and a common Subnet mask. As an example, assign one PC an IP address of 192.198.0.1 and assign the second PC an IP address of 192.198.0.2. Both machines should use the Subnet mask 255.255.255.0.

Reference : need help to setup a lan connection between 2

<http://en.kioskea.net/forum/affich-2335-need-help-to-setup-a-lan-connection-between-2>

**QUESTION NO: 57**

You are an enterprise administrator for CertKiller.com. The company runs Windows Server 2008 on all the servers on the network.

You are in the process of setting up LAN. You need to accomplish this by using Windows 2008 Server RRAS. You thus have to know the routing algorithms or protocols that are supported by the Windows Server 2008 feature.

Determine the type of routing algorithms or protocols that cannot be used to organize the signal flow in this scenario?

- A. OSPF cannot be used to organize the signal flow.
- B. RIP cannot be used to organize the signal flow.
- C. RIP2 cannot be used to organize the signal flow.



D. None of the above.

**Answer: A**

**Explanation:**

OSPF cannot be used to organize the signal flow. OSPF is no longer supported in the RRAS of Windows Server 2008.

**Incorrect Answers:**

B: RIP is supported by Windows Server 2008.

C: RIP2 is supported by Windows Server 2008. Reference: Syngress - The Real MCTS-MCITP 70-649 Prep Kit - Independent and Complete Self-Paced Solutions Part 4, Configure IPsec (4 Questions)

**QUESTION NO: 58**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured with the Secure Server (Require Security) IPsec policy. During the course of the day you receive reports by the network users that they are unable to connect to CERTKILLER-SR01. CertKiller.com recently requested that you ensure that the network users are able to connect to CERTKILLER-SR01 whilst ensuring that all connections remains encrypted.

What should you do?

- A. You should consider having the Client (Respond Only) IPsec policy assigned to CERTKILLER-SR01 and all client computers.
- B. You should consider having the IPsec Policy Agent service restarted on CERTKILLER-SR01 and all client computers.
- C. You should consider having the Client (Respond Only) IPsec policy assigned to all client computers only.
- D. You should consider having the Server (Request Security) IPsec policy assigned to CERTKILLER-SR01 only.

**Answer: C**

**Explanation:**

The network users fail to connect to CERTKILLER-SR01 when Secure Server (Require Security) IPsec policy was assigned because this policy requires all communications to be secure. Once this policy has been applied, the server will neither send nor accept insecure communications. Any

client wanting to communicate with the server must use at least the minimum level of security described by the policy. The network users may not be fulfilling the defined security requirements.

To ensure that users can connect to CERTKILLER-SR01 and that all connections to CERTKILLER-SR01 must be encrypted, you need to assign the Client (Respond Only) IPsec policy to all client computers. This policy is designed to be run on client machines that don't normally need to worry about security. The policy is designed in such a way that the client will never initiate secure communications on its own. However, if a server requests that the client go into secure communications mode, the client will respond appropriately.

Reference : What are IPSEC Policies and how do I work with them?

[http://www.petri.co.il/what\\_are\\_ipsec\\_policies.htm](http://www.petri.co.il/what_are_ipsec_policies.htm)

### QUESTION NO: 59

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day you receive instruction from CertKiller.com to deploy a computer named CERTKILLER-SR01 as a Web server which will additionally have the FTP service installed for storing confidential files.

The CertKiller.com written security policy currently states that all communications to and from CERTKILLER-SR01 should be transmitted over the network using the most secure manner. During the course of your routine security inspection you discover that connections to and from CERTKILLER-SR01 are being transmitted over a network using no encryption. CertKiller.com wants you to ensure that encryption is used at all times when transmitting data to and from CERTKILLER-SR01.

What should you do? (Choose two)

- A. You should consider having the Server Message Block (SMB) signing used between the CERTKILLER-SR01 and other network computers where files are transmitted.
- B. You should consider having CERTKILLER-SR01 configured to activate offline files for the data stored on CERTKILLER-SR01 and the Encrypt contents to secure data option should be selected in the Folder Advanced Properties dialog box.
- C. You should consider having NTLM authentication methods used on CERTKILLER-SR01.
- D. You should consider having the confidential files published on CERTKILLER-SR01 using IIS and then activate SSL on CERTKILLER-SR01.
- E. You should consider having IPsec encryption used between CERTKILLER-SR01 and other network computers where files are transmitted.

**Answer: D,E**

**Explanation:**

To ensure that encryption is always used when the confidential files on the FSS1 server are transmitted over the network, you need to either publish the confidential files using IIS to and activate SSL on the IIS server or use IPSec encryption between the FSS1 server and the computers of the users who need to access the confidential files.

One of the features of IIS 7.0 is FTP over Secure Sockets Layer (SSL). This allows sessions to be encrypted between an FTP client and server.

IP Security (IPSec), mentioned briefly in previous sections, is essentially a mechanism for establishing end-to-end encryption of all data packets sent between computers. IPSec operates at Layer 3 of the OSI model and subsequently uses encrypted packets for all traffic between members.

IPSec is often considered to be one of the best ways to secure the traffic generated in an environment, and is useful for securing servers and workstations both in high-risk Internet access scenarios and also in private network configurations for an enhanced layer of security.

Reference : Using FTP Over SSL

<http://learn.iis.net/page.aspx/304/using-ftp-over-ssl/>

Reference : Using IPSec Encryption with Windows Server 2008

<http://my.safaribooksonline.com/9780672329302/ch14lev1sec5>

**QUESTION NO: 60**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the business day CertKiller.com decided to make changes to the written security policy which would require having all communications in the domain encrypted. CertKiller.com wants you to have IPSec configured to enforce the written security policy.

What should you do?

- A. You should consider having IPSec used with Authentication Header (AH) authentication.
- B. You should consider having IPSec used with Encapsulating Security Payload (ESP) authentication.

- C. You should consider having IPsec used in tunnel mode.
- D. You should consider having IPsec used with both AH and ESP authentication.

**Answer: B**

**Explanation:**

To provide or to ensure the security policy, you need to use Encapsulating Security Payload (ESP) authentication. This will provide data encryption.

**Incorrect Answers:**

- A: You should not use IPsec with Authentication Header (AH) authentication. Authentication Header (AH) authentication will not provide data encryption, only data authentication.
- C: You should not use IPsec should in tunnel mode. The tunnel mode will provide compatibility for some of the VPN gateways.
- D: You can use both AH and ESP authentication, however it will increase the processing overhead unnecessary. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.604

**QUESTION NO: 61**

You work as the Enterprise network administrator at CertKiller.com. CertKiller.com recently released a new network security policy which requires the computers in the CertKiller.com domain and Weyland.com located in the same forest to use IPsec communications. CertKiller.com wants you to choose which authentication methods should be used for IPsec.

What should you do?

- A. Use a Preshared key with IPsec.
- B. Use NTLM with IPsec.
- C. Use Certificates with IPsec.
- D. Use Kerberos authentication with IPsec.

**Answer: D**

**Explanation:**

The method of authentication that should be used is Kerberos authentication. It is the default authentication method in an Active Directory environment. Also Kerberos will provide authentication outside the Active Directory to provide authentication for IPsec communications.

**Incorrect Answers:**

- A: Preshared key is a password that is shared between two peers. It is also used to encrypt and decrypt data however; it does not have the same level of authentication as that of Kerberos.
- B: You should not use NTLM with IPsec. For a backup authentication for Active Directory, you should use NTLM. You cannot use it for an authentication method for IPsec.
- C: The best authentication to use is Kerberos authentication with IPsec. If you are using

Certificates with IPsec, both of the domains need to trust the CA that will issue the certificate to the peers. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.281, 282, 604

## QUESTION NO: 62

You work as a network administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory forest that contains three domains. All domain controllers on the CertKiller.com network run Windows Server 2008.

There are two DNS servers in the three domains. Every DNS server hosts the Active Directory-integrated zones for the three domains. CertKiller.com has recently acquired another company named Courseware Publishers. Courseware Publishers contains a single Active Directory forest with one domain. You receive an instruction from the CIO to ensure that name resolution for the resources in both forests is supplied by the DNS system in the CertKiller.com forest.

What should you do?

- A. You should consider creating a new conditional forwarder in the Active Directory. Thereafter the newly created conditional forwarder should be replicated to all DNS servers in the CertKiller.com forest.
- B. You should consider enlisting a directory partition for all DNS servers by creating a new application directory partition in the CertKiller.com forest.
- C. You should consider configuring the user workstations in the CertKiller.com forest to make use of the DNS server in the courseware.com forest as an alternate DNS server.
- D. You should consider creating a new host (A) record on one of the DNS servers in the CertKiller.com forest using the domain /forest details of Courseware publishers.

**Answer: A**

**Explanation:**

:

Your best option in this scenario would be to create a new conditional forwarder and store it in the Active Directory. This will allow you to configure the DNS system in the CertKiller.com forest in order to provide name resolution for resources in both forests. The conditional forwarder can then be replicated to the DNS servers in the CertKiller.com forest. You make use of conditional forwarding to speed up name resolution in scenarios where merged or collaborated companies resolve each other's namespace.

Reference : DNS Conditional Forwarding in Windows Server 2003

[http://www.windowsnetworking.com/articles\\_tutorials/DNS\\_Conditional\\_Forwarding\\_in\\_Windows\\_Server\\_2003.html](http://www.windowsnetworking.com/articles_tutorials/DNS_Conditional_Forwarding_in_Windows_Server_2003.html)

**QUESTION NO: 63**

You are employed as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest named CertKiller.com. The CertKiller.com forest contains four domains.

The DNS servers in the CertKiller.com forest are configured to run Windows Server 2008. You receive an instruction from the CIO to make sure that the public DNS queries are channeled through a single caching only DNS server.

What should you do? (Choose all that apply.)

- A. This can be accomplished by ensuring that the BINDsecondaries are disabled on a DNS Server.
- B. This can be accomplished by ensuring that a forwarder is configured.
- C. This can be accomplished by ensuring that a GlobalNames host (A) record for the hostname of the caching DNS server is configured.
- D. This can be accomplished by ensuring that the root hints is disabled.

**Answer: B,D**

**Explanation:**

In this scenario your best option would be to either configure a forwarder or the root hints on the caching only DNS Server. This will ensure that the public DNS queries are channeled through a single-caching-only DNS server. A caching-only DNS server reduces outgoing DNS traffic and speeds up name resolution. It receives queries from clients, executes the queries against other name servers, caches the results as well as returning the results to the client.

You are able to set up a caching-only server by configuring the DNS service with one or more forwarders, which are upstream DNS servers to which the local DNS server will forward queries (essentially acting as a DNS client). In some configurations, DNS servers include root hints that enable them to query the DNS root servers. In other configurations, servers forward all queries that they cannot answer to another server. Forwarding and root hints are both methods that DNS servers can use to resolve queries for which they are not authoritative.

Reference : Configure a caching-only DNS forwarder in Windows 2000 Server  
[http://articles.techrepublic.com.com/5100-10878\\_11-5819265.html](http://articles.techrepublic.com.com/5100-10878_11-5819265.html)

Reference : Reviewing DNS Concepts  
<http://technet2.microsoft.com/windowsserver2008/en/library/aeb2265d-8965-4b7e-bb28-704c36be4d401033.mspx?mfr=true>

**QUESTION NO: 64**

You are the newly appointed system administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com.

You are responsible for a Windows Server 2008 Core installation server named CERTKILLER-SR15. CERTKILLER-SR15 has the DNS server role installed. There is a single network interface named CertKiller Area Connection on CERTKILLER-SR15. The static IP address of CertKiller Area Connection is 10.0.0.1. During the course of the day you receive instruction from CertKiller.com to create a DNS zone named local.CertKiller.com on CERTKILLER-SR15.

What should you do?

- A. You should consider making use of the `dnscmd CERTKILLER-SR15/ZoneAdd local.CertKiller.com/DSPPrimary` command.
- B. You should consider making use of the `dnscmd CERTKILLER-SR15/ZoneAdd local.CertKiller.com/Primary /file local.CertKiller.com.dns` command.
- C. You should consider making use of the `ipconfig /registerdns:local.CertKiller.com` command.
- D. You should consider making use of the `netsh interface ipv4 set dnsserver name=local.CertKiller.com static 10.0.0.1 primary` command.

**Answer: B**

**Explanation:**

To create a DNS zone named local.CertKiller.com on CERTKILLER-SR15, you need to use `dnscmd CERTKILLER-SR15/ZoneAdd local.CertKiller.com/Primary /file local.CertKiller.com.dns` command.

`Dnscmd/ ZoneAdd` command adds a zone to the DNS server. The syntax for the command is `dnscmd [ ServerName ] /zoneadd ZoneName ZoneType [ /dp FQDN [{ /domain | /enterprise | /legacy }] ]`

Where `ServerName` specifies the DNS server, `ZoneName` specifies the name of the zone, `ZoneType` specifies the type of zone to create. Each type has different required parameters.

`/primary /file FileName` Creates a standard primary zone and specifies the name of the file that will store the zone information. Therefore this zone type is used here instead of `/dsprimary` which creates an Active Directory-integrated zone which is not required in this scenario.

Reference : Dnscmd Syntax

<http://technet2.microsoft.com/windowsserver/en/library/d652a163-279f-4047-b3e0->



0c468a4d69f31033.mspx?mfr=true

**QUESTION NO: 65**

You work as an enterprise administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory forest that contains a single Active Directory domain named us.CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are responsible for a Windows Server 2008 server named CERTKILLER-SR10. CERTKILLER-SR10 contains a DNS server role and hosts numerous secondary zones including us.CertKiller.com. You decide to reconfigure CERTKILLER-SR10 as a caching-only DNS server.

What should you do?

- A. You should consider disabling the DNS stub zones on CERTKILLER-SR10. Thereafter the DNS service should be enabled again.
- B. You should consider uninstalling the DNS service on CERTKILLER-SR10. Thereafter the DNS service should be installed again.
- C. You should consider enabling DNS Scavenging from CERTKILLER-SR10. Thereafter the DNS service should be restarted on CERTKILLER-SR10.
- D. You should consider modifying the DNS zones on CERTKILLER-SR10 to stub zones.

**Answer: B**

**Explanation:**

In order to reconfigure CERTKILLER-SR10 as a caching-only DNS server you need to uninstall and reinstall the DNS service on CERTKILLER-SR10. Uninstalling and reinstalling DNS service will remove all the previously configured data from CERTKILLER-SR10.

Reference : Install the DNS Server service

<http://technet2.microsoft.com/windowsserver/en/library/421cd57a-9fd4-42da-8d22-067738f034ee1033.mspx?mfr=true>

**QUESTION NO: 66**

You are employed as the network administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com has its headquarters in Athens and a branch office in Paris. At present the workstations at the Paris office makes use of a VPN connection to connect to the workstations in the Athens office. You receive an instruction from the CIO to make sure that clients are unable to

connect remotely to the VPN server between 22:00 and 04:00.

What should you do?

- A. This can be accomplished by enabling the Force logoff when logon hours expire option in order to configure the Logon Hours for the network policy.
- B. This can be accomplished by creating a Default Domain policy for the VPN connections, Thereafter an IP filter to deny access to the CertKiller.com network can be applied.
- C. This can be accomplished by specifying the VPN server on the Computer restrictions option in the Default Domain policy to configure the Logon hours for all user objects.
- D. This can be accomplished by creating a network policy for VPN connections. Thereafter the Day and time restrictions can be configured as desired.

**Answer: D**

**Explanation:**

To ensure that clients are unable to access the VPN server remotely from 22:00 to 04:00, you need to create a network policy for VPN connections and then modify the Day and time restrictions. The network policy provides a policy conditions called "Allow full network access for a limited time", which allow clients to temporarily access the full network. However, the NAP enforcement is delayed until the specified date and time.

Reference : Step By Step Guide: Demonstrate VPN NAP Enforcement in a Test Lab / NAP enforcement and network restriction

<http://www.microsoft.com/downloads/details.aspx?FamilyID=729bba00-55ad-4199-b441-378cc3d900a7&displaylang=en>

**QUESTION NO: 67**

You work as a network administrator at TesCKin.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network is configured to run Windows Server 2008.

You are responsible for a Windows Server 2008 server named CERTKILLER-SR06. CERTKILLER-SR06 is configured to run the DHCP Server role as well as the DNS Server role. The IP address of CERTKILLER-SR06 is 192.168.122.1. The CertKiller.com network contains another server named CERTKILLER-SR01. CERTKILLER-SR01 is configured to run a Server Core installation of Windows Server 2008.

All workstations on the network make use of the network interface named CertKiller Area Connection and are configured to only use CERTKILLER-SR06 for DNS name resolution. During routine monitoring you discover that CERTKILLER-SR06 goes offline occasionally. A new DNS

server named CERTKILLER-SR04 has been configured to make use of the IP address 192.168.122.254.

You decide to configure CERTKILLER-SR01 to make use of CERTKILLER-SR04 as the preferred DNS server and CERTKILLER-SR06 as the alternate DNS server.

What should you do?

- A. This can be accomplished by running the netsh interface ipv4 set dnsserver "CertKiller Area Connection" static 192.168.122.254 primary command as well as the netsh interface ipv4 set dnsserver "CertKiller Area Connection" static 192.168.122.1 both command on CERTKILLER-SR01.
- B. This can be accomplished by running the netsh interface ipv4 set dnsserver "CertKiller Area Connection" static 192.168.122.254 192.168.122.1 both command on CERTKILLER-SR01.
- C. This can be accomplished by running the netsh interface ipv4 set dnsserver "CertKiller Area Connection" static 192.168.122.254 primary command as well as the netsh interface ipv4 add dnsserver "CertKiller Area Connection" static 192.168.122.1 index=1 command on CERTKILLER-SR01.
- D. This can be accomplished by running the netsh interface ipv4 add dnsserver "CertKiller Area Connection" static 192.168.122.254 index=1 command on CERTKILLER-SR01.

**Answer: D**

**Explanation:**

:

Your best option in this scenario would be to run the netsh interface ipv4 add dnsserver "CertKiller Area Connection" static 192.168.122.254 index=1 command. Running this command will ensure that CERTKILLER-SR01 is configured to use CERTKILLER-SR04 as the preferred DNS server and CERTKILLER-SR06 as the alternate DNS server.

The actual command is:

```
netsh interface ipv4 add dnsserver [name=] "IDx" [address=] IPAddress [index=] ListNumber
```

Where:

IDx is the Identification of the Networking Interface for which you want to change the address. You can view the identification flags when you use the command netsh interface ipv4 show interfaces. When you only have one Networking Interface Card (NIC) the IDx of this card will be Local Area Connection.

IPAddress is the static IPv4 Address you want to provide to your Network Connection to use as the DNS server. In the first command this IP Address represents the primary DNS server. In the second command this IP Address represents the secondary DNS server.

ListNumber is the position in the DNS server list where you want to add the DNS Server address. The lower the number, the higher the DNS Server is added to the DNS Server list. For a secondary DNS server you can use index 2. For further DNS servers you can add IP addresses

with higher index numbers.

In the above scenario Index=1 represents that the DNS Server added is the primary DNS Server. You need not configure Server 2 because it is already configured and is currently offline.

Reference : Windows Server Core IP Configuration, Part 2 / Configuring DNS Servers

<http://blogs.dirteam.com/blogs/sanderberkouwera/archive/2008/01/26/windows-server-core-ip-configuration-part-2.aspx>

### QUESTION NO: 68

You are work as a network administrator for CertKiller.com. The CertKiller.com network consists of an Active Directory integrated DNS. All servers on the CertKiller.com network are configured to run Windows Server 2008.

You are in the process of running a network capture when you discover that the DNS server is sending DNS name resolution queries to a server named test.root-servers.net. You receive an instruction from the CIO to prohibit the DNS server from sending queries to test.root-servers.net. You should also ensure that the DNS server is able to resolve names for Internet Hosts.

What should you do? (Choose all that apply.)

- A. This can be accomplished by enabling forwarding to the companies ISPs DNS servers.
- B. This can be accomplished by enabling DNS scavenging for the IP subnets on the network.
- C. This can be accomplished by disabling the netmask ordering option on the DNS server.
- D. This can be accomplished by disabling the root hints on the DNS server.

**Answer: A,D**

#### Explanation:

To prevent the DNS server from sending queries to king.root-servers.net, you need to disable the root hints on the DNS server. Root hints are used to enable any DNS server to locate the DNS root servers. Because the root hints are enabled, the DNS server was sending all queries to test.root-servers.net.

Next to resolve names for Internet hosts, you need to enable forwarding to the companies ISPs DNS servers. Forwarding enables you to route name resolution through specific servers instead of using root hints.

Reference : Reviewing DNS Concepts/ Recursive name resolution

<http://technet2.microsoft.com/windowsserver2008/en/library/aeb2265d-8965-4b7e-bb28-704c36be4d401033.mspx?mfr=true>

**QUESTION NO: 69**

You are the newly appointed network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network are configured to run Windows Server 2008.

A new CertKiller.com directive states that the names of all user workstations should be changed according to the company standards. During routine monitoring you discover that the local DNS server resolves the names of the user workstations incorrectly from the cached information. In order to adhere to the company directives you decide to resolve the problem as well as to restore the correct name resolution.

What should you do?

- A. Your best option would be to restart all the DNS user workstations.
- B. Your best option would be to run the `dnscmd /clearcache` command on the DNS server.
- C. Your best option would be to restart the DNS Client service on the user workstations.
- D. Your best option would be to run the `ipconfig /flushdns` command at the user workstations.

**Answer: B**

**Explanation:**

If you run the `dnscmd /clearcache` command, it will clear the cache of the local DNS server. If the DNS server gets another query, it will query the other workstations and it will try to resolve the name.

**Incorrect Answers:**

- A: Selection this option is incorrect. If you restart the DNS user workstations it will only clear the DNS client cache. This will not resolve the problem and restore proper name resolution.
- D: Selection this option is incorrect. Restarting the DNS Client service on the user workstations will clear the DNS client cache however the DNS server will still respond to query the name of the workstation.

**QUESTION NO: 70**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows XP Professional.

You are assigned a Windows Server 2008 computer named CERTKILLER-SR05. When you specify the client computer by name in the UNC path you discover that CERTKILLER-SR05 is unable to communicate with the client computers running Microsoft Windows XP Professional. To

ensure productivity you need to make sure that CERTKILLER-SR05 is able to connect to client computers by specifying them in a UNC.

What should you do?

- A. You should consider decreasing the Time-to-Live (TTL) on the Start of Authority (SOA) record on CERTKILLER-SR05.
- B. You should consider disabling IPv6 on CERTKILLER-SR05.
- C. You should consider enabling NetBIOS on CERTKILLER-SR05.
- D. You should consider enabling IPv6 on CERTKILLER-SR05.

**Answer: C**

**Explanation:**

Your best option in this scenario would be to enable the NetBIOS on CERTKILLER-SR05.

**Incorrect Answers:**

- A: This option is incorrect. If you enable the Local Link Multicast Name Resolution (LLMNR), it will not enable UNC connectivity to the Microsoft Windows XP Professional computer. It will only enable UNC connectivity to the Vista and Windows Server 2008 computers.
- B: This option is incorrect. IPv6 does not block network functionality. This means you cannot use it to enable UNC connectivity.
- D: This option is incorrect. If you enable IPv6 on CERTKILLER-SR05, you will not enable extra functionality on the Microsoft Windows XP Professional computer.

**QUESTION NO: 71**

You work as a network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows XP Professional. Half the client computers are portable computers and the rest are desktop computers.

You are in the process of deploying a new DNS server in the CertKiller.com domain. You receive an instruction from the CIO to configure the deployed DNS server in order to identify the root server in the domain as its root server.

What should you do?

- A. This can be accomplished by replacing the Cache.dns file with a new version identifying the CertKiller.com root servers.
- B. This can be accomplished by configuring a HOSTS file with the names and addresses of the root servers in the domain.
- C. This can be accomplished by configuring an Lmhosts file with the names and addresses of the root server in the domain.

- D. This can be accomplished by configuring the new DNS Server to forward queries to the root server in the domain.
- E. This can be accomplished by disabling BIND secondaries.

**Answer: A**

**Explanation:**

Because you have deployed a new DNS server, you need to replace the Cache.dns file. The Cache.dns file contains the information of the root servers for the DNS namespace.

**Incorrect Answers:**

- B: This option is incorrect. HOSTS files will resolve hosts names to IP addresses. It will not identify the root servers.
- C: This option is incorrect. You should replace the Cache.dns file, because the Lmhosts file maps the NetBIOS names to IP addresses.
- D: This option is incorrect. You should replace the Cache.dns file that has the information of the root servers. Because when the forwarder fails the DNS server will still query the root servers. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.98, 108, 112

**QUESTION NO: 72**

You are employed as the enterprise administrator at CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows XP Professional. CertKiller.com has offices in Chicago and Miami. Both offices host an Active Directory domain.

You receive an instruction from the CIO to ensure that all clients are able to resolve names as well as browse the internal network of each other's offices. To ensure productivity at both offices you need to make sure that the clients are able to resolve Internet names. You should therefore configure the DNS server at the Miami office as well as the Chicago office correctly.

What should you do?

- A. This can be accomplished by configuring the parent DNS server in the Chicago office to forward queries destined for the Miami office DNS servers using conditional forwarding. Thereafter the parent servers in the Miami office should be configured to forward queries intended for the Chicago office to the Chicago DNS servers.
- B. This can be accomplished by configuring the root server in the Chicago office. Thereafter the Miami servers should be configured to forward queries to the root servers in the Chicago office
- C. This can be accomplished by configuring the parent DNS server in the Chicago office to forward queries to the parent servers in the rest of the CertKiller.com forest.



D. This can be accomplished by configuring the DNS servers at both offices to forward queries to an external forwarder.

**Answer: A**

**Explanation:**

When you apply this option, it will enable the DNS server to resolve the names in the local and remote domain and the Internet.

**Incorrect Answers:**

B: This will not allow the computer to resolve Internet names, neither for the Chicago DNS server to resolve names in Miami.

C: This is not the best way for the computers to resolve Internet names.

D: You should not configure the DNS servers at every office to forward queries to an external forwarder. The computers in the offices will not be able to resolve the computers in the other offices. Part 2, Configure DNS zones (24 Questions)

**QUESTION NO: 73**

CertKiller.com has employed you as a network administrator. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows XP Professional.

CertKiller.com has its headquarters in London and a branch office in Minsk. The Minsk office makes use of a WAN link to connect to the London office. The CertKiller.com domain contains a domain controller named CERTKILLER-DC01. CERTKILLER-DC01 is located at the London office and is also configured as a DNS server.

You receive an instruction from the CIO to install a new domain controller named CERTKILLER-DC02 at the Minsk office and configure it with DNS. To ensure productivity you need to make sure that the DNS service on CERTKILLER-DC02 is able to update records as well as answering queries in the event of a WAN link failure.

What should you do?

- A. This can be accomplished by configuring a new stub zone of CertKiller.com on CERTKILLER-DC02.
- B. This can be accomplished by switching the DNS CertKiller.com zone on CERTKILLER-DC01 at the London office to an Active Directory-integrated zone.
- C. This can be accomplished by setting the DNS server on CERTKILLER-DC02 to forward all requests to CERTKILLER-DC01 at the London office.
- D. This can be accomplished by increasing the Refresh Interval setting the Start of Authority (SOA) record for the CertKiller.com zone.

**Answer: B**

**Explanation:**

For this scenario your best option would be to select Option B. In order to ensure that the DNS service on CERTKILLER-DC02 is able to update records and answer queries in the event of a WAN link failure, you need to switch the DNS named CertKiller.com zone on CERTKILLER-DC01 at the London office to an Active Directory-integrated zone. This will ensure that the DNS will update the records and answer queries using the Active Directory infrastructure.

**Incorrect Answers:**

A: Selecting this option is incorrect. Configuring a new stub zone of CertKiller.com on CERTKILLER-DC02 is futile in this scenario because a stub zone requires a WAN link to communicate.

C: Selecting this option is incorrect. Setting the DNS on CERTKILLER-DC02 to forward requests to CERTKILLER-DC01 is not an option because CERTKILLER-DC01 is configured as a standard primary zone.

D: This option will minimize DNS zone traffic over WAN links. This is not addressing the question of making sure that the DNS service is able to update records as well as answering queries in case of WAN-link failure.

**QUESTION NO: 74**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and the client workstations run Windows XP Professional.

You are responsible for a DNS server named CERTKILLER-SR06. CERTKILLER-SR06 contains 10 Active Directory-integrated zones. You receive a request from the auditors to supply them with DNS zone records. You need to determine a strategy to make sure that the zone files are available for the auditors.

What should you do?

- A. You should consider executing the `dnscmd/zoneinfo` command.
- B. You should consider executing the `ipconfig/registerdns` command.
- C. You should consider executing the `dnscmd /zoneexport` command.
- D. You should consider executing the `ntdsutil Partition Management List` commands.

**Answer: C**

**Explanation:**

To ensure that the zone file copies of CERTKILLER-SR06 are available to the auditors, you need to make use of the `dnscmd /zoneexport` command. This command will export zone file copies in order for the auditors to view them.

**Incorrect Answers:**

- A: Selecting this option is incorrect. You cannot use `dnscmd/zoneinfo` command because this command will display the zone info and will not export the zone files to a folder.
- B: Selecting this option is incorrect. You cannot use `ipconfig/registerdns` command because this command is used to register the dns server and view the DNS servers. `ipconfig` is used to view the IP addresses, gateway addresses and other configurations. It is also used to view DNS servers.
- D: Selecting this option is incorrect. You cannot use `ntdsutil Partition management List` commands because these commands are used to view and manage partitions.

**QUESTION NO: 75**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are responsible for two DNS servers on the network named CERTKILLER-SR06 and CERTKILLER-SR07. The table below illustrates how the servers are configured:

You receive numerous complaints from domain users stating that they are unable to connect to the Internet. You check and discover that the users experiencing problems make use of CERTKILLER-SR07 as their preferred server. You need to ensure that all user computers have Internet name resolution enabled.

What should you do?

- A. You should consider updating the `.(root)` zone on CERTKILLER-SR07.
- B. You should consider configuring CERTKILLER-SR06 to have a `.(root)` zone.
- C. You should consider deleting the `.(root)` zone from the DNS server of CERTKILLER-SR07.
- D. You should consider deleting the DNS cache on CERTKILLER-SR07.
- E. You should consider reconfiguring the DNS server of CERTKILLER-SR06.

Thereafter you can connect it to the domain.

**Answer: C**

**Explanation:**

In this scenario, you should delete the `.(root)` zone on CERTKILLER-SR07 server as it is creating a problem. Windows Server 2008 follows specific steps for host name resolution. The server checks its zone records after querying its cache. After that, the DNS server sends requests to the forwarders and then tries resolution by using root servers. The CERTKILLER-SR07 server contains a root zone by default. This disables the DNS forwarding option and the DNS cannot act as a forwarder. To enable DNS forwarding, you have to delete the root zone. To delete the root zone you can either use the DNS snap-in or the `dnscmd.exe` command-line utility. You can use `dnscmd /zonedel` parameter and specify the name of the DNS zone that you want to delete.

**QUESTION NO: 76**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows XP Professional.

CertKiller.com has its headquarters in Seattle and branch offices in Denver, Houston, Phoenix and San Francisco. You are responsible for managing a domain controller named CERTKILLER-SR04 that is located at the Seattle office. CERTKILLER-SR04 is configured to run Windows Server 2008 and has the DNS role installed. CERTKILLER-SR04 is used to provide DNS services to all offices.

The branch offices contain a file server that is configured to run Windows Server 2008. You receive numerous complaints from employees at the branch offices regarding the long time it takes them to connect to the Seattle office in order to access it. You decide to test the WAN connectivity as well as the bandwidth but are unable to find any problems. To ensure productivity throughout the network you need to make sure that employees at the branch offices are able to access the resources as fast as possible.

What should you do? (Choose all that apply.)

- A. This can be achieved by configuring the entire CertKiller.com domain with a standard primary zone.
- B. This can be achieved by installing DNS servers at all branch offices throughout the CertKiller.com domain.
- C. This can be achieved by configuring a secondary zone at the branch office and ensuring that it makes use of CERTKILLER-DC04 as a master.
- D. This can be achieved by installing DNS forwarders at the branch offices and configuring them to point to CERTKILLER-DC04.

**Answer: B,C**

**Explanation:**

:

To ensure that employees at the branch offices are able to access network resources as quickly as possible, you need to install DNS servers at every branch offices with the intention that separate DNS zones can be created for every branch office. This is because a single zone becomes overburdened and consumes valuable bandwidth to serve the queries and responses of the client computers at the branch office.

You need to then configure a secondary zone in every branch offices that uses the main office DNS server as a master. For the quick access of network resources, you should distribute copies

of a zone file among several name servers. One file is designated the primary zone, and the others are secondary zones. Administrators make changes to the primary zone, and the changes replicate to the secondary zones; this replication is called a zone transfer .

A name server is not necessarily "primary" or "secondary": it might hold the primary zone for one portion of the organization's name space, and a secondary zone for another portion. Forwarders cannot be configured in the branch office because they do not contain any DNS servers. By using a forwarder, you can manage name resolution for names outside of your network, such as names on the Internet and not the names on the internal network.

Reference : Getting Started With Microsoft DNS Server Primary and Secondary Zones

<http://www.microsoft.com/technet/archive/winntas/plan/dns0197.mspx?mfr=true>

Reference : Understanding forwarders

<http://technet2.microsoft.com/windowsserver/en/library/a3cf0184-0594-4e78-8247-609f038434381033.mspx?mfr=true>

#### QUESTION NO: 77

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com domain contains an Integrated Active Directory DNS zone. CertKiller.com has acquired another company named Courseware Publishers. Courseware Publishers consists of a domain named courseware.com that contain an Integrated Active Directory DNS zone. You receive an instruction from the CIO to make the necessary changes to the IP addresses of the DNS servers in the courseware.com domain. To ensure productivity you need to make sure that the name resolution for CertKiller.com users to the resources in courseware.com since these are two separate DNS namespaces.

What should you do?

- A. This can be accomplished by configuring the application directory partition in the Courseware.com forest in order to enlist the DNS servers in the Courseware.com forest in the partition.
- B. This can be accomplished by creating a stub zone for Courseware.com on the DNS servers in the CertKiller.com network.
- C. This can be accomplished by configuring the Zone Replication Scope for Courseware.com in order to replicate to the DNS servers in the forest.
- D. This can be accomplished by configuring DNS forwarding on the DNS servers in the CertKiller.com forest in order to enlist the DNS servers in the courseware.com forest in the

partition.

**Answer: B**

**Explanation:**

To ensure name resolution for users in CertKiller.com to access resources in Courseware.com, you need to create a stub zone for partner.com on all DNS servers in CertKiller.com. A stub zone is a copy of a zone that contains only those resource records necessary to identify the authoritative Domain Name System (DNS) servers for that zone. A stub zone is used to resolve names between separate DNS namespaces. This type of resolution may be necessary when a corporate merger requires that the DNS servers for two separate DNS namespaces resolve names for clients in both namespaces

Reference : DNS Stub Zones in Windows Server 2003

[http://www.windowsnetworking.com/articles\\_tutorials/DNS\\_Stub\\_Zones.html](http://www.windowsnetworking.com/articles_tutorials/DNS_Stub_Zones.html)

**QUESTION NO: 78**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network are configured to run Windows Server 2008.

CertKiller.com has its headquarters in Chicago and a branch office in Dallas. There are domain controllers at the Chicago office as well as the Dallas office. The domain controllers at the Dallas office are configured as Read-Only Domain Controllers (RODC). At both offices the Active Directory-integrated DNS zones are installed on the domain controllers. The user workstations make use of the local domain controllers for DNS resolution.

The CIO wants you to make sure that any modifications to the IP address on an existing server at the Chicago office is reflected immediately on the DNS servers in the Branch office.

What should you do?

- A. You should consider decreasing the Minimum (default) TTL option on the Start of Authority (SOA) record for the CertKiller.com zone.
- B. You should consider running the `dnscmd /ZoneUpdateFromDs` command on a Read-Only Domain Controller at the Chicago office.
- C. You should consider running the `dnscmd /ZoneUpdateFromDs` command on the servers at the branch office.
- D. You should consider replacing the Read-Only Domain Controllers with the standard domain controllers at the branch offices at the Chicago office.

**Answer: C**

**Explanation:**

To reflect the change immediately, you need to run the `dnscmd /ZoneUpdateFromDs` command on the servers at the branch office. This command will update the specified ActiveDirectory-integrated zone from ADDS.

Reference : `dnscmd /zoneupdatefromds`

<http://technet2.microsoft.com/windowsserver2008/en/library/e7f31cb5-a426-4e25-b714-88712b8defd51033.mspx?mfr=true>

**QUESTION NO: 79**

You are employed as the exchange administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network are configured to run Windows Server 2008. CertKiller.com has its headquarters in Stockholm and a branch office in Paris.

You receive an instruction from the CIO to install DNS on a member server in a branch office. You need to make sure that the newly installed DNS server is able to query any DNS server at the Stockholm office as well as to permit a certain amount of DNS records to be transferred to the DNS server at the Paris office.

What should you do?

- A. This can be accomplished by installing a DNS server at the Paris office. Thereafter a secondary zone can be configured on it.
- B. This can be accomplished by installing a DNS server at the Paris office. Thereafter a stub zone can be configured on the DNS server at the Stockholm office.
- C. This can be accomplished by installing a DNS server at the Paris office. Thereafter a primary zone can be configured on it.
- D. This can be accomplished by installing a DNS server at the Paris office. Thereafter a stub zone can be configured on it.

**Answer: D**

**Explanation:**

To ensure that the DNS server at the Paris office is able to query any DNS server in the Stockholm office and that only a limited number of DNS records are transferred to the DNS server in the Paris office, you need to install a DNS server in the Paris office and configure a stub zone on it.

A stub zone is a copy of a zone that contains only the resource records that are necessary to



identify the authoritative DNS servers for that zone. A stub zone keeps a DNS server hosting a parent zone aware of the authoritative DNS servers for its child zone. Therefore it needs to be configured at the branch office only. Because a stub zone contains only a copy of the SOA record, NS records for all name servers authoritative, a records for all name servers authoritative for the zone and no CNAME records, MX records, SRV records, or a records for other hosts in the zone, they are always very small, just a few records. This will result in a limited numbers of DNS records being transferred to the DNS server in the Paris office and replicating zone information from master to stub zone adds almost nil DNS traffic to your network as the records for name servers rarely change unless you decommission an old name server or deploy a new one.

Reference : DNS Server Role

<http://technet2.microsoft.com/windowsserver2008/en/library/533a1cfc-5173-4248-914c-433bd018f66d1033.mspx?mfr=true>

Reference : What is Stub zone in DNS/ What Stub Zones Do

<http://caloni00net.blog.dada.net/post/439393/What+is+Stub+zone+in+DNS>

## QUESTION NO: 80

You are employed as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com is in partnership with another company named TestLabs.com. The servers on both domains are configured to run Windows Server 2008.

You are responsible for a CertKiller.com server named CERTKILLER-SR01. CERTKILLER-SR01 is configured to run the DNS server role. There is a server on the TestLabs.com network named TESTLABS-SR02 that is configured to run the DNS server role. CERTKILLER-SR01 contains a stub zone. The master for the stub zone on CERTKILLER-SR01 is CERTKILLER-SR02.

During routine monitoring you discover that CERTKILLER-SR02 has failed. CertKiller users complain that they are unable to resolve names for the TestLabs.com network. To ensure productivity you need to ensure that the CertKiller.com users are able to resolve names for the testlabs.com network.

What should you do?

- A. You should consider decreasing the Minimum (default) TTL setting in the SOA record for the zone on TESTLABS-SR02.
- B. You should consider modifying the stub zone to a secondary zone on CERTKILLER-SR01.
- C. You should consider creating a new Service Locator (SRV) record in the primary DNS zone on TESTLABS-SR02 as well as a new host (A) record for CERTKILLER-SR01.

- D. You should consider using DNS scavenging in the DNS zone on TESTLABS-SR02.
- E. You should consider using a DNS forwarder on TESTLABS-SR02.

**Answer: B**

**Explanation:**

Users are not able to resolve names for testlabs.com because the master server has failed. To ensure that users are able to resolve names for testlabs.com in such a scenario, you need to change the stub zone to a secondary zone on CERTKILLER-SR01. This is because the primary name server notifies the secondary zone server keeps an identical copy of the primary zone. Although it contains read-only zone information, it can resolve names of the existing names.

You need to remove the stub zone because it requires the IP address of at least one DNS server in the source domain to the DNS server hosting the stub zone. If this server goes down, then the stub zone records eventually expire.

Reference : The Long and Short of Stub Zones / What Happens if a Source Server Goes Offline?  
<http://redmondmag.com/columns/article.asp?EditorialsID=641>

Reference : DNS Stub Zones in Windows Server 2003  
[http://www.windowsnetworking.com/articles\\_tutorials/DNS\\_Stub\\_Zones.html](http://www.windowsnetworking.com/articles_tutorials/DNS_Stub_Zones.html)

**QUESTION NO: 81**

You are employed as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest. All the servers on the network are configured to run Windows Server 2008 and all the domain controllers run the DNS server role.

CertKiller.com has its headquarters in London and branch offices in Paris, Berlin, Madrid and Athens. You receive an instruction from the CIO to decommission the WINS service. To ensure productivity throughout the forest you need to enable forest-wide single name resolution.

What should you do?

- A. This can be accomplished by creating a LegacyWINS zone.  
Thereafter host (A) records should be created for single name resolution in a stub zone.
- B. This can be accomplished by creating a CKGlobalNames zone.  
Thereafter host (A) records should be created for single name resolution.
- C. This can be accomplished by creating Service Locator (SRV) records for the single name resolution.
- D. This can be accomplished by enabling WINS-R lookup in DNS for single name resolution.

**Answer: B**

**Explanation:**

In order to decommission the WINS service and to enable forest-wide single name resolution, you need to create an Active Directory-integrated zone named CKGlobalNames as well as creating host (A) records for the single name resources.

GNZ is intended to aid the retirement of WINS. Windows Server 2008 (WS2K8) introduces the GlobalNames zone (GNZ) where larger environments with multiple DNS suffixes can use a single name host across all domains.

To help customers migrate to DNS for all name resolution, the DNS Server role in Windows Server 2008 supports a special GlobalNames Zone (also known as GNZ) feature. Some customers in particular require the ability to have the static, global records with single-label names that WINS currently provides. These single-label names typically refer to records for important, well-known and widely-used servers for the company, servers that are already assigned static IP addresses and are currently managed by IT-administrators using WINS. GNZ is designed to enable the resolution of these single-label, static, global names for servers using DNS.

Reference : Understanding GlobalNames Zone in Windows Server 2008

<http://www.petri.co.il/windows-DNS-globalnames-zone.htm>

**QUESTION NO: 82**

You work as a network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network are configured to run Windows Server 2008.

A CertKiller.com employee named Mia Hamm is assigned a client workstation named CERTKILLER-WS05. You receive an instruction from the CIO to prohibit host (A) record scavenging on CERTKILLER-WS05. Mia Hamm accesses the network from time to time. CERTKILLER-WS05 is configured to obtain IP address data from the DHCP server on the network.

What should you do?

- A. Your best option would be to assign CERTKILLER-WS05 a static address.
- B. Your best option would be to disable scavenging on the zone which the record is created.
- C. Your best option would be to disable scavenging on the server which CERTKILLER-WS05 registers its record.
- D. Your best option would be to create an A record manually for CERTKILLER-WS05.

E. Your best option would be to create a SRV record for CERTKILLER-WS05

**Answer: D**

**Explanation:**

If a record is manually created, you can be assured that it will not be scavenged.

**Incorrect Answers:**

A: Although you assign a static address, it will still register the same way as the DHCP clients.

B: You are required to prevent the host (A) record from being scavenged. All the records in the zone will be affected when you disable scavenging.

C: You are required to prevent the host (A) record from being scavenged. Preventing scavenging on CERTKILLER-WS05 will affect all the records on it. You only want to prevent a single record.

**QUESTION NO: 83**

You work as a network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network are configured to run Windows Server 2008.

You have finished the configuration of a DNS server named CERTKILLER-SR06. CERTKILLER-SR06 will only be utilized to provide name resolution for the CertKiller.com domain. During routine monitoring you discover records of unauthorized workstations in the CertKiller.com zone. Upon further investigation you detect that these workstations do not have accounts in the domain. You receive an instruction to stop the unauthorized workstations from registering host (A) records with CERTKILLER-SR06.

What should you do? (Choose all that apply.)

A. You should consider clearing the option to store the zone in Active Directory.

B. You should consider configuring the zone to only accept secure updates.

C. You should consider configuring the zone to accept secure as well as nonsecure dynamic updates.

D. You should consider recreating the zone on the domain controller.

E. You should consider selecting the option to store the zone in Active Directory.

F. You should consider using the dnscmd ./clearcache command.

**Answer: B,D,E**

**Explanation:**

You should configure the zone to accept only secure updates. This will prevent the other workstations that do not belong to the Active Directory Domain from registering with CERTKILLER-SR06. However, this is only available if you store the DNS zone Active Directory and create the zone on a domain controller.

**Incorrect Answers:**

A: To obtain secure updates for the zone, you have to store the zone in the Active Directory.

C: CertKiller.com wants you to stop the unauthorized workstations from registering host (A) records. You should therefore not accept nonsecure dynamic updates.

F: This command will immediately resolve updated DNS records and the question asks specifically to stop unauthorized workstations from registering host (A) records.

**QUESTION NO: 84**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

As part of the upgrade process of CertKiller.com you need to transition the DNS services to the Active Directory integrated zones. To accomplish this task you need to determine the key features that are involved.

What should you identify?

- A. The Active Directory integrated zones will be stored in Active Directory.
- B. Dynamic updates will be allowed.
- C. Replication will be more efficient and secure.
- D. The zone records will be kept as Active Directory objects.

**Answer: A,B,C,D**

**Explanation:**

Permissions permits secure dynamic updates. The replication of zone records will happen at the property level. These records are encrypted and compressed. The records of the integrated zones are kept in the AD directory services. The records are kept inactive Directory which is objects that the permissions are assigned to.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 85**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You receive an instruction from the CIO to design a secure facility. You need to make sure that the secure facility is detached from the Internet. You need to determine what needs to be

recommended for DNS.

What should you do?

- A. Your best option would be to recommend the use of secure dynamic updates.
- B. Your best option would be to recommend the use of a private DNS infrastructure with internal root hint servers.
- C. Your best option would be to recommend the use of secondary zones.
- D. Your best option would be to recommend the use of Active Directory integrated zones.
- E. Your best option would be to recommend the use of stub zones.

**Answer: B,D**

**Explanation:**

In this scenario your best option would be to recommend the use of integrated Active Directory zones and a private DNS infrastructure with internal root hint servers. When the DNS infrastructure is isolated from the Internet you have to configure it with root hints. The root hints have to be pointed to the internal servers. The default Windows Server 2008 servers usually point to the Internet's root name servers. The Active Directory zones will supply you with extra security and fault tolerance.

Recommending the use of secure dynamic updates is incorrect. Dynamic updates should not be permitted in secure environments.

Recommending the use of secondary zones is incorrect. Secondary zones are less secure than Active Directory zones.

Recommending the use of stub zones is incorrect. Stub zones are used to streamline name resolution in split namespace scenarios.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 86**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com has its headquarters in Athens and a branch office in Madrid. The offices connect to each other via a WAN link. You are in the process of configuring a domain controller named CERTKILLER-DC05 at the Athens office as a DNS server for the CertKiller.com DNS zone. You configure CERTKILLER-DC05 as a standard primary zone.

You receive an instruction from the CIO to install a new domain controller at the Madrid office. You install DNS on the new domain controller is named CERTKILLER-DC09. To ensure productivity you need to make sure that the DNS service on CERTKILLER-DC09 is able to update records as well as resolving DNS queries in the event of a WAN link failure.

What should you do?

- A. You should consider converting maks.CertKiller.com on CERTKILLER-DC05 to an Active Directory-integrated zone
- B. You should consider configuring the DNS for conditional forwarding from CERTKILLER-DC05 to CERTKILLER-DC09.
- C. You should consider configuring a new stub zone on CERTKILLER-DC05. Thereafter the forwarding option should be set to CERTKILLER-DC09
- D. You should consider adding a secondary zone named raks.CertKiller.com on CERTKILLER-DC09

**Answer: A**

**Explanation:**

To make sure that the DNS service on CERTKILLER-DC09 can update records and resolve DNS queries in the event of a WAN link failure, you should convert maks.CertKiller.com on CERTKILLER-DC05 to an Active Directory-integrated zone. Active Directory-integrated DNS, offers two pluses over traditional zones. For one, the fault tolerance built into Active Directory eliminates the need for primary and secondary nameservers. Effectively, all nameservers using Active Directory-integrated zones are primary nameservers. This has a huge advantage for the use of dynamic DNS as well: namely, the wide availability of nameservers that can accept registrations. Recall that domain controllers and workstations register their locations and availability to the DNS zone using dynamic DNS. In a traditional DNS setup, only one type of nameserver can accept these registrations-the primary server, because it has the only read/write copy of a zone. By creating an Active Directory-integrated zone, all Windows Server 2008 nameservers that store their zone data in Active Directory can accept a dynamic registration, and the change will be propagated using Active Directory multimaster replication.

Reference: [http://safari.adobepress.com/9780596514112/active\\_directory-integrated\\_zones](http://safari.adobepress.com/9780596514112/active_directory-integrated_zones)

**QUESTION NO: 87**

You are employed as a network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The domain controllers on the CertKiller.com network run Windows server 2008 as is configured as DNS servers.



There is one Active-Directory integrated DNS zone configured on the domain. You receive an instruction from the CIO to ensure that any outdated DNS records are removed from the DNS zone automatically.

What should you do?

- A. Your best option would be to execute the netsh/Reset DNS command from the Command prompt.
- B. Your best option would be to enable Scavenging by accessing the zone properties.
- C. Your best option would be to disable the updates from the zone properties.
- D. Your best option would be to change the TTL of the SOA record by accessing the zone properties.

**Answer: B**

**Explanation:**

To remove the outdated DNS records from the DNS zone automatically, you should enable Scavenging through Zone properties. Scavenging will help you clean up old unused records in DNS. Since "clean up" really means "delete stuff" a good understanding of what you are doing and a healthy respect for "delete stuff" will keep you out of the hot grease. Because deletion is involved there are quite a few safety valves built into scavenging that take a long time to pop. When enabling scavenging, patience is required.

Reference: <http://www.gilham.org/Blog/Lists/Posts/Post.aspx?List=aab85845-88d2-4091-8088-a6bbce0a4304&ID=211>

**QUESTION NO: 88**

CertKiller.com has hired you as a network administrator for their network. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows server 2008 as is configured as DNS servers.

You are responsible for managing two domain controllers named CERTKILLER-DC01 and CERTKILLER-DC02. CERTKILLER-DC01 contains a standard Primary zone CERTKILLER-DC02 a standard secondary zone for the network. You receive an instruction from the CIO to ensure that the replication of the CertKiller zone is encrypted.

What should you do?

- A. Your best option would be to configure the zone transfer settings on the standard primary zone. Thereafter the master server's lists should be modified on the secondary zone.
- B. Your best option would be to create a stub zone. Thereafter the secondary zone can be modified into an additional primary zone.

- C. Your best option would be to convert the primary zone into an active directory zone.  
Thereafter the secondary zone can be deleted
- D. Your best option would be to change the interface where DNS server listens on both servers.

**Answer: C**

**Explanation:**

Your best option in this scenario is option C. To ensure that the replication of the CertKiller.com zone is encrypted to prevent data loss, you need to convert the primary zone into an active directory zone and delete the secondary zone.

**QUESTION NO: 89**

You are employed as a network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters in Dallas and a branch office in Chicago. All domain controllers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com network contains two domain controllers named CERTKILLER-DC01 and CERTKILLER-DC02. The Chicago office contains a Read-only domain controller named CERTKILLER-DC06. All domain controllers are configured as Active Directory integrated zones and have the DNS server role installed.

The DNS zones are configured to only permit secure updates. You receive an instruction from the CIO to enable dynamic DNS updates on CERTKILLER-DC06.

What should you do?

- A. This can be accomplished by creating an active partition on CERTKILLER-DC01.  
Thereafter the partition should be configured to store the Active Directory-integrated zones.
- B. This can be accomplished to reconfigure the RODC on CERTKILLER-DC06 in order to permit dynamic updates.
- C. This can be accomplished by executing the dnscmd/ZoneResetType command on CERTKILLER-DC06.
- D. This can be accomplished by decreasing the Minimum (default) TTL option to 10 minutes on the Start of Authority (SOA) record for the zone.

**Answer: B**

**Explanation:**

To enable the dynamic DNS updates on CERTKILLER-DC06, you should uninstall the Active Directory Domain services on CERTKILLER-DC06 and reinstall it as a writeable domain controller. A writeable domain controller performs originating updates and outbound replication.

Reference: <http://msdn.microsoft.com/en-us/library/cc207937.aspx>

**QUESTION NO: 90**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of an Active Directory forest that contains a single domain named us.CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The domain controllers on the network are configured as DNS servers. The CertKiller.com network contains two Active directory-integrated zones: CertKiller.com and courseware.com. Due to company growth CertKiller appoints a new user named Amy Walsh in the Research and Development department. You receive an instruction from the CIO to ensure that Amy Walsh is able to modify records in CertKiller.com. However, you need to ensure that she is unable to make any modifications the SOA record in the courseware.com zone.

What should you do?

- A. Your best option would be to modify the Domain Controllers organizational unit by accessing the Active Directory Users and Computers console.
- B. Your best option would be to modify the permission of the courseware.com zone by accessing the DNS Manager Console.
- C. Your best option would be to modify the permissions of courseware.com zone by accessing the WINS Manager Console.
- D. Your best option would be to configure the user permissions on CertKiller.com to encompass all users.

Thereafter the Minimum (Default) TTL should be reduces in the Start of Authority (SOA) records.

- E. Your best option would be to configure the user permissions on CertKiller.com to encompass all users.

Thereafter the user permissions should be configured on courseware.com to only permit the administrators group to make any modifications to the records.

**Answer: C**

**Explanation:**

Your best option in this scenario would be Option C. In order to allow the user to modify records in CertKiller.com and prevent him/her to modify the SOA record in courseware.com zone, you should set the permissions of CertKiller.com through DNS Manager Console. You set the permissions for the users to modify the records in CertKiller.com. You will be preventing users from modifying anything else on the other zones by setting permissions on one Active Directory integrated zone.

**QUESTION NO: 91**

You are the newly appointed systems administrator at CertKiller.com. CertKiller.com has its headquarters in Chicago and a branch office in Miami. All servers on the CertKiller.com network run Windows Server 2008.

The Chicago office consists of a domain controller named CERTKILLER-DC05. CERTKILLER-DC05 hosts a DNS primary zone. The Miami office contains a DNS server named CERTKILLER-SR03. CERTKILLER-SR03 hosts a DNS secondary zone.

The user workstations on the network are configured to make use of their local server for DNS resolution. In order to accomplish certain tasks you changed the IP address of an existing server named CERTKILLER-SR04 at the Chicago office. You need to make sure that CERTKILLER-SR03 reflects changes immediately.

What should you do?

- A. You should consider restarting the DNS Server service on CERTKILLER-DC05.
- B. You should consider running the `dnscmd /zonerefresh` command on CERTKILLER-SR03.
- C. You should consider running the `dnscmd /zonerefresh` command on CERTKILLER-DC05.
- D. You should consider changing all domain controllers to Read-Only domain controllers.

**Answer: B**

**Explanation:**

To ensure that CERTKILLER-SR03 reflects the change immediately, you need to run the `dnscmd` command on CERTKILLER-SR03. Thereafter the `/zonerefresh` option should be used for the command.

The `dnscmd /zonerefresh` option will manually force zone replication on CERTKILLER-SR03.

Reference : How can I easily administer DNS servers by using the command prompt?

[http://www.petri.co.il/dnscmd\\_command\\_in\\_windows\\_2000\\_2003.htm](http://www.petri.co.il/dnscmd_command_in_windows_2000_2003.htm)

**QUESTION NO: 92**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of an Active Directory forest that contains a single domain named `us.CertKiller.com`. All servers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com network contains a Windows Server 2008 server named CERTKILLER-SR01. CERTKILLER-SR01 is configured to run the DNS server role. During a routine security check you

discover a small number of stale resource records in the us.CertKiller.com zone. You decide to remove the stale records by enabling DNS scavenging on CERTKILLER-SR01.

A month later, during another security check, you detect that the same stale resource records are still there. You receive an instruction from the CIO to ensure that the stale resource records are removed.

What should you do?

- A. You should consider running the `dnscmd CertKillerServer1 /AgeAllRecords` command.
- B. You should consider stopping and restarting the DNS service on CERTKILLER-SR01.
- C. You should consider running the `dnscmd CERTKILLER-SR01/StartScavenging` command.
- D. You should consider enabling DNS scavenging on the us.CertKiller.com zone.
- E. You should consider running the `dnscmd ./zonerefresh` command.

**Answer: D**

**Explanation:**

Using the DNS scavenging will remove stale records even if there is no CertKiller.com integrated zone with AD DS installed on the server. Obviously it has to be enabled first.

Stopping and restarting the DNS service does not necessarily purge stale records ..

The StartScavenging command option is also configured for specific zones and to ensure that stale records are removed you should first enable scavenging.

The Zone Aging / Scavenging Properties need not be configured because they perform cleanup and removal of stale resource records (RRs), which can accumulate in zone data over time. With dynamic update, RRs are automatically added to zones when computers start on the network. However, in some cases, they are not automatically removed when computers leave the network. Thus they contain stale entries which may lead to wrong information.

The `dnscmd ./ zonerefresh` command reflects any changes in resource records immediately and not remove stale records.

**QUESTION NO: 93**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of an Active Directory forest that contains a single domain named us.CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. CertKiller.com has its headquarters in London and branch offices in Paris, Berlin and Athens. The offices are connected to each other via a WAN link.

The London office contains three domain controllers that are configured to run the DNS service. The Active Directory-integrated zone is configured at the London office for the domain. The branch

offices all contain a member server that is configured to host a secondary zone for the domain.

At present the DNS servers located at the branch office make use of the DNS server at the London office as the DNS Master server for the zone. You need to determine the best way to reduce DNS zone transfer traffic over the WAN links.

What should you do?

- A. Your best option would be to increase the Refresh Interval setting in the SOA record.
- B. Your best option would be to decrease the Refresh Interval setting in the SOA record.
- C. Your best option would be to increase the Retry Interval setting in the SOA record.
- D. Your best option would be to make use of caching only DNS servers for the zone.
- E. Your best option would be to disable the netmask ordering option in the properties of the DNS Master server for the zone.

**Answer: A**

**Explanation:**

To minimize DNS zone transfer traffic over the WAN links, you need to increase the Refresh Interval setting in the Start Of Authority (SOA) record for the zone. This is because the Refresh interval tells the secondary nameserver how often to poll the primary nameserver and how often to check for a serial number change.

This interval effects how long it takes for DNS changes made on the primary nameserver to propagate. If the refresh interval is higher that the transfers will occur less frequently and the DNS zone transfer traffic over the WAN links will be minimized.

Reference : DNS Resource Records / SOA Record Data Fields

[http://www.cisco.com/en/US/tech/CK648/CK362/technologies\\_tech\\_note09186a0080094727.shtml#topic2](http://www.cisco.com/en/US/tech/CK648/CK362/technologies_tech_note09186a0080094727.shtml#topic2)

**QUESTION NO: 94**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently has their office located in Miami where a public DNS server named CERTKILLER-SR01 and e-mail server named CERTKILLER-SR02 is located.

During the course of the day you receive complaints from the network users stating when outside the office they are unable to send e-mail messages to the CertKiller.com domain. You have later started troubleshooting and verified the availability of host (A) DNS records for CERTKILLER-

SR02 to the external client computers. CertKiller.com wants you to select the appropriate DNS record type which should be used on the CertKiller.com DNS zone to ensure e-mail is received.

What should you do?

- A. You should consider having a Service Location (SRV) DNS record added for CERTKILLER-SR02 and set the Service field to \_smtp and Protocol field to \_tcp, and the Port Number to 25.
- B. You should consider having a Canonical (CNAME) DNS record added for CERTKILLER-SR02 which maps CERTKILLER-SR02 to CertKiller.com.
- C. You should consider having a (A) Host record added for CERTKILLER-SR02.
- D. You should consider having a Mail Exchanger (MX) DNS record added for CERTKILLER-SR02.
- E. You should consider having a Mailbox (MB) DNS record added for CERTKILLER-SR02 and set the Mailbox Host setting to CERTKILLER-SR02.

**Answer: D**

**Explanation:**

:

To ensure that CERTKILLER-SR02 can receive e-mail messages from external client computers, you need to add a Mail Exchanger (MX) record for CERTKILLER-SR02. MX records control how e-mail is delivered. They are used to locate the receiving mail servers for a given host, and the order of priority of these mail servers. Sometimes the non-RFC-compliant servers fail to deliver email for domains that lack MX records, including certain versions of Microsoft Exchange.

You can configure Mail Exchanger (MX) record for CERTKILLER-SR02 also because host (A) DNS record for CERTKILLER-SR02 is available to external client computers, which is required for its configuration. It requires Mail Exchanger field that defines the destination host record for your mail server. The destination mail server record must be a host (A) record, not a CNAME or IP address

Reference : E-mail, Mail Exchangers, and DNS

[http://www.dyndns.com/support/kb/email\\_mail\\_exchangers\\_and\\_dns.html](http://www.dyndns.com/support/kb/email_mail_exchangers_and_dns.html)

## QUESTION NO: 95

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named us.CertKiller.com and public name space CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the business day you receive instruction from CertKiller.com to ensure that the CertKiller.com public DNS zone records are not copied without impacting the functionality of



public name resolution requests.

What should you do?

- A. You should consider having the Service Locator (SRV) resource record enabled on all domain controllers on us.CertKiller.com.
- B. You should consider having the Notify feature deselected for the CertKiller.com zone.
- C. You should consider having the Allow - Read permission in the Everyone group disabled on the CertKiller.com DNS domain
- D. You should consider having the Allow zone transfers only to servers listed on the Name Servers option enabled on CertKiller.com.

**Answer: D**

**Explanation:**

:

To ensure that public DNS zone records cannot be copied without impacting the functionality of public DNS name resolutions, you need to configure the Allow zone transfers only to servers listed on the Name Servers option on CertKiller.com. This setting allows you to restrict zone transfers only to DNS servers listed in the Name Servers resource option on CertKiller.com.

Reference : DNS Zones

<http://books.google.co.in/books?id=pL89TOMFcHsC&pg=RA1-PA244&lpg=RA1-PA244&dq=Allow+zone+transfers+only+to+servers+listed+on+the+Name+Servers+option+&source=web&ots=StFz29rSf5&sig=0wRSARkgYxCy2ohweQs4QUDMqEQ&hl=en#PRA1-PA243,M1>

## QUESTION NO: 96

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch offices in Toronto Atlanta and Philadelphia.

CertKiller.com currently has the domain controllers in the Miami office hosting an Active Directory-integrated zone. The Toronto Atlanta and Philadelphia offices DNS server hosts a secondary zone which has the Miami office DNS servers configured as Master Servers for the zone for the CertKiller.com domain.

During the course of the day you receive instruction to travel to London and deploy a new member server named CERTKILLER-SR07 which will have the DNS service installed and configured as a secondary zone for the domain. You later started configured CERTKILLER-SR04 and you discovered that the zone transfer fails. CertKiller.com wants you to provide zone data to the DNS servers in London.

What should you do?

- A. You should consider having CERTKILLER-SR07 added to the DNSUpdateProxy Global security group in Active Directory Users and Computers.
- B. You should consider having the `dnscmd /ZoneResetMasters` command run after adding CERTKILLER-SR07 to the global security group in Active Directory Users and Computers.
- C. You should consider having the Use Zone Transfers tab used on one DNS servers in the Miami office in order to add CERTKILLER-SR07 to it.
- D. You should consider having the `dnscmd /ZoneResetSecondaries` command run.

**Answer: C**

**Explanation:**

:

To configure DNS to provide zone data to the DNS server in the new branch office, you need to add the new DNS server to the Zone Transfers tab on one of the DNS servers in the main office. You can use any DNS servers in the main office because main office hosts an Active Directory-integrated zone and effectively, all nameservers using Active Directory-integrated zones are primary nameservers.

To enable zone transfers for a single zone, you need to click the "Records" button in the main window. Then in the DNS Records window, right-click on the zone that you wish the enabled zone transfers for and select "Properties" from the popup menu. In the "Zone Properties" dialog, select the "Zone Transfers" tab, and specify which IP addresses are allowed to zone transfer:

Reference : 4.8. Active Directory-Integrated Zones

[http://safari.adobepress.com/9780596514112/active\\_directory-integrated\\_zones](http://safari.adobepress.com/9780596514112/active_directory-integrated_zones)

Reference : Enabling Zone Transfers from another DNS server

<http://www.simplifiedns.com/kb.aspx?kbid=1156>

Part 3, Configure DNS records (8 Questions)

### QUESTION NO: 97

You are employed as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows XP Professional.

CertKiller.com has its headquarters in London and branch offices in Paris, Berlin, Milan and

Stockholm. All domain controllers at the London office host an Active Directory-integrated zone. All branch offices have one DNS server that host the secondary zone for the domain. These DNS servers make use of the DNS servers located at the London office as their DNS Master servers.

Due to company growth CertKiller.com opens another branch office in Athens. You install a new member server at the Athens office named CERTKILLER-SR10. You install the DNS service and configured a secondary zone on CERTKILLER-SR10 for the domain. Whilst monitoring CERTKILLER-SR10 you discover that the zone transfer fails. To ensure productivity from the Athens office you need to configure the DNS to provide CERTKILLER-SR10 with zone data.

What should you do?

- A. You should consider adding CERTKILLER-SR10 to the DNSUpdateProxy Global security group in Active Directory Users and Computers.
- B. You should consider adding CERTKILLER-SR10 on one of the DNS servers at the London office using the Zone Transfers tab.
- C. You should consider running the `dnscmd /ZoneResetMasters` command after adding CERTKILLER-SR10 to the global security group in Active Directory Users and Computers
- D. You should consider running the `dnscmd /ZoneResetSecondaries` command after adding CERTKILLER-SR10 to the global security group in Active Directory Users and Computers.

**Answer: B**

**Explanation:**

:

To configure DNS to provide zone data CERTKILLER-SR10 you need to add CERTKILLER-SR10 to the Zone Transfers tab on one of the DNS servers at the London office. You are able to use the DNS servers at the London office since it hosts the Active Directory-integrated zone. All nameservers using Active Directory-integrated zones are primary nameservers.

To enable zone transfers for a single zone, you need to click the "Records" button in the main window. Then in the DNS Records window, right-click on the zone that you wish the enabled zone transfers for and select "Properties" from the popup menu. In the "Zone Properties" dialog, select the "Zone Transfers" tab, and specify which IP addresses are allowed to zone transfer.

Reference : 4.8. Active Directory-Integrated Zones

[http://safari.adobepress.com/9780596514112/active\\_directory-integrated\\_zones](http://safari.adobepress.com/9780596514112/active_directory-integrated_zones)

Reference : Enabling Zone Transfers from another DNS server

<http://www.simplifiedns.com/kb.aspx?kbid=1156>

**QUESTION NO: 98**

You are an enterprise administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All domain controllers in the domain are configured to run Windows Server 2008 and all client computers Windows Vista.

CertKiller.com has recently went into partnership with another company named Courseware Ltd. The partner company consists of an Active Directory domain named courseware.com. Domain controllers at courseware.com are configured to run Windows Server 2008. You configure a two-way forest trust between tesCKin.com and courseware.com. You receive an instruction from the CIO to ensure that tesCKin.com users are able to access the resources in courseware.com. You decide to edit the CertKiller.com GPO to accomplish this task.

What should you do?

- A. This can be achieved by configuring the Allow DNS Suffix Appending to Unqualified Single-Label Name Queries option to False.
- B. This can be achieved by configuring the Primary DNS Suffix option to CertKiller.com, courseware.com.  
Thereafter the Primary DNS Suffix Devolution option should be changed to False.
- C. This can be achieved by configuring the DNS Suffix Search List option to CertKiller.com, courseware.com.
- D. This can be achieved by configuring the Allow DNS Suffix Appending to Unqualified Multi-Label Name Queries option to True.

**Answer: C**

**Explanation:**

:

To enable tesCKin.com users to access resources in thecourseware.com domain you need to configure the DNS Suffix Search List option to CertKiller.com, courseware.com.

DNS Suffix Search List needs to be configured where disjoint namespaces exist.

A merger or acquisition may cause you to have a topology with a disjoint namespace. A disjoint namespace scenario is one in which the primary DNS suffix of a computer does not match the DNS domain name where that computer resides. As in this case the two namespaces, ad.techblasters.com and ad.CertKiller.com exist. When you make the transition to a disjoint namespace, you need to create customized DNS suffix search lists to ensure that clients can locate services and other computers when they perform single-label name queries.

Reference : Understanding Disjoint Namespace Scenarios with Exchange 2007  
[http://technet.microsoft.com/en-us/library/bb676377\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb676377(EXCHG.80).aspx)

Reference : Create a Disjoint Namespace / Update the DNS suffix search list

<http://technet2.microsoft.com/windowsserver2008/en/library/afe94bc3-41fb-4817-84b5-5517c38a0d391033.msp?mfr=true>

### QUESTION NO: 99

You are the newly appointed network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You receive an instruction from the CIO to prevent then DNS zone records from being copied. You need to accomplish this task without affecting the functionality of the public DNS name resolutions.

What should you do?

- A. Your best option would be to deselect the Notify feature for the CertKiller.com zone in Active Directory Users and Computers.
- B. Your best option would be to disable the Allow-Read permission in the Everyone group on the CertKiller.com DNS domain in the Active Directory Users and Computers.
- C. Your best option would be to enable the All domain controllers in the domain zone replication option on CertKiller.com.
- D. Your best option would be to enable the Allow zone transfers only to servers listed on the Name Servers option on CertKiller.com.

**Answer: D**

**Explanation:**

:

To ensure that public DNS zone records cannot be copied without impacting the functionality of public DNS name resolutions, you need to configure the Allow zone transfers only to servers listed on the Name Servers option on contoso.com. This setting allows you to restrict zone transfers only to DNS servers listed in the Name Servers resource option on contoso.com.

Reference : DNS Zones

<http://books.google.co.in/books?id=pL89TOMFcHsC&pg=RA1-PA244&lpg=RA1-PA244&dq=Allow+zone+transfers+only+to+servers+listed+on+the+Name+Servers+option+&source=web&ots=StFz29rSf5&sig=0wRSARkgYxCy2ohweQs4QUdMqEQ&hl=en#PRA1-PA243,M1>

### QUESTION NO: 100

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are responsible for managing a Windows Server 2008 domain controller named CERTKILLER-SR05. CERTKILLER-SR05 is configured to host the DNS role. You receive an instruction from the CIO to make sure that enquiries regarding the company are sent to `dnsadmin@CertKiller.com`. To accomplish this you decide to modify certain DNS records.

What should you identify?

- A. You should modify the Start of Authority (SOA) record.
- B. You should modify the Name Server (NS) record.
- C. You should modify the Signature (SIG) record.
- D. You should modify the LM Hosts record.

**Answer: A**

**Explanation:**

To ensure that inquiries about CertKiller.com are sent to `dnsadmin@CertKiller.com`, you need to modify the Start of Authority (SOA) record on the domain controller. This is because it contains entry that includes the name of the machine on which this file was created, followed by the name of the responsible person in "dotted email address" form. Replace the first dot with an @ sign that allows you to ensure that inquiries of a domain are sent to the specified responsible person of the domain on the email address specified.

Reference : An Introduction to DNS

<http://www.htmlgoodies.com/beyond/webmaster/article.php/3473261>

Reference : Updating Zone Properties and the SOA Record

<http://safari.awprofessional.com/0735613540/IDAFMSU>

**QUESTION NO: 101**

You are an enterprise administrator for CertKiller.com. The corporate network of the company consists of a single Active Directory domain called CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client workstations run Windows Vista.

The CertKiller.com domain consists of a public DNS server and an e-mail server. The public DNS server is named CERTKILLER-SR05 and the e-mail server CERTKILLER-SR06. You receive numerous complaints stating that client workstations outside the CertKiller.com domain are experiencing problems sending e-mail messages to the company. You check and confirm the availability of host (A) DNS record for CERTKILLER-SR06 to external client computers. You need to make sure that CERTKILLER-SR06 is able to receive e-mail messages from client workstations outside the domain.

What should you do?

- A. This can be accomplished by adding a Service Location (SRV) record for CERTKILLER-SR06. Thereafter should set the Service field to `_smtp`, the Protocol field to `_tcp` and the Port Number to 25.
- B. This can be accomplished by adding a Canonical (CNAME) record that will map CERTKILLER-SR06 to CertKiller.com. Thereafter add a host (A) record.
- C. This can be accomplished by adding a Mail Exchanger (MX) record for CERTKILLER-SR06.
- D. This can be accomplished by adding a Mailbox (MB) record for CERTKILLER-SR06. Thereafter the Mailbox Host setting should be set to CERTKILLER-SR06.

**Answer: C**

**Explanation:**

:

Your best option in this scenario would be to select Option C. To ensure that CERTKILLER-SR06 is able to receive e-mail messages from external client computers you need to add a Mail Exchanger (MX) record for CERTKILLER-SR06. The MX records control how e-mail is delivered. They are used to locate the receiving mail servers for a given host, and the order of priority of these mail servers. Sometimes the non-RFC-compliant servers fail to deliver email for domains that lack MX records, including certain versions of Microsoft Exchange.

You are able to configure Mail Exchanger (MX) record for CERTKILLER-SR06 because a host (A) DNS record for CERTKILLER-SR06 is available to external client computers, which is required for its configuration. It requires the Mail Exchanger field that defines the destination host record for your mail server. The destination mail server record must be a host (A) record, not a CNAME or IP address

Reference : E-mail, Mail Exchangers, and DNS

[http://www.dyndns.com/support/kb/email\\_mail\\_exchangers\\_and\\_dns.html](http://www.dyndns.com/support/kb/email_mail_exchangers_and_dns.html)

## QUESTION NO: 102

You are employed as a network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com domain contains two Windows Server 2008 servers named CERTKILLER-SR01 and CERTKILLER-SR02. CERTKILLER-SR01 and CERTKILLER-SR02 are configured to host the DNS server role. You configure an additional Windows Server 2008 server named CERTKILLER-SR03 to forward DNS requests to CERTKILLER-SR02. You receive an instruction from the CIO to



make that CERTKILLER-SR03 is able to resolve the updated DNS record immediately when you update DNS records on CERTKILLER-SR02.

What should you do?

- A. You should consider running the `ipconfig /flushdns` command on all CertKiller.com client computers.
- B. You should consider running the `dnscmd /clearcache` command on CERTKILLER-SR03.
- C. You should consider increasing the Retry Interval value to 10 minutes on the Start of Authority (SOA) record of CertKiller.com.
- D. You should consider decreasing the Time-to-Live (TTL) to 10 minutes on the Start of Authority (SOA) record of CertKiller.com.
- E. You should consider restarting the DNS Client service on the all the CertKiller.com client computers.

**Answer: B**

**Explanation:**

:

To ensure that CERTKILLER-SR03 is able to resolve the updated DNS record immediately you need to run the `dnscmd . /clearcache` command on CERTKILLER-SR03.

Both the DNS server and the local DNS resolver cache any records they receive for a period of time determined by a TTL setting in the record. The SOA for the zone determines the default TTL, which is one hour for Windows DNS servers. To ensure that server immediately finds the updated record, you need to use the Clear Cache option in the server's property menu in the DNS console or use the `Dnscmd` utility with the syntax `dnscmd /clearcache`, so that less records needs to be searched.

If you restart the DNS user workstations it will only clear the DNS client cache. This will not resolve the problem and restore proper name resolution however the DNS server will still respond to query the name of the workstation.

Reference : `dnscmd . /clearcache`

<http://technet2.microsoft.com/windowsserver2008/en/library/e7f31cb5-a426-4e25-b714-88712b8defd51033.msp?mfr=true>

Reference : 10 DNS Errors That Will Kill Your Network

<http://mcpmag.com/features/article.asp?editorialsid=413>

**QUESTION NO: 103**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com network consists of two Servers named CERTKILLER-SR01 and CERTKILLER-SR02. CERTKILLER-SR01 is a domain controller that is configured to run the DNS server role. CERTKILLER-SR02 is configured to run a legacy application. You receive an instruction from the CIO to include parameters like Service, Priority, Weight Protocol, Port number and Host offering this service for the custom application on CERTKILLER-SR01. You decide to configure the DNS on CERTKILLER-SR01 to accomplish this.

What should you do?

- A. You should consider creating Host Info (HINFO) records.
- B. You should consider creating Well-Known Service (WKS) records.
- C. You should consider creating Service Locator (SRV) records.
- D. You should consider creating Pointer (PTR) resource records.
- E. You should consider creating Start of Authority (SOA) records.

**Answer: C**

**Explanation:**

Your best option in this scenario would be to create a Service Locator (SRV) record. To configure DNS on CERTKILLER-SR01 to include the parameters such as Service, Priority, Weight Protocol, Port number, and Host offering this service for the custom application, you need to configure Service Locator (SRV) records. An SRV record or Service record is a category of data in the Internet Domain Name System specifying information on available services. Service locator (SRV) resource record. Allows multiple servers providing a similar TCP/IP-based service to be located using a single DNS query operation. This record enables you to maintain a list of servers for a well-known server port and transport protocol type ordered by preference for a DNS domain name.

References : SRV Record

[http://en.wikipedia.org/wiki/SRV\\_record](http://en.wikipedia.org/wiki/SRV_record)

Resource records reference / SRV

<http://technet2.microsoft.com/windowsserver/en/library/9b561e1b-9a0d-43e5-89a8-9daf07afac0d1033.mspx?mfr=true>

**QUESTION NO: 104**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network

run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com is a fast growing company and has recently invested in an additional DNS server named CERTKILLER-SR08. You receive an instruction from the CIO to remove the pointer record for the IP address 192.168.1.100.

What should you do?

- A. You should consider running the `dnscmd /ZoneDelete 100.in-addr.arpa` command at the command prompt.
- B. You should consider running the `dnscmd /RecordDelete 192.in-addr.arpa. 100.1.168 PTR` command at the command prompt.
- C. You should consider deleting the 100.in-addr.arpa zone using DNS manager.
- D. You should consider running the `dnscmd /RecordDelete 192.168.1.100` command at the command prompt.

**Answer: B**

**Explanation:**

To delete the pointer record for the IP address 192.168.1.100, you need to use the command `run the dnscmd /RecordDelete 192.in-addr.arpa. 100.1.168 PTR`

In the above command the DNS namespace of the Pointer (PTR) resource record is specified by `targeted_domain_name`. This is often used in special domains such as the in-addr.arpa domain tree to provide reverse lookups of address-to-name mappings.

A PTR record always has a Reverse Lookup zone and reverse look-up files refer to domains by reversing the IP address octets; the filenames are usually similar. Therefore the IP address you specify is 192.in-addr.arpa. 100.1.168 PTR, which is the IP address of the Reverse loop up zone for the zone 192.168.1.100. The above given command will delete all PTR records at the 192.168.1.100 address.

The rest of the commands cannot be used because they cannot delete a PTR record.

References : Delete a resource record from a zone

<http://technet2.microsoft.com/windowsserver/en/library/9b561e1b-9a0d-43e5-89a8-9daf07afac0d1033.mspx?mfr=true>

Domain Name Service Basics

<http://www.windowsitlibrary.com/Content/212/03/3.html>

Part 4, Configure DNS replication (8 Questions)

**QUESTION NO: 105**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest that contains four domains.

All servers on the CertKiller.com network run Windows Server 2008. The domain controllers are configured as DNS servers. All CertKiller.com users make use of a Web server named TestWebApp to accomplish their daily tasks. You receive an instruction from the CIO to make sure that users are able to access the Web server via the Internet Explorer Browser tool to `http://TestWebApp`.

What should you do? (Each correct answer presents part of the solution. Choose THREE.)

- A. Your best option would be to create a GlobalNames zone on a DNS server.
- B. Your best option would be to configure TestWebApp in order to enable DFS-R on it.
- C. Your best option would be to replicate the GlobalNames zone to all domains controllers in the CertKiller.com forest.
- D. Your best option would be to create a host (A) record for TestWebApp in the GlobalNames zone.
- E. Your best option would be to create a LegacyWINS zone on a DNS server.
- F. Your best option would be to replicate the GlobalNames zone in the DNS zone for the forest root domain.

**Answer: A,C,D**

**Explanation:**

To ensure that users from all domains are able to access a TestWebApp by browsing to `http://TestWebApp` you need to create a zone named GlobalNames on a DNS server. Then GlobalNames zone can be replicated to all domain controllers in the forest. Lastly a host (A) record can be created for TestWebApp in the zone.

GlobalNames Zone (also known as GNZ) is designed to enable the resolution of the single-label, static, global names for servers using DNS. GNZ is intended to aid the retirement of WINS, and it's not a replacement for WINS. GNZ is not intended to support the single-label name resolution of records that are dynamically registered in WINS, records which typically are not managed by IT administrators.

Reference : Understanding GlobalNames Zone in Windows Server 2008

<http://www.petri.co.il/windows-DNS-globalnames-zone.htm>

**QUESTION NO: 106**

You are an Enterprise administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com has its headquarters in Chicago and branch offices in Phoenix and Miami. The offices are connected to each other via a WAN link. The Chicago office consists of three domain controllers that are configured to run the DNS service. The Active Directory-integrated zone is configured at the Chicago office for the domain. And the branch offices consist of a member server that hosts a secondary zone for the domain.

The DNS servers in the branch offices make use of the DNS server at the Chicago office as the DNS Master server for the zone. You receive an instruction from the CIO to reduce the DNS zone transfer traffic over the WAN links.

What should you do?

- A. You need to increase the Refresh Interval setting in the Start Of Authority (SOA) record for the zone.
- B. You need to reduce the Retry Interval setting to 15 minutes in the Start Of Authority (SOA) record for the zone.
- C. You need to disable the netmask ordering option in the properties of the DNS Master server for the zone.
- D. You need to run the `ipconfig /flushdns` command on a member server at the branch offices.
- E. You need to reduce the Refresh Interval setting in the Start Of Authority (SOA) record for the zone.

**Answer: A**

**Explanation:**

In order to reduce DNS zone transfer traffic over the WAN links you need to increase the Refresh Interval setting in the Start Of Authority (SOA) record for the zone. The Refresh interval tells the secondary nameserver how often to poll the primary nameserver and how often to check for a serial number change.

This interval effects how long it takes for DNS changes made on the primary nameserver to propagate. If the refresh interval is higher that the transfers will occur less frequently and the DNS zone transfer traffic over the WAN links will be minimized.

Reference : DNS Resource Records / SOA Record Data Fields

[http://www.cisco.com/en/US/tech/CK648/CK362/technologies\\_tech\\_note09186a0080094727.shtml#topic2](http://www.cisco.com/en/US/tech/CK648/CK362/technologies_tech_note09186a0080094727.shtml#topic2)

**QUESTION NO: 107**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista. CertKiller.com has its headquarters in London and a branch office in Paris.

The CertKiller.com network contains a domain controller server named CERTKILLER-DC03 that is located at the London office. CERTKILLER-DC03 is configured to host the DNS primary zone. The DNS secondary zone is hosted on a server named CERTKILLER-SR02 at the Paris office. The client computers on the CertKiller.com network use their local server for DNS resolution.

You receive an urgent task from the CIO and make the necessary changes to the IP address of a server named CERTKILLER-SR03 at the London office. You need to ensure that the changes reflect immediately on CERTKILLER-SR02.

What should you do?

- A. You need to run the `dnscmd /zonerefresh` command on CERTKILLER-DC03.
- B. You need to change all the domain controllers to Read-Only domain controllers.
- C. You need to run the `dnscmd /zonerefresh` command on CERTKILLER-SR02.
- D. You need to restart the DNS Server service on CERTKILLER-DC03.
- E. You need to set the refresh interval to 15 minutes on the Start Of Authority (SOA) record.

**Answer: C**

**Explanation:**

To ensure that the changes reflect immediately on CERTKILLER-SR02 you need to run the `dnscmd` command on CERTKILLER-SR02 and use the `/zonerefresh` option for the command.

The `dnscmd /zonerefresh` option will manually force zone replication on CERTKILLER-SR02.

Reference : How can I easily administer DNS servers by using the command prompt?

[http://www.petri.co.il/dnscmd\\_command\\_in\\_windows\\_2000\\_2003.htm](http://www.petri.co.il/dnscmd_command_in_windows_2000_2003.htm)

**QUESTION NO: 108**

You work as a network administrator at CertKiller.com. CertKiller.com has their main office located in New York and branch office located in Toronto. The main office Active Directory domain is named CertKiller.msft and the branch office Active Directory domain is named us.CertKiller.msft. CertKiller.com has discovered that the main office users require access to resources located in the us.CertKiller.com domain.

CertKiller.com informs you that the name resolution for computer names in the remote domain is very slow. CertKiller.com wants you to improve the response times of name resolution for names in us.CertKiller.com by keeping an updated list of remote name servers authoritative for the us.CertKiller.com domain whilst minimizing zone transfer traffic.

What should you do?

- A. On the us.CertKiller.msft domain perform a delegation on the DNS servers at the main office.
- B. On the DNS servers at the main office create a secondary zone of the us.CertKiller.msft domain.
- C. Conditional forwarding should be configured so queries for names in the us.CertKiller.msft domain are automatically forwarded to name server in that domain.
- D. On the DNS server at the main office create a stub zone of the us.CertKiller.msft domain.
- E. Configure DHCP clients on the client computers.

**Answer: D**

**Explanation:**

You should create a stub zone of the branch offices at the main office. This will then keep an updated list of the server in the branch office. This will also improve the name resolution.

**Incorrect Answers:**

- A: You cannot perform a delegation on the main offices. You only can perform a delegation on a child zone.
- B: You can create a secondary zone because it will also keep an updated list of the server in the branch office. This will also improve the name resolution. However, you need to update the lists of remote name servers and that will not minimize the zone transfer traffic.
- C: The conditional forwarding will provide name resolution and minimize the zone traffic transfer, however it will not update the lists of remote name servers.
- E: The client computers already have an address in the APIPA range. So they are already set up as DHCP clients. Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.134, 165, 202

**QUESTION NO: 109**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com.

You are in the process of deploying a Windows Server 2008 server named CERTKILLER-SR01. You migrate the DNS zone to CERTKILLER-SR01 using the option to store the zone in Active Directory. During routine monitoring you discover that the zone does not appear on a domain controller named CERTKILLER-SR06 that is configured to run Windows 2000 Server. CERTKILLER-SR06 was configured with the DNS server component. You receive an instruction



from the CIO to ensure that the zone appear on all domain controllers in the CertKiller.com domain.

What should you do?

- A. Your best option would be to check the option to store the zone in all DNS servers in the forest.
- B. Your best option would be to check the option to store the zone in the new partition when creating a new directory partition.
- C. Your best option would be to check the option to store the zone in all domain controllers in the domain.
- D. Your best option would be to check the option to store the zone in all DNS servers in the domain.

**Answer: C**

**Explanation:**

You should store the zone in all domain controllers in the domain. It will store data in the domain partition, which will be visible to the domain controller running Windows 2000 Server.

**Incorrect Answers:**

- A: You should not store the zone in all DNS servers in the forest CERTKILLER-SR06 will still not be able to see the data.
  - B: You should not create a new partition in a newly created directory partition. CERTKILLER-SR06 will still not be able to see the data.
  - D: You should not store the zone in all DNS servers in the domain. CERTKILLER-SR06 will still not be able to see the data.
- Reference: JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp.194

**QUESTION NO: 110**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest containing a single domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office in Toronto.

CertKiller.com has deployed domain controllers in the Toronto office which is configured as an Active Directory site. You are aware that All the CertKiller.com Active Directory sites are connected with the DEFAULTIPSITELINK object. During the course of the day you receive instruction from CertKiller.com to decrease the replication latency between the CertKiller.com domain controllers.

What should you do?

- A. You should consider having the replication interval for the DEFAULTIPSITELINK object decreased.

- B. You should consider having the replication interval for the DEFAULTIPSITELINK object increased.
- C. You should consider having the cost between the connection objects decreased.
- D. You should consider having the refresh interval reduced in the Start of Authority (SOA) record.
- E. You should consider having the connection replication interval for all connection objects decreased.

**Answer: A**

#### **QUESTION NO: 111**

Exact replica of the previous question. You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest containing a single domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office in Toronto.

CertKiller.com has deployed domain controllers in the Toronto office which is configured as an Active Directory site. You are aware that All the CertKiller.com Active Directory sites are connected with the DEFAULTIPSITELINK object. During the course of the day you receive instruction from CertKiller.com to decrease the replication latency between the CertKiller.com domain controllers.

What should you do?

- A. You should consider having the replication interval for the DEFAULTIPSITELINK object decreased.
- B. You should consider having the replication interval for the DEFAULTIPSITELINK object increased.
- C. You should consider having the cost between the connection objects decreased.
- D. You should consider having the connection replication interval for all connection objects decreased.

**Answer: A**

#### **QUESTION NO: 112**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently makes use of several servers named CERTKILLER-SR01, CERTKILLER-SR02, CERTKILLER-SR03, CERTKILLER-SR04 and CERTKILLER-SR05 which run Microsoft Windows Server 2008.

CertKiller.com has configured CERTKILLER-SR01 as the DNS server for the domain. During the

course of the business day you receive instruction by CertKiller.com to create a new Active Directory-integrated zone whilst ensuring the new zone is only replicated to four of the domain controllers.

What should you do?

- A. You should consider having a new delegation configured in the ForestDnsZones application directory partition.
- B. You should consider having the dnscmd/createdirectorypartition command run from the command prompt.
- C. You should consider having the dnscmd/enlistdirectorypartition command run from the command prompt. Then enlist all DNS servers in the partition.
- D. You should consider enlisting all DNS servers in the DomainDnsZones application directory partition.

**Answer: B**

**Explanation:**

Part 5, Configure name resolution for client computers (5 Questions)

### QUESTION NO: 113

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com has its headquarters in Phoenix and branch offices in Dallas and Miami. All domain controllers located at the Phoenix office host an Active Directory-integrated zone. The Branch offices are configured with a DNS server as well as an application server. The DNS servers at the branch offices make use of the DNS servers at the Phoenix office as their DNS Master server for the zone.

To access their local application server the branch offices use the fully qualified domain name. To ensure that productivity continues in the event of a WAN link failure of five days you need to make sure that the branch office users are able to access their local application server.

What should you do?

- A. You should consider enabling Scavenge Stale resource records in the Zone Aging / Scavenging Properties dialog box.  
Then the No-refresh interval setting should be set to 4 days.
- B. You should consider increasing the Refresh Interval setting on the Start of Authority (SOA) record for the zone to 6 days.

- C. You should consider increasing the Expires After setting on the Start of Authority (SOA) record for the zone to 6 days.
- D. You should consider enabling Scavenge Stale resource records in the Zone Aging / Scavenging Properties dialog box.
- Then the Refresh setting should be set to 6 days.
- E. Configure the Allow zone transfers only to servers listed on the Name Servers option on CertKiller.com. Then set the Refresh setting to 4 days.

**Answer: C**

**Explanation:**

To ensure that users in the branch offices can access their local application server even if the WAN links are down for 6 days, you need to increase the Expires After setting to 6 days on the Start of Authority (SOA) record for the zone. The Start of Authority (SOA) tab is the location on the Zone Properties dialog box where you can configure options or settings that are specific for the SOA resource record for the zone.

The Expires After field has a default setting of 24 hours. The value of this field determines the time duration after which a secondary DNS server that has no contact with its configured master server discards zone data. You can change this setting according to your requirements. In this scenario you can change it to 6 days so that DNS server that has no contact with its configured master server does not discard zone data till 6 days so that users in the branch offices can access their local application server.

The Zone Aging / Scavenging Properties need not be configured because they perform cleanup and removal of stale resource records (RRs), which can accumulate in zone data over time. With dynamic update, RRs are automatically added to zones when computers start on the network. However, in some cases, they are not automatically removed when computers leave the network. Thus they contain stale entries which may lead to wrong information.

Reference : Installing and Configuring DNS / Configuring DNS Zone Properties  
<http://www.tech-faq.com/installing-and-configuring-dns.shtml>

**QUESTION NO: 114**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest that contains two domains named us.CertKiller.com and uk.CertKiller.com.

All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista. You receive an instruction from the CIO to configure the user workstations in the us.CertKiller.com zone in order to improve the name resolution response time for resources at the

uk.CertKiller.com zone.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. You should consider creating and configuring a GPO with DNS Suffix Search List option to uk.CertKiller.com, us.CertKiller.com.
- B. You should consider configuring the priority value for the SRV records on all the domain controllers of us.CertKiller.com to 5.
- C. You should consider applying the policy to all user workstations in the us.CertKiller.com zone.
- D. You should consider creating and configuring a GPO with the Local-Link Multicast Name Resolution feature disabled.
- E. You should consider creating and configuring a GPO with the Local-Link Multicast Name Resolution feature enabled.

**Answer: A,C**

**Explanation:**

To configure the user workstations in the us.CertKiller.com zone to improve the name resolution response time for resources in the uk.CertKiller.com zone you need to configure a new GPO that configures the DNS Suffix Search List option to us.CertKiller.com, us.CertKiller.com. Thereafter the policy can be applied to all user workstations in the us.CertKiller.com zone.

A customized DNS suffix search lists to ensures that clients can locate services and other computers when they perform single-label name queries.

Link-Local Multicast Name Resolution cannot be used because it allows IPv6 hosts on a single subnet without a DNS server to resolve each other names. Therefore it need not be used here. DNS SRV records cannot be used because they are the service records, which are a type of DNS entry that specify information on a service available in a domain. They are typically used by clients who want to know the location of a service within a domain. When multiple hosts are configured for the same service, the priority determines which host is tried first.

Reference : Create a Disjoint Namespace / Update the DNS suffix search list

<http://technet2.microsoft.com/windowsserver2008/en/library/afe94bc3-41fb-4817-84b5-5517c38a0d391033.mspx?mfr=true>

Reference : Introducing MS Windows Vista / Learning about Dual Stack and IP Management Enhancements

[http://download.microsoft.com/download/5/7/8/578cbb95-c42e-4b9f-9989-93ffdeae8af4/Introducing\\_Windows\\_Vista.pdf](http://download.microsoft.com/download/5/7/8/578cbb95-c42e-4b9f-9989-93ffdeae8af4/Introducing_Windows_Vista.pdf)

Reference : Understanding DNS SRV records and SIP

<http://blog.lithiumblue.com/2007/07/understanding-dns-srv-records-and-sip.html>

**QUESTION NO: 115**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory forest that has a single active Directory domain named us.CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The corporate network contains a server named CERTKILLER-SR01. CERTKILLER-SR01 is configured to run the DNS server role. During routine monitoring you notice a number of stale records in the us.CertKiller.com zone. You then enable DNS scavenging on CERTKILLER-SR01 to remove the stale records.

Weeks after enabling DNS scavenging you discover that the same stale records still appear in the us.CertKiller.com zone. You receive an instruction from the CIO to remove those records from the us.CertKiller.com zone.

What should you do?

- A. You should consider running the `dnscmd CERTKILLER-SR01 /AgeAllRecords` command.
- B. You should consider running the `"dnscmd" CERTKILLER-SR01 /StartScavenging` command.
- C. You should consider stopping the DNS service on CERTKILLER-SR01 and then restart the DNS service again.
- D. You should consider enabling DNS scavenging on the us.CertKiller.com zone.
- E. You should consider running the `dnscmd ./zonerefresh` command.

**Answer: D**

**Explanation:**

You again noticed the same stale resource records still lay us.CertKiller.com even after enabled DNS scavenging on CERTKILLER-SR01 because the CERTKILLER-SR01 may not have us.CertKiller.com zone integrated with ADDS and loaded at the server.

To ensure that the stale resource records are removed from us.CertKiller.com, you need to enable DNS scavenging on the us.CertKiller.com zone. The aging and scavenging can be configured for specified zones on the DNS server to make sure that the stale records are removed from the specified zone.

Reference : Enable Aging and Scavenging for DNS

<http://technet2.microsoft.com/windowsserver2008/en/library/7972082c-22a1-44fc-8e39-841f7327b6051033.mspx?mfr=true>

**QUESTION NO: 116**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of two Active Directory domain named us.CertKiller.com and uk.tesCKin.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com users are able to connect to resources in each domain by specifying a Fully Qualified Domain Name (FQDN). CertKiller.com recently decided that users in the us.CertKiller.com domain should have the ability to connect to computers in uk.CertKiller.com by specifying the computers with a single name tag in a UNC path.

What should you do?

- A. You should do nothing as the DNS suffix of the other will automatically be appended to single-tag name queries.
- B. You should consider configuring the TCP/IP properties of the local are connection to use the connections DNS suffix in DNS registration on the clients in us.CertKiller.com.
- C. You should consider using Group Policy in us.CertKiller.com to configure the network clients with a DNS suffix search list.  
Thereafter the domain suffix uk.CertKiller.com should be added to the list.
- D. You should consider configuring the clients in us.CertKiller.com to forward queries for names in uk.CertKiller.com to the DNS servers in the uk.CertKiller.com domain using conditional forwarding.

**Answer: C**

**Explanation:**

You should use Group Policy to configure network clients with a DNS suffix search list and add the domain suffix uk.CertKiller.com to the list. This will allow the suffix to append to a DNS query which in turn will enable the user to submit a tag name query in a UNC path and will have the client automatically append the name.

**Incorrect Answers:**

- A: This option will not work. The client will append a single-tag name with the clients own domain name.
- B: This will only allow the client to ensure that its name is registered in the DNS not to connect to resources.
- D: Conditional forwarders will only allow the computer to resolve names in other domains. In the scenario that is already happening. However, this option will not allow clients to connect to resources, using a single-tag name.



**QUESTION NO: 117**

You are the newly appointed network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

During routine monitoring you discover that a client computer named CERTKILLER-WS04 failed to register its DNS record with the DNS server. You check and discover that CERTKILLER-WS04 is configured with a static IP address as well as with the address of the server authoritative for the CertKiller.com domain.

You receive information from the CIO stating that the TCP/IP properties on CERTKILLER-WS04 are left as default. You receive an instruction from the CIO to make sure that CERTKILLER-WS04 registers its own name with the DNS server.

What should you do?

- A. You should consider enabling the option to use the connections DNS suffix in DNS registration.
- B. You should consider configuring a primary DNS suffix.
- C. You should consider configuring a connection-specific suffix.
- D. You should consider enabling the option to register the connections addresses in DNS.
- E. You should consider configuring a DNS Suffix Search List option to CertKiller.com.

**Answer: B**

**Explanation:**

When you configure a primary DNS suffix, it will allow a DNS client to register its static address with the server.

**Incorrect Answers:**

- C: This action will register a connection-specific suffix, if the client is configured. However, if the settings are at default value for the non-DHCP client it will have no effect.
- D: This will not allow a computer to register with DNS even if the settings have its default values.

**QUESTION NO: 118**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as the corporate Virtual Private Network (VPN) server. CertKiller.com has remote users working outside the office who access and transmit sensitive information to CERTKILLER-SR01.

The CertKiller.com written security policy states that the user or computer accessing CERTKILLER-SR01 should make use of Public Key Infrastructure (PKI) to connect to the domain for transmission of the sensitive data. CertKiller.com wants you to ensure that CERTKILLER-SR01 is configured to comply with the security policy.

What should you do?

- A. You should consider having the `secedit/refreshpolicy machine_policy` command run from the command prompt.
- B. You should consider having L2TP/IPsec policy implemented to create certificate-based authentication.
- C. You should consider having the Kerberos version 5 authentication protocol used to create a custom IPsec policy.
- D. You should consider having the Pre-shared authentication used by creating a policy for a highly secure data transmission.
- E. You should consider using MS CHAP v2 authentication.

**Answer: B**

**Explanation:**

To secure the VPN connection, you don't have to create a custom IPsec policy when there is a much easier way.

The L2TP/IPsec ensures that the data is transmitted securely by implementing the Internet Protocol Security. The policy will create certificate-based authentication to identify the users.

**QUESTION NO: 119**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day you receive instruction from CertKiller.com to travel to the Toronto office and deploy a computer named CERTKILLER-SR21 which should remotely connect to a Windows Server 2008 core installation.

What should you do? (Choose two)

- A. You should consider having the `winrs -r <server core name> dir c:\Windows` command run on CERTKILLER-SR21.
- B. You should consider having the Server Manager run on CERTKILLER-SR21 and connect it to the Windows core installation server.

- C. You should consider having the SImgr.vbs -ato script run on the Windows core installation server.
- D. You should consider having the netsh and set port status command run on the Windows core installation server.
- E. You should consider configuring all remote connections to require Kerberos v5 authentication.
- F. You should consider having the netsh interface ipv4 set dnsserver command run on the remote server.

**Answer: A,D**

**Explanation:**

The netsh command allows you to configure the Windows core installation server to accept the remote connection and 'set port status' command allows you to designate a port for the remote connection. On the new server, you execute the windows remote service command and -r will specify the localhost or the NetBIOS name of the server. The server core name should be specified and then the location of the windows folder. The other two options are not useable because the Server manager on the new server will not allow remote connection and the SImgr.vbs -ato script is used to activate windows remotely. It can be used after you install the windows Server 2008 on the new server remotely.

**QUESTION NO: 120**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which is configured to provide Routing and Remote Access to the members of the KingRemote group. The current CertKiller.com written security allows the KingRemote group to dial-in to CERTKILLER-SR01. During the course of the day you receive instruction from CertKiller.com to increase remote access security by issuing smart cards to the KingRemote members. CertKiller.com wants you to configure CERTKILLER-SR01 and the Remote Access Policy to support smart card service for dial-up connections.

What should you do?

- A. You should consider having a remote access policy created which enables users to authenticate connection using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).
- B. You should consider having a remote access policy created which enables users to authenticate using Shiva Password Authentication Protocol (SPAP).

- C. You should consider a remote access policy that requires Kerberos v5 authentication.
- D. You should consider having CERTKILLER-SR01 installed and configured as a Network Policy Server.
- E. You should consider having a remote access policy created which enables users to authenticate using Microsoft Challenge Handshake Authentication Protocol, version 2 (MS-CHAPv2).

**Answer: A**

**Explanation:**

You should create a remote access policy that allows users to use Extensible Authentication Protocol Layer Security (EAP - TLS) because EAP-TLS requires a user certificate for the user requesting access and a computer certificate for the authenticating server. All other options like SPAP are not right because SPAP causes the remote access machine to send an encrypted password to the remote access server

**QUESTION NO: 121**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com has recently decided to deploy a computer named CERTKILLER-SR01 to the Miami office for providing remote access to external users from the Toronto office. During the course of the day whilst performing maintenance you discovered that a virus has infected several internal network clients. You have later determined that the virus is spread by a remote user accessing CERTKILLER-SR01. CertKiller.com wants you to ensure that the CertKiller.com corporate network is protected against viruses and malicious programs.

What should you do?

- A. You should consider having all remote users added in an organizational unit which would have antivirus software installed.
- B. You should consider having a network health policy created which requires anti-spyware to run on CERTKILLER-SR01 whilst ensuring the software automatically updates itself.
- C. You should consider having a network health policy created which requires anti-virus software running and updating itself frequently.
- D. You should consider having file-level anti-virus software installed on CERTKILLER-SR01 whilst configuring the software to update automatically.
- E. You should considering all users to make remote connections from a single client computer that has anti-virus software installed and Automatic Updates checked.

**Answer: C**

**Explanation:**

You need to configure a network health policy that requires anti-virus software to execute and check all the incoming files from the remote computer. In order to keep the anti-virus database up to date, you need to check the automatic updates option so you don't have to do the manual updates.

**QUESTION NO: 122**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista and Windows XP Professional (SP2). The CertKiller.com network currently has network computers at the office which are not part of the domain.

During the course of the day you receive instruction from CertKiller.com to have all client computers join the domain. CertKiller.com wants you to ensure that client's computers which are non-compliant are restricted from communicating on the network by having the client computers meet the system health requirements.

What should you do?

- A. You should consider having the Terminal Services licensing installed.
- B. You should consider having the Terminal Services gateway installed.
- C. You should consider having the Network policy and Access services installed.
- D. You should consider having all client computers running anti-virus software.
- E. You should consider having the Routing and Remote Access services installed.

**Answer: C**

**Explanation:**

The Network Access Protection (NAP) is a component of the Network policy and Access services that allow protecting network resources by enforcing compliance with system health requirements.

Reference: Security and Policy Enforcement

<http://www.microsoft.com/windowsserver2008/en/us/security-policy.aspx>

**QUESTION NO: 123**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com has recently decided to deploy a computer named CERTKILLER-SR01 to the Miami office for providing remote access to external users from the Toronto office. During the course of the day whilst performing maintenance you discovered that a virus has infected several internal network clients. You have later determined that the virus is spread by a remote user accessing CERTKILLER-SR01. CertKiller.com wants you to ensure that the CertKiller.com corporate network is protected against viruses and malicious programs.

What should you do?

- A. You should consider having a network health policy configured which will have the client computers required to have an anti-spy ware application whilst additionally ensuring the software is updated.
- B. You should consider having a new Organizational Unit (OU) created for remote users. You should then make use of a Group Policy Object (GPO) to have antivirus software deployed.
- C. You should consider having anti-virus software installed on CERTKILLER-SR01. You should then configure CERTKILLER-SR01 to have the anti-virus software automatically updated.
- D. You should consider having a network health policy configured which will have the client computers required to have anti-virus software installed and ensures the anti-virus application is up to date.
- E. You should consider having a network policy configured that run Automatic Updates of all new data that is downloaded.

**Answer: D**

**Explanation:**

:

To protect the network from virus infections transmitted via remote users, you need to configure a network health policy which enforces that anti-virus software is running and the anti-virus application is up to date. A network health policy can be configured by implementing NAP. Deploying anti-virus software on RRAS server will not ensure the implementation of NAP, which is important to ensure that the client computers on a private network meet administrator-defined requirements for system health. A network health policy which enforces that an anti-spy ware application is running and is up to date will not help because the anti-spyware software does not give protection from virus infections.

Reference : SolutionBase: Introducing Network Access Protection for Windows  
[http://techrepublic.com.com/2415-1035\\_11-177853.html](http://techrepublic.com.com/2415-1035_11-177853.html)

Reference : Network Access Protection

<http://technet2.microsoft.com/windowsserver2008/en/library/40dcd5ed-1cb9-4f29-8470-f6b4548c8e121033.msp?mfr=true>

### QUESTION NO: 124

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as a Network Address Translation (NAT) server. During the course of the day you receive instruction to deploy a computer named CERTKILLER-SR21 to the Toronto office.

CertKiller.com wants you to have port forwarding configured on CERTKILLER-SR01 to CERTKILLER-SR21 whilst ensuring network administrators are able to access CERTKILLER-SR21 using the Remote Desktop Protocol (RDP).

What should you do?

- A. You should consider having CERTKILLER-SR01 configured to forward port 3389 to CERTKILLER-SR01.
- B. You should consider having CERTKILLER-SR01 configured to forward port 25 to CERTKILLER-SR01.
- C. You should consider having CERTKILLER-SR01 configured with Conditional forwarding.
- D. You should consider having CERTKILLER-SR01 configured to forward port 1432 to CERTKILLER-SR01.
- E. You should consider having CERTKILLER-SR01 configured to forward port 389 to CERTKILLER-SR01.

**Answer: A**

**Explanation:**

:

To ensure that administrators can access the server, CERTKILLER-SR21 by using Remote Desktop Protocol (RDP), you need to configure the CERTKILLER-SR01 to forward port 3389 to CERTKILLER-SR21.

The Remote Desktop Protocol is designed to work across TCP port 3389.If you are attempting to



connect to a remote machine that sits behind a firewall, then the firewall must allow traffic to flow through TCP port 3389.

Reference : Troubleshooting Remote Desktop / The Remote Computer Cannot be Found

[http://www.windowsnetworkking.com/articles\\_tutorials/Troubleshooting-Remote-Desktop.html](http://www.windowsnetworkking.com/articles_tutorials/Troubleshooting-Remote-Desktop.html)

#### QUESTION NO: 125

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day you receive instruction from CertKiller.com to deploy a Virtual Private Network (VPN) server behind the existing firewall which is configured to allow secured Web communications only. CertKiller.com wants you to create a connection for the remote users to use when connecting to the corporate network securely as possible without configuring additional ports on the firewall.

What should you do?

- A. You should consider having an IPsec tunnel for remote users.
- B. You should consider having a PPTP VPN for remote users.
- C. You should consider having a L2TP VPN connection for remote users.
- D. You should consider having a SSTP VPN connection created for remote users.
- E. You should consider using half duplex tunneling over a secure SSL channel.

**Answer: D**

#### Explanation:

The question states that the firewall is configured to allow only secure web communications. Secure Web Communications use SSL. Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP traffic through an SSL channel.

#### QUESTION NO: 126

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. The CertKiller.com offices are connected via a Virtual Private Network (VPN) connection.

During the course of the day you receive instruction from CertKiller.com to ensure that the VPN connection uses end-to-end encryption when encrypting data transmitted between offices. CertKiller.com additionally wants you to ensure that computer-level authentication is used which do not have user named or passwords used for authentication.

What should you do?

- A. You should consider having a L2TP/IPsec connection used with EAP-TLS authentication.
- B. You should consider having a IPsec connection in tunnel mode with preshared key authentication.
- C. You should consider having a PPTP connection used with MS-CHAP v2 authentication.
- D. You should consider having a network policy stating Kerberos authentication to be used at all times.
- E. You should consider having a L2TP/IPsec connection used with MS-CHAP v2 authentication.

**Answer: A**

**Explanation:**

To ensure that the VPN connections between the main office and the branch offices meet the given requirements, you need to configure a L2TP/IPsec connection to use the EAP-TLS authentication.

L2TP leverages PPP user authentication and IPSec encryption to encapsulate and encrypt IP traffic. This combination, known as L2TP/IPSec, uses certificate-based computer identity authentication to create the IPSec session in addition to PPP-based user authentication.

Therefore it ensures that all data is encrypted by using end-to-end encryption and the VPN connection uses computer-level authentication. To ensure that User names and passwords cannot be used for authentication, you need to use EAP-TLS authentication.

With EAP-TLS, the VPN client sends its user certificate for authentication and the VPN server sends a computer certificate for authentication. This is the strongest authentication method as it does not rely on passwords.

Reference : Virtual Private Networking with Windows Server 2003: Deploying Remote Access VPNs / Layer Two Tunneling Protocol with IPSec/ Authentication Protocols  
<http://www.scribd.com/doc/2320023/DeployRasWithVPN>

**QUESTION NO: 127**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters

located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as the Routing and Remote Access server. During the course of the day CertKiller.com configured a Network Access Protection policy for the domain. CertKiller.com wants you to have Point-to-Point Protocol (PPP) authentication used on CERTKILLER-SR01.

What should you do?

- A. You should consider having the Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) authentication method used.
- B. You should consider having the Challenge Handshake Authentication Protocol (CHAP) authentication method used.
- C. You should consider having the Password Authentication Protocol (PAP) authentication method used.
- D. You should consider having the Extensible Authentication Protocol (EAP) authentication method used.
- E. You should consider having the Shiva Password Authentication Protocol (SPAP) authentication method used.

**Answer: D**

**Explanation:**

To configure the Point-to-Point Protocol (PPP) authentication method on CERTKILLER-SR01, you need to configure Extensible Authentication Protocol (EAP) authentication method.

Microsoft Windows uses EAP to authenticate network access for Point-to-Point Protocol (PPP) connections. EAP was designed as an extension to PPP to be able to use newer authentication methods such as one-time passwords, smart cards, or biometric techniques.

Reference : Making sense of remote access protocols in Windows / DIAL-UP AUTHENTICATION  
[http://articles.techrepublic.com.com/5100-10878\\_11-1058239.html](http://articles.techrepublic.com.com/5100-10878_11-1058239.html)

**QUESTION NO: 128**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. During the course of the day you receive instruction from

CertKiller.com to deploy a computer named CERTKILLER-SR01 to the Miami office as a Virtual Private Network (VPN) server by installing the required roles.

What should you do? (Choose two)

- A. You should consider having the Windows Deployment Services role installed.
- B. You should consider having the Host Credential Authorization Protocol role service installed.
- C. You should consider having the Routing and Remote Access Services role service installed.
- D. You should consider having the Deployment Server role service installed.
- E. You should consider having the Deployment Transport Role Service installed.
- F. You should consider having the Network Policy and Access Services role installed

**Answer: C,F**

**Explanation:**

To configure the server as a VPN server, you need to install Network Policy and Access Services role and Routing and Remote Access Services role service on the server. To install the Routing and Remote Access Services role service on the server, you need to first install the Network Policy and Access Services role on the server.

Reference : Configuring Windows Server 2008 as a Remote Access SSL VPN Server (Part 2) / Install the RRAS Server Role on the VPN Server

<http://www.windowsecurity.com/articles/Configuring-Windows-Server-2008-Remote-Access-SSL-VPN-Server-Part2.html>

**QUESTION NO: 129**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day you receive instruction from CertKiller.com to install a remote access server in the Miami office. TesKing.com currently has users working out of office with portable wireless computers which require access to resources in the Miami office. CertKiller.com wants you to have remote access configured to use the existing Active Directory credentials whilst minimizing costs.

What should you do? (Choose two)

- A. You should consider having a new server connected to the public Internet and configured as a RADIUS server.

You should then have the client computers configured to submit RADIUS authentication requests

to the server when connecting to remote networks.

B. You should consider having the remote access server connected to both the public Internet and the intranet which will be configured to accept incoming VPN connections.

C. You should consider having reaching an agreement with the ISP to provide dial-up access to remote users whilst configuring a new server as a RADIUS server.

You should then have the ISP configure the modem banks to submit authentication requests to the RADIUS server.

D. You should consider having a new server configured to accept dial-up connections and lease whilst additionally leasing a circuit from the telecommunications provider for PSTN connections.

You should then have management purchase a modem bank cable which accepts simultaneous connections and will be connected to the new configured server.

**Answer: B,C**

**Explanation:**

You can establish an agreement for the provision of integrated VPN connections which will be then authenticated to the internal RADIUS server. This will also allow for the clients that are using the public Internet for authentication and encryption.

**Incorrect Answers:**

A: You should not use this option. The clients do not directly submit to a RADIUS server.

Furthermore, the client computers will not be able to access the internal network without a VPN connection.

D: You can configure a Windows Server 2008 computer to accept dial-up connections and lease a circuit from the telecommunications provider for 30 PSTN connections. Furthermore you can also purchase a modem bank cable to accept 30 simultaneous connections which will be connected to the Windows Server 2008 computer. However this option will be cost-effective. Furthermore it will outsource the dial-up access to an ISP.

**QUESTION NO: 130**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. The CertKiller.com network users travel frequently from the office and required access to the Miami office when traveling.

During the course of the day you deploy a computer named CERTKILLER-SR01 as a Virtual Private Network (VPN) server and prepared the configuration. The remote users recently informed you that at times they are not able to access CERTKILLER-SR01. You investigated and discovered that the firewall is blocking PPTP and L2TP traffic. CertKiller.com wants you to ensure that the remote users use SSTP VPN connection by upgrading their operating systems to Windows that supports SSTP VPN connections.

What should you do?

- A. You should consider having the remote computers upgrade to Windows 2000 Professional
- B. You should consider having the remote computers upgrade to Windows XP Professional
- C. You should consider having the remote computers upgrade to Windows Vista with Service Pack 1 or Windows Server 2008.
- D. You should consider having the remote computers upgrade to Windows Millennium Edition.

**Answer: C**

**Explanation:**

Windows Vista with Service Pack 1 and Windows Server 2008 supports SSTP VPN connections.

**Incorrect Answers:**

D: Windows 2000 Professional, Windows Millennium Edition and Windows XP Professional do not support SSTP.

**QUESTION NO: 131**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which runs Windows Server 2008.

During the course of the day you receive instruction from CertKiller.com to configure a VPN which will be used by network users when out of office. CertKiller.com wants you to configure CERTKILLER-SR01 by determining which procedures should be followed before the configuration.

What should you do? (Choose two)

- A. You should consider having the SSTP protocols for the VPN configured.
- B. You should consider ensuring a clean installation of Microsoft Windows Server 2008 was installed.
- C. You should consider having the Drive option disabled in the RDP-Tcp Client Setting properties for CERTKILLER-SR01.
- D. You should consider having the Add Roles Wizard run in order to ensure that the RRAS role is installed.
- E. You should consider having an IPSec tunnel for VPN connections.

**Answer: B,D**

**Explanation:**

Your best option would be to enter the Add Roles Wizard and make sure that the RRAS role is installed as well as ensuring that the clean installation of Windows Server 2008 is installed. These

options are pre-requisites to setting up a VPN. When you have RRAS installed you will not be able to proceed with the VPN configuration.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

### QUESTION NO: 132

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which runs Windows Server 2008 and has the Terminal Services role installed.

During the course of the day you receive instruction from CertKiller.com to deploy a remote application named CKRemotes on CERTKILLER-SR01. The CertKiller.com security policy currently states that the network users should never be allowed to copy and paste information to a local computer during a Terminal Services session. CertKiller.com wants you to ensure that the requirements of the security policy are met.

What should you do?

- A. You should consider having the Use temporary folders per session option enabled.
- B. You should consider having the Security Encryption Level to FIPS Compliant changed.
- C. You should consider having the Drive option disabled in the RDP-Tcp Client Setting properties for the server.
- D. You should consider having the Clipboard option deselected in the RDP Settings for the published application.
- E. You should consider having the security layer for each server set to the RDP Security layer.

**Answer: D**

### Explanation:

To ensure that the users are not allowed to copy and paste information to a local computer during a Terminal Services session, you need to deselect the Clipboard option in the RDP Settings for the published application

When connecting to a terminal server using an RDP client, many of the local resources are available within the remote session, including the client file system, smart cards, audio (output), serial ports, printers (including network), and the clipboard. These redirection facilities allow users to easily take advantage of the capabilities of their client device from within the remote session. Similarly clipboard can be used to copy and paste information to local computer. To stop the copy paste, you need to go to Terminal Services Configuration and on the Client Settings tab, under Disable the following Clipboard mapping to disable client clipboard mapping.



Reference : Configure settings for mapping client devices/ Using Terminal Services Configuration  
<http://technet2.microsoft.com/windowsserver/en/library/17d44d9a-cf4b-4a6a-94ec-093cb5f8b2b71033.mspx?mfr=true>

Reference : Frequently Asked Windows Terminal Services Questions! / New Features and Improvements  
<http://www.msterialservices.org/faq/WindowsTerminalServices/?page=5>

### QUESTION NO: 133

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2003 and the client computers run Microsoft Windows Vista.

During the course of the day you receive instruction from CertKiller.com to migrate the network servers to Microsoft Windows Server 2008. You later received additional instruction to configure the RADIUS settings by making use of Internet Authorization Servers (IAS) for Windows Server 2003. CertKiller.com wants you to make use of the Network Policy Server (NPS) of Microsoft Windows Server 2008 by selecting the true statement.

Which of the statements below are true?

- A. You should be aware that the Connection Request Processing node will still exist in NPS.
- B. You should be aware that you would not be able to validate if user account dial-in properties.
- C. You should be aware that the Remote Access Logging folder would contain the Local file or the SQL Server nodes in Network Policy Servers (NPS).
- D. You should be aware that the Remote Access policies are replaced by the Network policies. You should additionally note that this has been moved to the Policies node.

**Answer: D**

#### **Explanation:**

The functionality is still the same as with IAS. Noticeable changes have however been made to the interface.

#### **Incorrect Answers:**

- A: The Remote Access Logging folder is replaced by the Accounting node. The Accounting node will no longer have the Local file or the SQL Server nodes.
- C: There will be no Connection Request Processing node.

### QUESTION NO: 134

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which runs Windows Server 2008 and has the Routing and Remote Access Service installed.

During the course of the day you receive instruction from CertKiller.com to configure CERTKILLER-SR01 as the Windows authentication provider whilst administering several Remote access policies for RRAS to CERTKILLER-SR01. CertKiller.com wants you to determine which of the connection settings would not be authenticated prior to authorization occurring by policies.

What should you do?

- A. You should be aware that you would be unable to validate remote access permissions.
- B. You should be aware that none of the options apply.
- C. You should be aware that you would not be able to validate if user account dial-in properties are ignored.
- D. You should be aware that you would be to validate advanced conditions like access server identity, access client phone number or MAC addresses.
- E. You should be aware that Network policies replaces Remote Access policies.

**Answer: B**

**Explanation:**

All the options are incorrect in this scenario.

You are able to validate the conditions prior to authorization occurring with the set policies. You are able to access the server identity access phone number or the MAC address with ease with Windows Server 2008.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 135**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of four servers named CERTKILLER-SR01, CERTKILLER-SR02, CERTKILLER-SR03 and CERTKILLER-SR04 configured as shown below:

CERTKILLER-SR01 is installed with the Terminal Services Gateway role service. CERTKILLER-SR02 is installed with the Terminal Services role and configured in a Load Balancing Terminal Server farm named CKFarms. CERTKILLER-SR03 is installed with the Terminal Services role and configured in a Load Balancing Terminal Server farm named CKFarms. CERTKILLER-SR04 is

configured with the Terminal Services (TS) Session Broker service.

During the course of the day you decided to deploy a hardware load balancing device specialized to support terminal services routing tokens to the Terminal Server farm to handle the load distribution.

You have later discovered that the TS Session Broker service started failing after the installation of the hardware device. CertKiller.com wants you to ensure that the TS Session Broker functions properly.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. You should consider having a GPO created which enables the Use IP Address Redirection policy setting in the Session Directory section of the Terminal Server Group Policy template.
- B. You should consider having a GPO created which disables the Use TS Session Broker Load Balancing policy setting in the Session Directory section of the Terminal Server Group Policy template.
- C. You should consider having a GPO created which enables the Use TS Session Broker Load Balancing policy setting in the Session Directory section of the Terminal Server Group Policy template.
- D. You should consider having a GPO created which disables the Use IP Address Redirection policy setting in the TS Session Broker section of the Terminal Server Group Policy template.
- E. You should then have the GPO applied to the domain.
- F. You should then have the GPO applied to the Terminal Server farm.

**Answer: D,F**

**Explanation:**

To ensure that the TS Session Broker works correctly in the above given scenario, you need to create a GPO that disables the Use IP Address Redirection policy setting in the TS Session Broker section of the Terminal Server Group Policy template.

The TS Session Broker service is failing because you have recently deployed a hardware load balancing device that has specialized support for terminal servers and routing tokens to the Terminal Server farm. When routing tokens are used the IP address of the terminal server is not sent to the client. Instead, the IP address is embedded in a token. This can happen when you disable Use IP Address Redirection policy setting.

When a client reconnects to the load balancer, the routing token is used to redirect the client to their existing session on the correct terminal server in the farm.

Reference: TS Session Broker

<http://technet2.microsoft.com/windowsserver2008/en/library/8a46c71e-cc7d-4bf0-82cc-8261f7c3069c1033.mspx?mfr=true>

**QUESTION NO: 136**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which runs Windows Server 2008 and has the Terminal Services Gateway (TS Gateway) role installed. CertKiller.com has several network users who leave the office who require access to the network desktop computers located at the office through CERTKILLER-SR01. During the course of the day you created a security group named KingSecurity to secure the network connection for the remote users. CertKiller.com wants you to enable the remote users to connect to CERTKILLER-SR01.

What should you do? (Choose all that apply)

- A. You should consider having the policy applied to CERTKILLER-SR01.
- B. You should consider having the KingSecurity security group added whilst having the Users enabled to connect to any resource.
- C. You should consider having the KingSecurity security group added to the local remote desktop users group on CERTKILLER-SR01
- D. You should consider having a client authorization policy created.
- E. You should consider having a resource authorization policy created.
- F. You should consider having the KingSecurity security group added whilst enabling Device redirection.

**Answer: D,F**

**Explanation:**

To enable the remote users belonging to KingSecurity to connect to the TS Gateway, you need to create a client authorization policy. Add the KingSecurity security group and enable Device redirection. A connection authorization policy (CAP) allows you to control who can connect to the Terminal Server through the Terminal Services Gateway.

The Device Redirection gives you the option of disabling redirection for trusted a remote client devices. The tab contains a series of checkboxes that you can use to disable things like disk drives, the Windows clipboard, printers, serial ports, and even plug and play devices.

Reference: Configuring the Windows Server 2008 Terminal Services Gateway (Part 2)/ Create a Terminal Services Gateway CAP

<http://www.windowsecurity.com/articles/Configuring-Windows-Server-2008-Terminal-Services-Gateway-Part2.html>

Reference: An Overview of Longhorn Server's Terminal Service Gateway (Part 4)

<http://www.msternalservices.org/articles/Overview-Longhorn-Servers-Terminal-Service-Gateway-Part4.html>

### QUESTION NO: 137

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows XP Professional SP2. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which has the Terminal Services role and Terminal Services Web Access role installed.

During the course of the day you decided to enable Network Level Authentication on CERTKILLER-SR01. You are aware that the Terminal Services Web Access role bakes use of Active Directory Domain Services (AD DS). CertKiller.com wants you to deploy an application named KingSales on CERTKILLER-SR01 whilst ensuring that the network users are able to launch KingSales from the Terminal Services Web Access Web page.

What should you do?

- A. You should consider having publishing to AD DS for the KingSales application disabled.
- B. You should consider having the Remote Desktop Client 6.1 application installed on the client computers.
- C. You should consider having a Microsoft Windows Installer package of the KingSales application published on CERTKILLER-SR01 and distribute the Windows Installer package to the users.
- D. You should consider having a Install the Terminal Services Gateway (TS Gateway) role installed on CERTKILLER-SR01 and reconfigure the remote application publishing for the KingSales application to reflect the change.
- E. You should consider having the firewall on each server configured to block certain ports.

**Answer: B**

### Explanation:

To ensure that the users can launch KingSales on CERTKILLER-SR01 from the Terminal Services Web Access Web page, you need to install the Remote Desktop Client 6.1 application on the client computers, which eases the deployment of Windows Server 2008 Terminal services on the client computers that run Windows XP Service Pack 2.

Because the Remote Desktop Client 6.1 application supports Terminal Services Web Access, the Windows XP users can launch KingSales on CERTKILLER-SR01 from their Terminal Services Web Access Web page.

Reference: Download Microsoft Remote Desktop Connection (Terminal Services Client 6.1) for

Windows XP SP2

<http://www.dabcc.com/article.aspx?id=8044>

### QUESTION NO: 138

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which has the Terminal Services role installed. During the course of the day you receive instruction from CertKiller.com to deploy an application named KingSales by making use of the Terminal Services RemoteApp Manager. You later set the Terminal Servers security layer to negotiate. CertKiller.com wants you to ensure that the domain users are not prompted for credentials when accessing the application.

What should you do?

- A. You should consider having the Credential Delegation settings modified in the local Group Policy on CERTKILLER-SR01.
- B. You should consider having the Password Policy settings modified in the local Group Policy on CERTKILLER-SR01.
- C. You should consider having the Password Policy settings modified in the local Group Policy on all the client computers.
- D. You should consider having the Credential Delegation settings modified in the local Group Policy on all client computers.
- E. You should consider having the network policies replaced by Remote Access policies on CERTKILLER-SR01.

**Answer: D**

### Explanation:

To ensure that domain users are not prompted for credentials when they access the application, you need to modify the Credential Delegation settings in the local Group Policy on all client computers.

Windows Vista introduces a new authentication package called the Credential Security Service Provider, or CredSSP, that provides a single sign-on (SSO) user experience when starting new Terminal Services sessions. CredSSP enables applications to delegate users' credentials from the client computer (by using the client-side security service provider) to the target server (through the server-side security service provider) based on client policies. CredSSP policies are configured via Group Policy, and delegation of credentials is turned off by default



In addition, a few of the policy settings might increase or decrease the risk. For example, the Allow Default Credentials with NTLM-only Server Authentication and Allow Fresh Credentials with NTLM-only Server Authentication policy settings remove the restriction to require the Kerberos authentication protocol for authentication between the client and server.

Reference: Credential Security Service Provider and SSO for Terminal Services Logon  
<http://technet2.microsoft.com/WindowsVista/en/library/6b6bf605-0b9f-45ed-9900-12aca2a0f2a21033.mspx?mfr=true>

### QUESTION NO: 139

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which runs the Terminal Services role for the required applications the network user's access from their terminals.

During the course of the day you receive instruction from CertKiller.com to deploy an application named KingSales on CERTKILLER-SR01. You have verified that the application can be deployed in a Terminal Services environment. CertKiller.com has informed you that the features of the KingSales application does not use Windows Installer Packages for installation and the application makes changes in the registry of the current user. CertKiller.com wants you to select the proper installation of the application to support multiple user sessions.

What should you do? (Choose all that apply.)

- A. You should consider having the change logon /disable command run on CERTKILLER-SR01.
- B. You should consider having the change logon /enable command run on CERTKILLER-SR01.
- C. You should consider having the mstsc /v: CERTKILLER-SR01/console command run from the client computer to log on to CERTKILLER-SR01.
- D. You should consider having the change user /install command run on CERTKILLER-SR01.
- E. You should consider having the application installed.
- F. You should consider having the change user /execute command run on CERTKILLER-SR01.

**Answer: D,E,F**

### Explanation:

To install the application to support multiple user sessions in the above scenario, you need to first run the change user /install command on CERTKILLER-SR01 because You must put a Terminal Services server in Install mode to install or remove programs on the server. You can put a Terminal Services server in Install mode either by using the Add/Remove



Programs tool in Control Panel to add or remove a program, or by using the change user command at a command prompt. You need to then install the application.

When you are finished installing the program, you need to return the Terminal Services server to Execute mode, to execute the application. Therefore, to return to the Execute mode, you need to run the change user /execute command on CERTKILLER-SR01 .

Reference : HOW TO: Use the CHANGE USER Command to Switch to Install Mode in Windows 2000 Terminal Services

<http://support.microsoft.com/kb/320185>

### QUESTION NO: 140

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which runs the Terminal Services role for the required applications the network user's access from their terminals. During the course of the day you receive instruction from CertKiller.com to prevent new sessions on CERTKILLER-SR01 whilst not affecting current user sessions.

What should you do?

- A. You should consider having the Change user /execute disable command run.
- B. You should consider having the Change logon /disable command run.
- C. You should consider having the Tskill /server:CERTKILLER-SR01/A command run.
- D. You should consider having the Taskkill /S CERTKILLER-SR01 /fi "MODULES eq TermSrv" command run.
- E. You should consider accessing the TaskManager and manually terminate all new sessions on CERTKILLER-SR01.

**Answer: B**

### Explanation:

To prevent new sessions on the Terminal Server without affecting current user sessions, you need to run Change logon /disable command. This command disables subsequent logons from client sessions, but not from the console. This also ensures that the currently logged on users do not get affected.

Reference: Change logon

<http://technet2.microsoft.com/windowsserver/en/library/85af3fd0-b518-4b91-9f93->

24c75173494e1033.mspx?mfr=true

**QUESTION NO: 141**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com network makes use of Terminal services that resides on a server named CERTKILLER-TS12. These services allow the remote users of CertKiller.com to use their specific applications from their workstation.

However, a CertKiller.com user named Mia Hamm has contacted you for help to run one of the applications that resides on CERTKILLER-TS12. You decide to log onto CERTKILLER-TS12 and discover that you are unable to run any applications. You receive an instruction from the CIO to ensure that Mia Hamm is able to operate applications on CERTKILLER-TS12.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. You should make use of the default settings of the Use remote control.
- B. You should enable the Use remote control with the following settings option in the RDP-TCP properties on CERTKILLER-TS12. Then the Level of control policy setting should be configured to Interact with the session.
- C. You should thereafter inform Mia Hamm to log off and back on again.
- D. You should run the Tscon /v command on CERTKILLER-TS12.
- E. You should thereafter reconnect to the session.
- F. You should run the Chgusr /execute command on CERTKILLER-TS12.

**Answer: B,C**

**Explanation:**

To assist Mia Hamm, you should enable the Use remote control with the following settings option and then configure the Level of control policy setting to Interact with the session. You should also instruct her to log off and log back on. When you use this setting, you can also control the user's session with your keyboard and mouse.

Reference : Need to monitor a terminal services session? Use Shadow. / How to Configure Remote Control Settings

<http://www.myitforum.com/articles/16/view.asp?id=5808>

**QUESTION NO: 142**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are responsible for a Windows Server 2008 server named CERTKILLER-TS13. CERTKILLER-TS13 contains the Terminal Services Gateway (TS Gateway) role. You receive an instruction from the CIO to ensure that the security group named Test\_Secure has access to CERTKILLER-TS13.

What should you do?

- A. This can be accomplished by adding Test\_Secure to the TS Web Access Computers group.
- B. This can be accomplished by adding Test\_Secure to the Remote Desktop Users group.
- C. This can be accomplished by ensuring that Test\_Secure is able to access CERTKILLER-TS13 via the TS Gateway by means of a Connection Authorization Policy.
- D. This can be accomplished by ensuring that Test\_Secure is able to access CERTKILLER-TS13 via the IP Gateway by means of a Resource Authorization Policy.

**Answer: C**

**Explanation:**

In order to provide Test\_Secure access to the TS Gateway server, you need to create and configure a Connection Authorization Policy. The connection authorization policy (CAP) will permit you to control who can connect to the Terminal Server via the Terminal Services Gateway. You are also able to configure which groups are able to access the Terminal Server through the TS Gateway.

Reference: Configuring the Windows Server 2008 Terminal Services Gateway (Part 2) / Create a Terminal Services Gateway CAP

<http://www.windowsecurity.com/articles/Configuring-Windows-Server-2008-Terminal-Services-Gateway-Part2.html>

**QUESTION NO: 143**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. The CertKiller.com network makes use of Terminal services that resides on a server named CERTKILLER-TS14.

These services allow the remote users of CertKiller.com to use their specific applications from their workstation. You have received word that an application on the terminal service named CK\_ACC does not respond. During the investigation, you monitor CK\_ACC and detect that it

contains a memory leak. To address the problem, you create a new resource-allocation policy configured a Process Matching Criteria named TrackMem for the application in Microsoft Windows Server Resource Manager. To ensure productivity you need to set CK\_ACC on CERTKILLER-TS14 to end the application when more than half of the available memory is in use.

What should you do? (Choose all that apply.)

- A. The best option is to set up the resource-allocation policy.
- B. Set the maximum committed memory option to half the available memory on CERTKILLER-TS14.
- C. Set the maximum working set limit option to half the available memory on CERTKILLER-TS14.
- D. You should set the new policy as a Managing Policy.
- E. You should set the new policy as a Profiling Policy.

**Answer: A,B,D**

**Explanation:**

To terminate the application when the application consumes more than half of the available memory on CERTKILLER-TS14, you need to configure the resource-allocation policy and set the maximum committed memory option to half the available memory on the server and then set the new policy as a Managing Policy.

A memory limit should be set when an application is leaking memory from the Memory tab. Select the Use Maximum Committed Memory For Each Process check box. In Maximum Committed Memory Limit Per Process, you can type a value in megabytes. The Maximum Committed Memory Limit Per Process field allows you to limit the memory on per process basis.

Now you're ready to set the new resource allocation policy to manage the computer. In the console tree, click Resource Allocation Policies. In the details pane, right-click the resource allocation policy you want to set, and then click Set As Managing Policy. This is because this policy is for computer management and not for profile management.

Reference: Use Windows System Resource Manager to control a server's powers  
[http://articles.techrepublic.com.com/5100-10878\\_11-5054954.html](http://articles.techrepublic.com.com/5100-10878_11-5054954.html)

**QUESTION NO: 144**

You are the newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. The CertKiller.com network makes use of Terminal services that is located on a server named CERTKILLER-TS16.

These services allow the remote users of CertKiller.com to use their specific applications from their workstation. TesCKng.com contains two organizational units (OU's) named CK\_Users and CK\_Admin. CK\_Users is used for users that connect to CERTKILLER-TS16. CK\_Admin is used by the administrative body that connects to CERTKILLER-TS16.

A CertKiller.com policy states that only CK\_Users and CK\_Admin are allowed access to CERTKILLER-TS16. You have received instructions from management to only permit users in CK\_Admin to run the Remote Desktop Protocol files.

What should you do? (Each correct answer presents part of the solution. Choose THREE.)

- A. You should enable the Allow rdp files from the valid publishers and users' default .rdp settings policy setting.
- B. You should enable the Allow .rdp files from valid publishers and users default .rdp settings policy setting.
- C. You should disable the Allow .rdp files from unknown publisher's policy setting.
- D. You should apply the GPO to CK\_Users.
- E. You should enable the Specify SHA1 thumbprints of certificates representing trusted .rdp publisher's policy setting.
- F. You should apply the GPO to CK\_Admin.
- G. You should consider creating a group policy object (GPO).

**Answer: B,D,G**

**Explanation:**

To ensure that only members of CK\_Admin can run the Remote Desktop Protocol files, you need to enable the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template.

This policy setting allows you to specify whether users can run Remote Desktop Protocol (.rdp) files from a publisher that signed the file with a valid certificate. A valid certificate is one issued by an authority recognized by the client, such as the issuers in the client's Third-Party Root Certification Authorities certificate store. This policy setting also controls whether the user can start an RDP session by using default .rdp settings (for example, when a user directly opens the Remote Desktop Connection [RDC] client without specifying an .rdp file).

If you enable this policy setting, users can run .rdp files that are signed with a valid certificate. Users can also start an RDP session with default .rdp settings by directly opening the RDC client. When a user starts an RDP session, the user is asked to confirm whether they want to connect.

If you disable this policy setting, users cannot run .rdp files that are signed with a valid certificate. Additionally, users cannot start an RDP session by directly opening the RDC client and specifying the remote computer name. When a user tries to start an RDP session, the user receives a

message that the publisher has been blocked

Reference: Remote Desktop Connection Client

<http://technet2.microsoft.com/windowsserver2008/en/library/76fb7e12-b823-429b-9887-05dc70d28d0c1033.mspx?mfr=true>

### QUESTION NO: 145

You are the newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its head quarters in Milan and branch offices around the region. All servers on the CertKiller.com network run Windows Server 2008.

The branch offices at CertKiller.com make use of VPN connections to connect to the Milan office. You have received instructions from management to prohibit the users to connect to the VPN server remotely from 18:00 to 07:00.

What should you do?

- A. This can be accomplished by creating a network policy for VPN connections. Thereafter the Day and time restrictions can be configured as desired.
- B. This can be accomplished by enabling the Force logoff when logon hours expire option in order to configure the Logon Hours for the default domain policy.
- C. This can be accomplished by creating a Default Domain policy for the VPN connections, Thereafter an IP filter to deny access to the CertKiller.com network can be applied.
- D. This can be accomplished by specifying the VPN server on the Computer restrictions option in the Network policy to configure the Logon hours for all user objects.

**Answer: A**

### Explanation:

To ensure that users cannot access the VPN server remotely from 18:00 to 07:00, you need to create a network policy for VPN connections and then modify the Day and time restrictions. The network policy provides a policy conditions called "Allow full network access for a limited time", which allow clients to temporarily access full network. However, the NAP enforcement is delayed until the specified date and time.

Reference : Step By Step Guide: Demonstrate VPN NAP Enforcement in a Test Lab / NAP enforcement and network restriction

<http://www.microsoft.com/downloads/details.aspx?FamilyID=729bba00-55ad-4199-b441-378cc3d900a7&displaylang=en>

**QUESTION NO: 146**

You are an enterprise administrator for CertKiller.com. The company runs Windows Server 2008 on all the servers on the network.

You are responsible for evaluating remote access technologies. Determine the statements that are true regarding the comparison of a dial-up connection to that of a VPN connection. What should you identify? (Choose two.)

- A. A dial-up connection as well as a VPN connection can authenticate to the same RADIUS server. The RADIUS server can be hosted on a Windows Server 2008 computer.
- B. A VPN connection offers you a better performance than the dial-up connections. Whereas dial-up connections are adequate for common tasks, including e-mail and streaming video.
- C. A VPN connection needs an existing Internet connection and a dial-up connection can completely bypass the Internet.
- D. Information sent across a VPN connection can be intercepted and interpreted by an attacker that may have access to the infrastructure of the ISP. Dial-up connections offer a higher level of security by using PSTN.

**Answer: A,C**

**Explanation:**

VPN servers as well as dial-up servers are able to authenticate to a central RADIUS server. Dial-up connections are able to connect to a server directly on the companies' intranet by bypassing the Internet completely.

Virtual Private Network connections will offer you better performance than dial-up connections. Dial-up connections are not adequate for streaming a video.

Virtual Private Networks encompasses encryption. It stops an attacker with access to the transmission from interpreting the information.

Reference : Syngress - The Real MCTS-MCITP 70-649 Prep Kit - Independent and Complete Self-Paced Solutions

Part 2, Configure Network Access Protection (NAP) (24 Questions)

**QUESTION NO: 147**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters



located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which has Network Access Protection configured at the Miami office. The CertKiller.com written security policy currently states that data transmitted between CERTKILLER-SR01 and client computers should be secure. The Toronto office users connect to the Miami office using portable computers. During the course of the day you receive instruction from CertKiller.com to create a access requirement for preventing other non network users from connecting to CERTKILLER-SR01.

What should you do?

- A. You should consider having a Wired Network Group policy with all computers using MS-CHAP authentication, added and configured
- B. You should consider having an Extensible Authentication Protocol (EAP) Enforcement Network policy added and configured. Further ensure that EAP-TLS authentication is used.
- C. You should consider having an IPsec Enforcement Network policy added and configured.
- D. You should consider having an 802.1X Enforcement Network policy added and configured.
- E. You should consider having a network policy that restricts all remote connections.

**Answer: C**

**Explanation:**

To implement the restricted access control, you should choose option C. You need to configure an IPsec Enforcement Network Policy. The Internet Protocol Security will authenticate the IPs of authenticated users through its security. All you have to do is create an enforcement network policy that uses IPsec.

The option D is a wireless enforcement network policy. So you could not use it in this scenario.

The other options like option A are out of the context. You cannot use Wired Network Group policy for security and restricted access. It is just a group policy for wired network.

**QUESTION NO: 148**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as the NAP server using default settings. CertKiller.com currently makes use of a network application

which accesses a remote database. During the course of the day you tried deploying the application to the Toronto office but the application fails to run on the client computers. You have later discovered that the client computers using anti-virus software which causes the problems. You later attempt disabling the anti-virus software and the application still fails. CertKiller.com wants you to ensure that the application can be used on the client computers.

What should you do?

A. You should consider having the Windows Defender service on client's computer configured to a manual startup.

You should then have the Windows Defender service disabled and enable.

B. You should consider having the system health agent failure option configured through Error code resolution to healthy.

C. You should consider having the anti-spyware setting "up to date" on the Windows Security Health Validator window unchecked.

D. You should consider having the Anti-spyware setting "Application is on" on the Windows Security Health Validator window unchecked.

E. You should consider having MS-CHAP v2 authentication used on all the client computers.

**Answer: D**

**Explanation:**

To ensure that the application works normally on every client computer, you should choose the option B. You have to turn the anti-spyware settings "application is on" off on the Windows Security Health Validator window. The Windows Security Health Validator keeps all the important application on to ensure that the critical applications are working. Since the Anti-spyware is not compatible with the application you are installing on client computers, you should turn it off in the Windows Security Health Validator Window.

You should not choose option A because it will update the anti-spyware software. Similarly, the Windows Defender Service is also not an option for this scenario because it will not hinder with the new application and there is no use starting it manually and disabling it.

**QUESTION NO: 149**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which has Network Access Protection (NAP) and Active Directory Certificate Services (AD CS) installed.

During the course of the day you receive instruction from CertKiller.com to have the newly acquired portable computers connected to the wireless network and join the domain.

CertKiller.com has additionally informed you that the portable computers make use of PEAP-MS-CHAP V2 for authentication. CertKiller.com wants you to ensure that the portable computers are able to join the domain when restarted.

What should you do?

- A. You should consider having a group policy configured with the use of Windows WLAN Auto Config service for clients policy setting enabled.
- B. You should consider having a group policy configured with the use of Windows WLAN Auto Config service for clients policy setting disabled.
- C. You should consider having the netsh wlan export profile command run on all portable computers.
- D. You should consider having each portable computer configure with a Bootstrap wireless profile.
- E. You should consider having each portable computer join the domain via a browser.

**Answer: D**

**Explanation:**

:

To ensure that the Wireless client laptops running Windows Vista using PEAP-MS-CHAP V2 for authentication can join the AD domain when users restart them, you need to configure each laptop computer with a Bootstrap wireless profile, which is a temporary wireless profile that can be used to obtain connectivity to a secure wireless network. Once connected to the wireless network, the wireless client user can join the computer to the domain after providing security credentials for authentication by a RADIUS server.

These credentials may include a username and password (for Protected EAP [PEAP]-Microsoft Challenge Handshake Authentication Protocol version 2 [MS-CHAP v2]) or certificates (for EAP-TLS).

Reference Joining a Windows Vista Wireless Client to a Domain

[http://technet.microsoft.com/hi-in/library/bb727033\(en-us\).aspx](http://technet.microsoft.com/hi-in/library/bb727033(en-us).aspx)

## QUESTION NO: 150

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured as the

NAP server using default settings. CertKiller.com currently makes use of a network application which accesses a remote database located at the back-end.

During the course of the day you tried deploying the application to the Toronto office but the application fails to run on the client computers. You have later discovered that the client computers using anti-virus software which causes the problems. You later attempt disabling the anti-virus software and the application still fails. CertKiller.com wants you to ensure that the application can be used on the client computers.

What should you do?

- A. You should consider having the Error code resolution setting for the System Health agent failure option configured to Healthy.
- B. You should consider having the An anti-spyware application is on setting disabled on the Windows Security Health Validator dialog box.
- C. You should consider having a group policy for client computers configured with the use of Windows WLAN Auto Config service for clients policy setting enabled.
- D. You should consider having the Anti-spyware is up to date setting disabled on the Windows Security Health Validator dialog box.

**Answer: B**

**Explanation:**

The application failed even after disabling the anti-spyware on the client computers because the client computers are supposed to be using an anti-spyware application according to Windows Security Health Validator (SHV) policy that is configured on the client computers through NAP. To resolve the problem, you need to disable the anti-spyware application is on setting on the Windows Security Health Validator dialog box

Disabling the Anti-spyware is up to date setting on the Windows Security Health Validator dialog box will not help if anti-spyware application is on setting on because the Anti-spyware is up to date setting will not ensure that the client is not using an anti-spyware application. Configuring the Windows Defender service or configuring the Error code resolution setting for the System Health agent failure option will not help because neither Windows defender nor System Health agent is creating problem in his case.

Reference : An Introduction to Network Access Protection (Part 4)

[http://www.windowsnetworkKing.com/articles\\_tutorials/Introduction-Network-Access-Protection-Part4.html](http://www.windowsnetworkKing.com/articles_tutorials/Introduction-Network-Access-Protection-Part4.html)

**QUESTION NO: 151**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently makes use of a computer named CERTKILLER-SR01 which has Active Directory Certificate Services (AD CS) and Network Access Protection (NAP) installed. CertKiller.com currently has Toronto office users connecting to the Miami office using wireless computers. During the course of the day you receive instruction from CertKiller.com to configure NAP policies whilst ensuring that the created policy is enforced on wireless connections accessing the Miami office.

What should you do?

- A. You should consider having 802.1X authentication used on all access points.
- B. You should consider having the Prevent connections to infrastructure networks option enabled in the wireless Group Policy settings in the Network Policies.
- C. You should consider having MS-CHAP v2 authentication required on all portable computers.
- D. You should consider having the Prevent connections to infrastructure networks option disabled in the wireless Group Policy settings in the Group Policy Management Console.
- E. You should consider disabling then re-enabling the Prevent Connections to infrastructure networks option in the wireless Group Policy settings in the Network Policies.

**Answer: A**

**Explanation:**

To ensure that NAP policies are enforced on portable computers that use a wireless connection to access the network, you need to configure all access points to use 802.1X authentication.

802.1X enforcement enforces health policy requirements every time a computer attempts an 802.1X-authenticated network connection. 802.1X enforcement also actively monitors the health status of the connected NAP client and applies the restricted access profile to the connection if the client becomes noncompliant.

Reference : Microsoft Improves Security Policy Compliance with Network Access Protection  
<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000983>

**QUESTION NO: 152**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run

Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured with Network Access Protection (NAP).

CertKiller.com currently has Toronto office client computers who remote connect to the Miami office. During the course of the day you receive instruction from CertKiller.com to ensure that data transmission between the Toronto office remote connections and the Miami office are secure as possible.

What should you do?

- A. You should consider having DHCP clients restricted by using NAP in the wireless Group Policy settings.
- B. You should consider having an IPsec NAP policy applied in the Group Policy Management Console.
- C. You should consider having SPAP authentication used for all VPN connections.
- D. You should consider having a NAP policy configured for 802.1x wireless connections.

**Answer: D**

**Explanation:**

To ensure that NAP policies are enforced on portable computers that use a wireless connection to access the network, you need to configure all access points to use 802.1X authentication.

802.1X enforcement enforces health policy requirements every time a computer attempts an 802.1X-authenticated network connection. 802.1X enforcement also actively monitors the health status of the connected NAP client and applies the restricted access profile to the connection if the client becomes noncompliant.

Reference : Microsoft Improves Security Policy Compliance with Network Access Protection  
<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000983>

**QUESTION NO: 153**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto.

The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com currently makes use of a computer named CERTKILLER-SR01 configured with the Network Policy Server (NPS) service role. During the course of the day you receive instruction from CertKiller.com to ensure that you allow VPN access



to members of a global group named CKRemote exclusively.

What should you do?

- A. You should consider having CKRemote added to the RAS and IAS Servers group in the Default Domain Policy.
- B. You should consider having CKRemote added to the Network Configuration Operators group in the Default Domain Policy.
- C. You should consider having a new network policy created with a group-based condition for CKRemote.

You should then have the access permission set to Access Granted, and the processing order of the policy set to 1.

- D. You should consider having a new network policy created with a group-based condition for CKRemote.

You should then have the access permission set to Access Granted, and the processing order of the policy set to 3.

**Answer: C**

**Explanation:**

To allow access to only the members of CKRemote VPN to the network, you need to create a new network policy and define a group-based condition for CKRemote then set the access permission of the policy to Access Granted and set the processing order of the policy to 1.

You can create different compliance standards for users based on role, department, geography, and so on and then create network policies based on them. For the same reason you can create a policy of CertKillerStaff VPN group and set the processing order of the policy to one. This is because the policies are evaluated from top to bottom and processing stops once a policy rule is matched. First is the Com-pliant FullAccess policy which states that machines that pass all SHV checks are granted unrestricted network access should be listed. Having this policy listed first reduces processing load and time on the NPS.

The next policy used should be for Non-com-pliant or Restricted machines and the third policy is for backward compatibility of computers.

Reference: Security Watch Network Access Protection / Contoso NAP Deployment  
<http://technet.microsoft.com/en-us/magazine/cc162368.aspx>

**QUESTION NO: 154**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters



located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista. CertKiller.com has recently decided to configure Network Access Protection (NAP) configured at the Miami office.

During the course of the day you receive instruction from CertKiller.com to configure 802.1 x authentications to all access points which will be used to access the Miami office by wireless client computers. CertKiller.com wants you to ensure that the client computers are evaluated by NAP before given access to the Miami office network.

What should you do?

- A. You should consider having a Wireless Network Policy configured having the Remote Access Server as the only available authentication method.
- B. You should consider having all access points configured as RADIUS clients to the Network Policy Server (NPS) in the wireless group policy setting.
- C. You should consider having a Connection Request Policy configured having EAP-TLS as the only available authentication method.
- D. You should consider having all access points configured as RADIUS clients to the Remediation Servers.

**Answer: C**

**Explanation:**

To ensure that all the client computers that try to access the corporate network are evaluated by NAP, you need to create a Connection Request Policy that specifies EAP-TLS as the only available authentication method.

By default, Windows Server2008 supports the EAP methods: PEAP-MS-CHAPv2, EAP with Transport Layer Security (TLS) or EAP-TLS, and PEAP-TLS.

The connection request policy can impose connection requirements. For example, for 802.1X and VPN enforcement, the connection request policy requires the use of a Protected Extensible Authentication Protocol (PEAP)-based authentication method. If the connecting client does not use PEAP, the connection request is rejected.

Reference: The Cable Guy Troubleshooting NAP Enforcement / Health Requirement Policies  
<http://technet.microsoft.com/en-us/magazine/cc434701.aspx>

Reference: What Works Differently / 802.1X Authenticated Wired and Wireless Access  
<http://technet2.microsoft.com/windowsserver2008/en/library/ec5b5e7b-5d5c-4d04-98ad-55d9a09677101033.mspx?mfr=true>

**QUESTION NO: 155**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com and an Enterprise Root Certificate authority. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day you receive instruction to use Network Access Protection (NAP) on a computer named CERTKILLER-SR01. CertKiller.com has additionally deployed two computers named CERTKILLER-SR02 and CERTKILLER-SR03 configured as shown in the table below:

CertKiller.com wants you to ensure that a system health policy is implemented on all client computers attempting to access CERTKILLER-SR03 through a secure SSL tunnel or VPN connections.

What should you do?

- A. You should consider having a NAP role configured and added to a server that serves as a domain controller.
- B. You should consider having CERTKILLER-SR03 reconfigured as a Radius client.
- C. You should consider having a NAP role added on the Enterprise Certificate Server on a separate server in the domain.
- D. You should consider having CERTKILLER-SR02 reconfigured as a Radius Client.

**Answer: B**

**Explanation:**

To ensure that the system health policy is implemented on all client computers that attempt a VPN connection, you should reconfigure CERTKILLER-SR03 as a Radius client. The CERTKILLER-SR03 will authenticate and authorize the client VPN connections and won't allow those clients who don't have a system health policy added on their machines.

**QUESTION NO: 156**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com network users currently travel between office and require access to the corporate

network. CertKiller.com has recently decided to have the traveling users divided into two global groups named CKTravel1 and CKTravel2. During the course of the day you receive instruction from CertKiller.com to install the Network Policy Server (NPS) service role on a computer named CERTKILLER-SR01. CertKiller.com wants you to ensure that CKTravel1 global group is allowed VPN access to the corporate network.

What should you do?

A. You should consider having a new network policy created with a group-based condition for CKTravel1 in the Default Domain Policy.

You should then have the access permission of the policy set to Access granted and the processing order of the policy set to 3.

B. You should consider having a new network policy created with a group-based condition for CKTravel1.

You should then have the access permission of the policy set to Access granted and the processing order of the policy set to 1.

C. You should consider having CKTravel1 global group added to the RAS and IAS Servers group in the Network Policies.

D. You should consider having CKTravel1 global group added to the Network Configuration Operators group.

**Answer: B**

**Explanation:**

:

Network Policy Server (NPS) in Windows Server 2008 allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

To allow only members of a global group named CKTravel1 VPN access to the network, you need to create a new network policy and define a group-based condition for CKTravel1. Set the access permission of the policy to Access granted. Set the processing order of the policy to 1

Processing order specifies the numeric position of this policy in the list of policies configured on the NPS. Policies highest in the list (for example, at first position) are processed by NPS first. Policies added at positions above other policies cause the positions of the other policies to drop in the list by one position. If processing order is not specified, the policy is added at the end of the list.

Reference : Connection Request Policy Commands

<http://technet2.microsoft.com/windowsserver2008/en/library/c504902c-9765-4c26-9306-fca4a14f7fba1033.msp?mfr=true>

Reference : Configuring Exemption Policies for Configuration Manager Network Access Protection

<http://technet.microsoft.com/en-us/library/bb693983.aspx>

### QUESTION NO: 157

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

The CertKiller.com Miami office currently makes use of Network Access Protection (NAP) for enforcing policies on client computers connecting to the office. The CertKiller.com written security policy states that the client computers which have updates labeled Important and Critical installed should be able to access network resources. You have later configured a group policy to configure the client computers to obtain updates from a WSUS server. CertKiller.com wants you to ensure that the client computers comply with the security policy.

What should you do?

- A. You should consider having automatic updates enabled on each client.
- B. You should consider having the clients quarantined which do not have all available security updates installed.
- C. You should consider excluding all non-compliant client computers by applying a restricted access in the Network Policies.
- D. You should consider having the remote connection disconnected until the required updates are installed.
- E. You should consider having the Security Center enabled on each client in the Default Domain Group Policy.

**Answer: B**

**Explanation:**

:

To ensure that client computers meet the company policy requirement, you need to Quarantine clients that do not have all available security updates installed.

Using the NAP Client Configuration tool, you can configure separate enforcement policies for remote access clients. Administrators can use NAP to enforce health requirements for all computers that are connected to an organization's private network, regardless of how those computers are connected to the network. You can use NAP to improve the security of your private network by ensuring that the latest updates are installed before users connect to your private

network. If a client computer does not meet the health requirements, you can prevent the computer from connecting to your private network. To enforce remote access NAP, open NAP Client Configuration tool, double-click Remote Access Quarantine Enforcement Client, and then select the Enable This Enforcement Client check box.

Reference : Understanding Network Access Protection / Using Network Access Protection  
[http://e-articles.info/e/a/title/Network-Access-Protection-\(NAP\)-in-Windows-Vista/](http://e-articles.info/e/a/title/Network-Access-Protection-(NAP)-in-Windows-Vista/)

### QUESTION NO: 158

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

CertKiller.com currently has the Miami office configured with Network Access Protection (NAP) enforcement deployed for the Virtual Private Network (VPN) servers. During the course of the day you receive instruction from CertKiller.com to ensure that the health of all client computers can be monitored and reported.

What should you do? (Each correct answer presents part of the solution. Choose THREE.)

- A. You should consider having a network access policy.
- B. You should consider having the Require trusted path for credential entry option set to Enabled.
- C. You should consider having a Group Policy object (GPO) created.
- D. You should consider having the (GPO) linked to the Domain Controllers organizational unit (OU).
- E. You should consider having the GPO linked to the domain.
- F. You should consider having the Security Center enabled.

**Answer: C,E,F**

### Explanation:

The NAP replaces Network Access Quarantine Control (NAQC) in Windows Server 2003, which provided the ability to restrict access to a network for dial-up and virtual private network (VPN) clients. The solution was restricted to dial-up/VPN clients only.

NAP improves on this functionality by additionally restricting clients that connect to a network directly, either wirelessly or physically using the Security Center . NAP restricts clients using the following enforcement methods: IP security (IPsec), 802.1x , Dynamic Host Configuration Protocol (DHCP) and VPN.

However, to enable NAP on all the clients in your domain, you should create a group policy and link it to a domain and then enable the Security Center

Reference : Network Access Protection

[http://www.biztechmagazine.com/article.asp?item\\_id=382](http://www.biztechmagazine.com/article.asp?item_id=382)

Reference : Enabling NAP on clients through group security policies

<http://forums.technet.microsoft.com/en-US/winserverNAP/thread/749e65c7-42fa-40da-84b8-c8edc62b3eda/>

### QUESTION NO: 159

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day you receive instruction from CertKiller.com to have Network Access Protection enforcement configured in a test environment. CertKiller.com has additionally requested that you create a network policy for preventing noncompliant computers from accessing the network.

What should you do?

- A. You should consider having Access Permission set to Deny Access in the Overview tab.
- B. You should consider having NAP Enforcement set to Allow Limited Access in the Settings tab.
- C. You should consider having an IP filter created which drops all traffic in the Settings tab.
- D. You should consider having the Session Timeout set to 0 in the Constraints tab.
- E. You should consider using the Group Policy Management Console to access the wireless Group Policy settings, and enable the Prevent connections to ad-hoc networks option.

**Answer: B**

#### Explanation:

You should set NAP Enforcement to Allow Limited Access in the Settings tab. If you do not do that then the clients will be denied the network access.

#### Incorrect Answers:

- A: You should not set the Access Permission to Deny Access in the Overview tab. This will result in the blocking of the complaint and noncompliant clients.
- C: Only the remote access connection uses IP filtering. This means that the NAP policies will not apply.
- D: You should not set the Session Timeout to 0 in the Constraints tab. In doing so, will result in the

disconnecting of the remote users after a certain amount of time.

**QUESTION NO: 160**

You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day CertKiller.com requested that you develop NAP scenarios which can be used for future deployment. CertKiller.com wants you to have remediation servers configured which will be accessible to clients which do not support NAP.

What should you do? (Choose TWO.)

- A. You should consider having a network policy created with a Condition type of NAP-Capable computers.
- B. You should consider having a health policy created and is set to Client Fails All SHV Checks.
- C. You should consider having a connection request policy created with a Condition type of NAP-Capable computers.
- D. You should consider having a remediation server group created whilst ensuring that the server is accessible.
- E. You should consider having all client computers configured to have access points as RADIUS clients to the Remediation servers.

**Answer: A,D**

**Explanation:**

You should create a remediation server group with the server being accessible and a network policy with a Condition type of NAP-Capable computers. The computers without the support of NAP need a separate network policy. However the policy with the computers that are NAP-enabled should match the conditions of the Only Computers that are Not NAP-enabled. Furthermore, the remediation of server groups will define the servers that are accessible, with minimal access.

**Incorrect Answers:**

- B: Health policies do not apply to Not NAP -capable computers only to NAP-capable computers.
- C: You should not create a connection request policy with a Condition type of NAP-Capable computers. You should only use a single connection request.

**QUESTION NO: 161**



You work as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. CertKiller.com has its headquarters located in Miami and branch office located in Toronto. The CertKiller.com network servers run Microsoft Windows Server 2008 and the client computers run Microsoft Windows Vista.

During the course of the day you receive instruction from CertKiller.com to configure a computer named CERTKILLER-SR01 configured as a DHCP server. You have later decided to have a Network Access Policy (NAP) configured on the network to use DHCP enforcement. CertKiller.com wants you to ensure that the NPS and DHCP services are configured to run on different computers.

What should you do? (Choose two)

- A. You should consider having CERTKILLER-SR01 installed with NPS.
- B. You should consider having CERTKILLER-SR01 configured as a RADIUS proxy.
- C. You should consider having CERTKILLER-SR01 configured as an upstream server.
- D. You should consider having CERTKILLER-SR01 configured for Certificate Services.
- E. You should consider having CERTKILLER-SR01 installed with HRA.

**Answer: A,B**

**Explanation:**

You should configure a RADIUS proxy and install an NPS on a DHCP server. You should first install the NPS on the DHCP server and then configure RADIUS proxy. This will then forward the RADIUS request to the primary NPS server.

**Incorrect Answers:**

- C: Certificate Services are not needed with DHCP enforcement.
- D: HRA is only needed for IPsec enforcement.

**QUESTION NO: 162**

You work as a network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com.

You receive an instruction from the CIO to remediate the Windows Vista Servers, the Windows 2008 Servers as well as Windows XP service Pack 3. You need to determine the appropriate software that will be required to ensure that the Remediation Server is operational.

What should you identify?

- A. You will require the Routing and Remote Access Services (RRAS).
- B. You will require the Network Protection Services (NPS).

- C. You will require the Windows Security Health Validator (WSHV).
- D. You will require the Windows Server Update Services (WSUS).
- E. You will require Integrated Windows Authentication (IWA).

**Answer: D**

**Explanation:**

Remediation Servers requires that some kind of software be in place in order to correct users and make them compliant to accessing the secured network. By default the Windows Security Health Validator should be installed on the clients. When the Microsoft software has to be upgraded the clients will need Windows Server 2003 or Windows Server 2008 that runs the Windows Server Update Services.

**Incorrect Answers:**

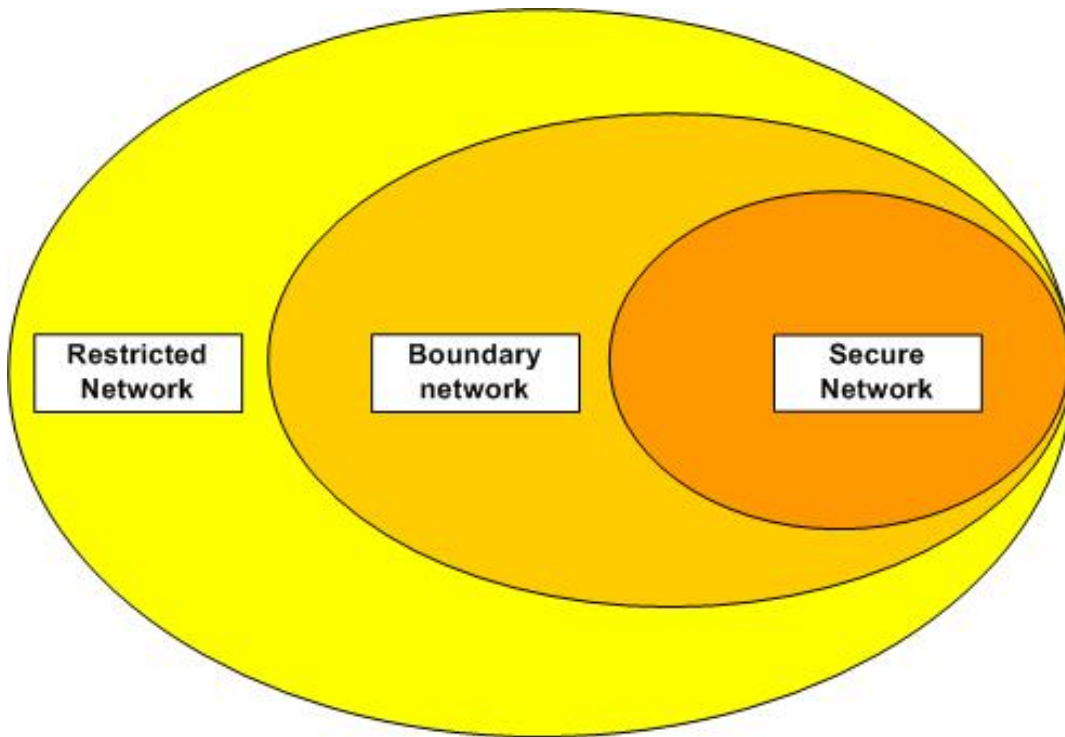
A: The requirement of Network Protection Services (NPS) and Routing and Remote Access Services (RRAS) options are incorrect. A service or a role does not remediate an in compliant workstation.

B: You make use of Windows Security Health Validator (WSHV) to check whether a workstation is compliant. The Windows Security Health Validator (WSHV) does not remediate a server. Reference: Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 163**

You work as a network administrator at CertKiller.com. The company runs Windows Server 2008 on all the servers on the network. The CertKiller.com network consists of a Windows Server 2008 single Active Directory domain.

You need to determine where the Remediation Server will be located on the network. The diagram below illustrates the network design of CertKiller.com.



- A. The appropriate location for the Remediation Server will be in the Restricted Network.
- B. The appropriate location for the Remediation Server will be in the Boundary Network.
- C. The appropriate location for the Remediation Server will be in the Secure Network.
- D. The appropriate location for the Remediation Server is irrelevant. It will perform its service from any location.

**Answer: B**

**Explanation:**

The diagram illustrates an IPsec NAP enforcement design. The Remediation Server in this scenario is located in the Boundary Network. This will enable the Secure Network to connect to the device using IPsec authentication as well as permitting the restricted network to connect in order for users to be remediated. The users will then have access to the Secured Network.

The Remediation Server was located on the Secure Network. Noncompliant computers will not be able to remediate on this network.

The Remediation Servers has to be accessible to both Secure Networks and Restricted Networks.

The location of the Remediation Servers is of no importance.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 164**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a NAP Health Policy Server named CERTKILLER-SR11 that has the following tasks: Storing the health requirement policies  
Providing health state validation for the NAP Infrastructure.

You have received instructions from management to configure CERTKILLER-SR11.

What should you do?

- A. The best option is to install the DHCP Server Role to configure CERTKILLER-SR11.
- B. The best option is to install the NAP Server Role to configure CERTKILLER-SR11.
- C. The best option is to install the NPS Server Role to configure CERTKILLER-SR11.
- D. The best option is to install the Active Directory Domain Role to configure CERTKILLER-SR11.
- E. The best option is to install the File Server role to configure CERTKILLER-SR11

**Answer: C**

**Explanation:**

You need to install the NPS Server Role to support the NAP Health Policy Server. You are permitted to install other server roles however; NPS is the primary role that has to be installed.

The DHCP Server Role, the NAP Server and the Active Directory Domain Role are all incorrect. These roles are not needed to install the NPS role on the Windows 2008 Server

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 165**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com makes use of NAP Health Policies. The NAP Health Policies comprises of settings for health determination as well as enforcement of infrastructure compliance. You have received instruction From the CIO to launch the set of settings that will comprise of the NAP Health Policies.

What should you do?

- A. You should identify the Network Policies as it includes the NAP Network Policies.

- B. You should identify the NAP Health Policies as it includes the Health Policies.
- C. You should identify the NAP Health Policies as it includes the Connection Request Policies.
- D. You should identify the NAP Health Policies as it includes the Network Access Protection Settings.
- E. You should identify the NAP Health Policies as it includes the Default Domain Policy.

**Answer: A,B,C,D**

**Explanation:**

The NAP Health Policies comprises of the Health Policies, Network Policies, Network Access Protection Settings and the Connection Request Policies. You configure the NAP Health Policies in the Network Policy Server console.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prepare.Mar.2008

**QUESTION NO: 166**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com makes use of the Network Access Protection snap-in together with NAP on their network. The previous administrator configured a set of monitoring policies on the network. You receive an instruction from the CIO to identify the purpose of the new NAP monitor policies of Windows Server 2008.

What should you tell the CIO?

- A. You should tell the CIO that it will record the compliance of all computers logging in to the system.
- B. You should tell the CIO that it will restrict non-compliant users of access.
- C. You should tell the CIO that it non-compliant users will be isolated.
- D. You should tell the CIO that it will be visible in the Windows Reliability and Performance Monitor.
- E. None of the above.

**Answer: A**

**Explanation:**

The new NAP monitor policy will record the compliance of every computer that logs into the system. NAP provides you with Monitor policies as well as Isolate policies.

Isolate policies will accomplish the isolation of the non-compliant users as well as the restriction of

access of non-compliant users.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

### QUESTION NO: 167

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com.

You are responsible for a DHCP server named CERTKILLER-SR24. You are in the process of setting up a NAP enforcement point using CERTKILLER-SR24. After the installation you receive numerous complaints from Windows Vista users stating that they are unable to operate NAP. You check and discover that DHCP is working properly.

You decide to make use of the 802.1x certified switches to validate the installation. You then setup a Windows Server 2008 server named CERTKILLER-SR25 with DHCP and Network Policy and Access Services server roles. Thereafter you set the DHCP settings for DHCPv6 Stateless Mode as well as the NPS policies with the NAP wizard.

Identify what is wrong with this set up?

- A. You should identify that IPv6 is not supported by NAP.
- B. You should identify that CERTKILLER-SR25 does not have RRAS.
- C. You should identify that IPv4 is not supported by NAP.
- D. You should identify that CERTKILLER-SR25 does not have any Network Policies configured.
- E. You should identify that the equipment in this case has to support 802.11 certified devices.

**Answer: A**

#### **Explanation:**

The scenario will work, however, NAP supports IPv4 not IPv6.

#### **Incorrect Answers:**

- B: You do not require 802.1x certified devices with a DHCP implementation.
- C: NAP does support IPv4. Reference: Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

### QUESTION NO: 168

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

At present CertKiller.com network makes use of Network Access Protection (NAP). CertKiller uses NAP to protect the network to various network communications types. You receive an instruction from the CIO to identify the communication type that is supported by NAP.

What should you identify?

- A. You should identify that DHCP Supported Network can support NAP.
- B. You should identify that RRAS Connections can support NAP.
- C. You should identify WINS Supported Network can support NAP.
- D. You should identify that IEEE 802.11B Wireless Network can support NAP.
- E. You should identify WINS configured in DHCP settings can support NAP.

**Answer: A,B,D**

**Explanation:**

NAP supports IEEE 802.1x authenticated networks, DHCP address configurations, NPSVPN connections as well as IPsec protected traffic.

Incorrect Answer:

D: NAP does not support WINS. You only make use of WINS when a Windows 2008 Server infrastructure makes use of older operating systems.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 169**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You receive an instruction from the CIO to implementing NAP on the company's network. For security purposes you need to determine how the Restricted Network will be protected from the Remediation Network.

What should you do?

- A. You should consider using IP packet filters.
- B. You should consider using IPsec with Health Certificates.
- C. You should consider using VLANs in order to split the network.
- D. You should consider using a secondary switch in order to split the network.
- E. You should consider using an isolated test network.



**Answer: A,B,C**

**Explanation:**

The IP packet filters will work if you make use of a RRASVPN as an enforcement point. Using IPsec with Health Certificates will offer you with a great way to split the network. Users connecting to the restricted network will require a valid Health Certificate in order to authenticate to the network. A VLAN can be used but when secondary switches are added it will not secure the restricted network from a secured network.

Incorrect Answer:

D: Adding a secondary switch will not split the network as the infrastructure requires.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

**QUESTION NO: 170**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com network makes use of Network Access Protection (NAP) to protect the network. A CertKiller.com policy requires that only healthy and compliant users can access the restricted network of CertKiller.com. You need to determine the valid enforcement points that will accomplish this.

What should you identify?

- A. Your best option would be to use the HUB as an enforcement point.
- B. Your best option would be to use the Windows 2008 VPN Server as an enforcement point.
- C. Your best option would be to use the IEEE 802.1x Network Access Device as an enforcement point.
- D. Your best option would be to use the DHCP Server as an enforcement point.
- E. Your best option would be to use enforcement points in the Network Policy.

**Answer: B,C,D**

**Explanation:**

The valid enforcement points are the Health Registration Authority, the DHCP Server the IEEE 802.1x Network Access Device as well as the Windows 208 VPN Server.

Incorrect Answer:

A: The hub is not a valid enforcement point. A hub is a physical layer device that is not 802.1x compliant.

Reference : Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

Part 3, Configure network authentication (13 Questions)

**QUESTION NO: 171**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are in the process of creating a Windows CardSpace in the CertKiller.com domain. All employees from the Marketing group that is also included in the Market organizational unit will be making use of this new feature. The Marketing personnel are always away from the office and require access to the secured content from various sources. These employees access their data via notebook computers, Palm devices and user workstations and Internet cafes. You receive an instruction from the CIO to ensure that these employees are able to access the secured information using Windows CardSpace in order to accomplish their daily tasks. You should thus ensure that these employees have the necessary authentication.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. You should consider putting the Marketing group in the local security group of Windows Authentication Access domain.
- B. You should consider creating and configuring machine Access Restrictions in SDDL (Security Descriptor Definition Language).  
Thereafter the remote access setting should be configured for the marketing group.
- C. You should consider assigning a password to all users in order to access the exported file containing digital identities.
- D. You should consider creating a new GPO and it to the Marketing group in the Market OU.
- E. You should consider setting the User Account Control for the marketing employees to prompt for credentials.
- F. You should consider allowing the employees to export their digital identities to a USB drive.

**Answer: C,F**

**Explanation:**

To make sure that the employees are able to access the secured content from anywhere, you need to select option D. It is the easiest and safest way to use the exported file containing digital identities to access secured content. USB drive is easy to carry and it is a plug n play device. Employees can plug the USB drive to any computer and access the exported file containing digital identities to view the secured content.

All other options are invalid in this scenario. You cannot put the sales global group in the local security group of windows Authentication Access domain because it is for local security. Users of the local security group will not be in the group once they leave their personal computer.

**QUESTION NO: 172**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com network contains two servers named CERTKILLER-SR01 and CERTKILLER-SR02. CertKiller makes use of digital authentication using Windows CardSpace to authenticate users accessing online services on internal websites on CERTKILLER-SR01. You receive an instruction from the CIO to deploy the card information on CERTKILLER-SR02. You need to identify the best method to transfer the card information to CERTKILLER-SR02.

What should you do?

- A. Your best option would be to configure the NTbackup utility to backup card information on CERTKILLER-SR01 and restore it on CERTKILLER-SR02.
- B. Your best option would be to install and configure the third party backup tool and backup the card information on CERTKILLER-SR01.  
Thereafter a third party restore backup tool should be used to restore the backup on CERTKILLER-SR02.
- C. Your best option would be to create a backup of card information on CERTKILLER-SR01 on a client computer.  
Thereafter it should be accessed from CERTKILLER-SR02 in order to restore the backup to CERTKILLER-SR02.
- D. Your best option would be to backup the card information on CERTKILLER-SR01 and restore it on CERTKILLER-SR02 using Windows CardSpace.
- E. Your best option would be to backup the card information on CERTKILLER-SR01 and restore it on CERTKILLER-SR02 using 802.1 X authentications.

**Answer: D**

**Explanation:**

The Microsoft recommended method for transferring the card information to CERTKILLER-SR02 is option D. You should use Windows CardSpace to backup card information and restore it on CERTKILLER-SR02. You cannot use third party software for backup and restore because it is not recommended by Microsoft. It is obvious that Windows CardSpace should be used to backup and restore the card information. NTbackup tool will not be able to restore the backup on the other

server and putting the card information on a client computer and accessing it from CERTKILLER-SR02 to restore the information is certainly not an option because you cannot use the third party backup for this scenario. You have to select the option which is recommended by Microsoft.

**QUESTION NO: 173**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com has Network Access Protection configured in order to limit the network access of workstations based on their predefined health requirements. A CertKiller.com security policy ensures that confidentiality of information that is in transit between the servers and the workstations. You receive an instruction from the CIO to ensure that notebook computers that do not comply with the policy requirements are stopped from accessing the resources in the company.

What should you do?

- A. This can be accomplished by creating an 802.1X enforcement network policy.
- B. This can be accomplished by creating a wired network (IEEE 802.3) group policy.
- C. This can be accomplished by creating an IPSec enforcement network policy.
- D. This can be accomplished by creating an extensible authentication protocol enforcement policy.
- E. This can be accomplished by creating a Network Policy that restricts remote connections.

**Answer: C**

**Explanation:**

:

Because the scenario suggests the configuration of the security policy on the network, you need to create an IPSec enforcement network policy as a Network Access Protection Mode to ensure that personal portable computers that don't comply with policy requirements are prohibited from accessing company resources.

IPSec enforcement network policy authenticates NAP clients when they initiate IPsec-secured communications with other NAP clients.

**Incorrect Answers:**

A: The 802.1x-based enforcement network policy and the wired network (IEEE 802.3) group policy cannot be used because they are switch-based enforcement. Every time a client activates a switch port, it's placed in a limited-access VLAN until it authenticates to a NAC server and passes assessment, which is not required here

B: The 802.1x-based enforcement network policy and the wired network (IEEE 802.3) group policy cannot be used because they are switch-based enforcement. Every time a client activates a switch

port, it's placed in a limited-access VLAN until it authenticates to a NAC server and passes assessment, which is not required here

D: Extensible authentication protocol enforcement policy is not required here because it is used to allow EAP method vendors to easily develop and install new EAP methods on both client computers and NPS servers. Reference: NAP protects networks by restricting client connections [http://www.biztechmagazine.com/article.asp?item\\_id=382](http://www.biztechmagazine.com/article.asp?item_id=382) Reference: The Cable Guy IEEE 802.1X Wired Authentication <http://technet.microsoft.com/en-us/magazine/cc194418.aspx>

#### QUESTION NO: 174

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. You are in the process of implementing Windows CardSpace in the organization.

All departments have their respective organizational units configured in the AD. Users in the Research and development department are members of the Development global group that in turn reside in the Research and Development OU. Due to the nature of their daily tasks the Research and Development users need to access secure content from various sources and confidential information from workstations at different locations. You receive an instruction from the CIO to ensure that the Research and Development users make use of Windows CardSpace for authentication.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. You should consider configuring a new group policy object (GPO) and link it to the Research and Development OU.
- B. You should consider configuring the User Account Control: Behavior of the elevation prompt for standard user GPO setting to prompt for credentials.
- C. You should consider enabling the users to export their digital identities to a USB drive.
- D. You should consider placing the Development global group into the Windows Authorization Access domain local security group.
- E. You should consider configuring a password for all users for access to the exported file.
- F. You should consider configuring the DCOM: Machine Access restrictions in security descriptor definition language setting (SDDL) syntax setting.
- G. You should consider configuring the Allow remote access setting for the Development group.

**Answer: C,E**

#### Explanation:

To ensure the Research and Development users of the company use Windows CardSpace for authentication from any computer to any of the most secured content locations, you need to

enable the users to export their digital identities to a USB drive and then configure a pass phrase for access to the exported file.

The Card Export feature of Windows CardSpace allows the copying of information cards onto an external storage medium, such as a USB drive. The USB drive can then be used to install cards onto other machines from where the user needs to access the information. For security purposes a user selected pass-phrase is used to encrypt information cards so that even if the storage medium is lost, only someone who knows the pass-phrase can decrypt the cards it contains.

None of the other options can be used because configuring group policies cannot ensure the use of Windows CardSpace for roaming users.

Reference : Introducing Windows CardSpace / Roaming with Information Cards  
[http://msdn2.microsoft.com/en-us/library/aa480189.aspx#introinfocard\\_topic4](http://msdn2.microsoft.com/en-us/library/aa480189.aspx#introinfocard_topic4)

#### **QUESTION NO: 175**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com has its headquarters in London and branch offices in Paris, Berlin, Milan and Athens. The workstations located at the branch offices make use of VPN connection to connect to the London office. You receive an instruction from the CIO to prevent users from remotely accessing the VPN server between 20:00 until 05:00.

What should you do?

- A. You should consider creating a network policy for VPN connections.  
Thereafter the IP filter should be applied to deny access to the corporate network.
- B. You should consider creating a network policy for VPN connections.  
Thereafter the Day and time restrictions should be configured accordingly.
- C. You should consider configuring the Logon hours for all user objects by only indicating the VPN server on the Computer restrictions option of the Network Connections tab.
- D. You should consider configuring the Logon Hours for the network policy by enabling the Force logoff when logon hours expire option.

**Answer: B**

#### **Explanation:**

To ensure that users cannot access the VPN server remotely from 20:00 to 05:00, you need to create a network policy for VPN connections and then modify the Day and time restrictions. The

network policy provides a policy conditions called "Allow full network access for a limited time", which allow clients to temporarily access full network. However, the NAP enforcement is delayed until the specified date and time.

Reference : Step By Step Guide: Demonstrate VPN NAP Enforcement in a Test Lab / NAP enforcement and network restriction

<http://www.microsoft.com/downloads/details.aspx?FamilyID=729bba00-55ad-4199-b441-378cc3d900a7&displaylang=en>

#### **QUESTION NO: 176**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are responsible for managing a server named CERTKILLER-SR01 which has the File Server role installed. CERTKILLER-SR01 is used by all departments in order to access their work. CERTKILLER-SR01 contains a shared folder named Sales that is used by the Finance department. You receive an instruction from the CIO to make sure that the users that belong to the Finance group are able to view and open files in Sales.

What should you do?

- A. Your best option would be to change the remote access permissions in the Network Policy for the Finance group to Modify.
- B. Your best option would be to change the share permissions for the Finance group to Read.
- C. Your best option would be to change the NTFS permissions for the Authenticated Users group to Modify and the share permissions to Contributor in the Network Policy.
- D. Your best option would be to change the share permissions for the Finance Users group to Contributor.

**Answer: B**

#### **Explanation:**

To ensure members of the Finance group can only view and open files in the shared folder, you need to modify the share permissions for the Marketing group to Read.

NTFS permissions are associated with the object, so the permissions are always connected with the object during a rename, move, or archive of the object.

Share permissions are only associated with the folder that is being shared. The share permissions standard list of options is not as robust as the NTFS permissions. The share permissions only



provide Full Control, Change, and Read. Therefore you need to assign read permission.

Reference : Share Permissions

<http://www.windowsecurity.com/articles/Share-Permissions.html>

#### QUESTION NO: 177

You are an Enterprise administrator for CertKiller.com. CertKiller.com recently hired a new trainee which you are directed to show around. CertKiller.com later directs you to enable ICS for the client computers. The new trainee as a result wants to know how ICS changes the IP settings on the computer.

What should you do? (Choose two)

- A. On the external NIC DHCP services are enabled.
- B. On the internal NIC DHCP services are enabled.
- C. The external NIC IP address will be changed to 192.168.1.100
- D. The internal NIC IP address will be changed to 192.168.0.1.
- E. The DHCP server will be restarted.

**Answer: B,D**

#### Explanation:

You should change the internal NIC IP address to 192.168.0.1. The clients on the internal interface will also get the correct IP configuration when the ICS is automatically enabled on the DHCP server.

#### Incorrect Answers:

- A: The IP address will not change on the external network, when enabling ICS changes because it is defined at your ISP.
- C: The DHCP server will be enabled on the internal network when you enable ICS, however not the external network.

#### QUESTION NO: 178

You are an Enterprise administrator for CertKiller.com. CertKiller.com recently asked you to help solve a NAT problem on the network. CertKiller.com has several plans and require you to identify which scenarios would not likely work with NAT without additional configuration.

What should you identify?

- A. Intranet clients accessing a Web server on the Internet using HTTPS.

- B. Intranet clients streaming video using a TCP connection from a server on the Internet.
- C. Intranet clients downloading e-mail from an Exchange server on the Internet.
- D. Internet clients accessing a Web server in the intranet using HTTP.
- E. Internet clients accessing a CertKiller.com server using 802.1x authentication.

**Answer: D**

**Explanation:**

NAT will not work if you leave it at its default value. For NAT to work, you need to use additional configuration. It will work if you configure port forwarding on a server that is running NAT.

Incorrect answers:

- A: The HTTPS works that same as the TCP functions. So the clients that are using HTTPS will not have a problem when connecting to the NAT server.
- B: If the streaming video using a TCP connection from a server on the Internet, the connection will work. If the streaming video uses UDP, you can come up with a problem because the NAT devices will fail a lot.
- C: Intranet clients downloading e-mail from an Exchange server on the Internet will be allowed because NAT will establish a TCP connection from the Internet.

**QUESTION NO: 179**

You are an Enterprise administrator for CertKiller.com. The CertKiller.com network currently consists of a single Windows Server 2008 computer.

CertKiller.com recently directed you to configure the only server with two NIC's for sharing a single Internet connection. You later connected one NIC to the DSL modem and the second NIC to the Layer 2-switch connecting all other computers. You later enabled ICS on the Internet NIC and require determining the IP address of the Internal NIC.

What should the IP address be?

- A. The IP will be 192.168.0.1.
- B. The IP will be 192.168.1.100.
- C. The IP will be 192.168.255.255.255.192.
- D. The IP will be the DNS server address provided by the ISP.
- E. The IP will be the public address provided by the ISP.

**Answer: A**

**Explanation:**

The internal network adapter will always receive the IP address of 192.168.0.1 from an ICS.

**Incorrect Answers:**

B: The IP address of 192.168.1.100 is not a valid address. The address of 192.168.0.0/24 however is an internal network that the client can received from the ICS.

C: This address is incorrect.

D: You should not use the IP address that the DNS server provides. The configuration should be as follows: The ICS server should send queries the DNS server and the client computers should send DNS queries to the ICS server.

E: The internal address will not be provided by the ISP. Only the Internet network adapter will have an IP address from the ISP.

**QUESTION NO: 180**

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The previous administrator has configured the network using a private Class C address space. Due to company growth you notice that you are reaching the maximum amount of devices and have to expand. You don't anticipate that the company will require more than 8188 addresses.

You need to determine a way to solve this problem. You have to accomplish this with the minimum of disruption to the network.

What should you do?

- A. The best option is to change the IP addressing scheme from Class C to Class B.
- B. The best option is to change the default subnet to 255.255.224.0.
- C. The best option is install a router and to create two new scopes on the DHCP server and reassign the IP addresses.
- D. The best option is to assign the new workstations on the network IP addresses from the existing address pool.
- E. Your best option is to configure a DHCP Relay agent on a member server.

**Answer: B**

**Explanation:**

When you modify the subnet mask from 255.255.255.0 to 255.255.224.0 it will increase the address space. This option will permit the existing users to continue using their IP addresses. The IP address space will span from 192.168.32.x to 192.168.223.254. It will slow down the network traffic as the additional IP addresses will be on the network as the existing ones.

**Incorrect Answers:**

A: When you change the address scheme from Class C to Class B will yield more host addresses as required. It will also take more configuration than changing the subnet mask.

C: You are able to install a new router in order to create a new subnet. The creation of a subnet mask is easier and you will not need to create two new scopes on the DHCP server.

D: Permitting the new workstations to lease IP addresses from the existing pool will result in overlapping IP addresses. Reference: Syngress.The.Real.MCTS.MCITP.Exam.70-648.Prep.Kit.Mar.2008

### QUESTION NO: 181

You work as a newly appointed enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You have received instructions from the CEO to subnet a network in the test lab for a future class. However, you have only received the following information:

131.107.32.x/6.6 subnets

You need to find out the subnet mask and the first address in every subnet.

What should you use?

- A. You should consider using 255.255.255.252/ 131.107.32.1, 131.107.64.1, 131.107.96.1, 131.107.128.1, 131.107.160.1 and 131.107.192.1
- B. You should consider using 255.255.255.240/ 131.107.32.1, 131.107.64.1, 131.107.96.1, 131.107.128.1, 131.107.160.1 and 131.107.192.1
- C. You should consider using 255.255.255.224/ 131.107.32.1, 131.107.64.1, 131.107.96.1, 131.107.128.1, 131.107.160.1 and 131.107.192.1
- D. You should consider using 255.255.255.192/ 131.107.32.1, 131.107.64.1, 131.107.96.1, 131.107.128.1, 131.107.160.1 and 131.107.192.1
- E. You should consider using a 24-bit subnet mask.

**Answer: C**

#### Explanation:

The /25 network notation indicates that you have to use 32 network bits. You make use of 255.255.255.224 for the subnetted subnet mask of the Class C networks. It makes use of 13 host bits. It will thus equal 224 that results in a subnet mask of 255.255.255.224. The first assignable IP address on every subnet will have to be set at 1, 32, 64 and 96.

The subnet mask of 255.255.255.252 will be notated as 131.107.32.x/30 which would have the order for the last octet set to 1111 1100

The subnet mask of 255.255.255.240 will be notated as 131.107.32.x/28 which would have the order for the last octet set to 1111 0000.

The subnet mask of 255.255.255.192 will be notated as 131.107.32.x/64 which would have the order for the last octet set to 1111 1100 255.

### QUESTION NO: 182

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com network contains 15 Web servers where one, named CERTKILLER-SR23 has the FTP service installed. All the classified files of CertKiller.com reside on CERTKILLER-SR23. A new CertKiller.com security policy requires that all the classified data should be transmitted in a secure manner.

Whilst running a security check you discover that the classified files on CERTKILLER-SR23 are transmitted over the Internet without encryption. You receive an instruction from the CIO to make sure that the classified data is transmitted over the network.

What should you do? (Each answer presents a complete solution. Choose TWO.)

- A. You should consider using NTLM authentication on CERTKILLER-SR23.
- B. You should consider using IIS and then activate SSL on the IIS server when classified data is published on CERTKILLER-SR23.
- C. You should consider using the Server Message Block (SMB) signing between CERTKILLER-SR23 and other network computers when files need to be transmitted.
- D. You should consider using IPSec encryption between CERTKILLER-SR23 and other network computers when files need to be transmitted.
- E. You should consider using a network policy that enforces the use of 802.1X authentication
- F. You should consider activating offline files for the classified files stored on CERTKILLER-SR23. Thereafter the Encrypt contents to secure data option should be selected in the Folder Advanced Properties dialog box.

**Answer: B,D**

### Explanation:

To ensure that encryption is always used when the confidential files on the FSS1 server are transmitted over the network, you need to either publish the confidential files using IIS to and activating SSL on the IIS server or use IPSec encryption between the FSS1 server and the

computers of the users who need to access the confidential files.

One of the features of IIS 7.0 is FTP over Secure Sockets Layer (SSL). This allows sessions to be encrypted between an FTP client and server.

IP Security (IPSec), mentioned briefly in previous sections, is essentially a mechanism for establishing end-to-end encryption of all data packets sent between computers. IPSec operates at Layer 3 of the OSI model and subsequently uses encrypted packets for all traffic between members.

IPSec is often considered to be one of the best ways to secure the traffic generated in an environment, and is useful for securing servers and workstations both in high-risk Internet access scenarios and also in private network configurations for an enhanced layer of security.

Reference : Using FTP Over SSL

<http://learn.iis.net/page.aspx/304/using-ftp-over-ssl/>

Reference : Using IPSec Encryption with Windows Server 2008

<http://my.safaribooksonline.com/9780672329302/ch14lev1sec5>

### **QUESTION NO: 183**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are responsible for a Windows Server 2008 server named CERTKILLER-SR24. CERTKILLER-SR24 is used to store confidential information. During a routine monitoring you notice that CERTKILLER-SR24 has been attacked numerous times. In order to secure the network you decide to disable all incoming connections to CERTKILLER-SR24.

What should you do?

- A. You should consider using the Domain Profile in Windows Firewall and enable the Block all connections option.
- B. You should consider using the Internal Profile in Windows Firewall and enable the Block all connections option.
- C. You should consider using the Public Profile in Windows Firewall and enable the Block all connections option.
- D. You should consider disabling the IP Helper in the Services snap-in.
- E. You should consider disabling Net Logon service in the Services snap-in.

**Answer: A**

**Explanation:**

To immediately disable all incoming connections to the server, you need to enable the Block all connections option on the Domain Profile from Windows Firewall.

You can configure inbound connections to Block all connections from Windows Firewall by configuring Firewall properties. When Block all connections is configured for a Domain profile, Windows Firewall with Advanced Security ignores all inbound rules, effectively blocking all inbound connections to the domain.

Reference : Configuring firewall properties

<http://technet2.microsoft.com/windowsserver2008/en/library/19b429b3-c32b-4cbd-ae2a-8e77f2ced35c1033.mspx?mfr=true>

Part 4, Configure wireless access (9 Questions)

**QUESTION NO: 184**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are in the process of deploying a protected IEEE 802.11 wireless network as well as securing the wireless network by configuring it to make use of smartcards. Thereafter, you configure the certificate infrastructure and Active Directory users and groups for wireless access. After the configuration you receive numerous complaints from users who are unable to access the wireless network. To ensure productivity you need to make sure that all users are able to access the wireless network.

What should you do?

- A. You should consider configuring the users and computer accounts on the client computers. Thereafter remote access permission should be set with the appropriate settings.
- B. You should consider configuring the users and computer accounts on the client computers. Thereafter the certificate authority should be installed on every client computer.
- C. You should consider configuring installing APs as well as configuring RADIUS settings.
- D. You should consider configuring a group policy object link it to the server.
- E. Configure the NTFS permissions on the wireless network to Allow Full Control permission.

**Answer: A**



**Explanation:**

The correct answer for this question is option A. You need to set the remote access permission by configuring the user accounts on client computers. The users can automatically connect to the wireless network through their user accounts.

**Incorrect Answers:**

B: Installing certificate authority on each client computer has nothing to do with wireless access because you have already configured and checked the certificate infrastructure.

C: Installing Access Points (APs) and configuring RADIUS settings is not a valid option in this scenario because the signals are full. APs are installed and configured when client machines are not receiving full signals.

**QUESTION NO: 185**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista

You are responsible for a IAS server named CERTKILLER-SR01. You receive an instruction from the CIO to deploy and configure wireless APs in order to provide wireless coverage from the wireless network. You make use of the relevant policies to deploy the AP's as well as to configure them to support an authentication mechanism. The authentication mechanism is Wireless Encryption Protocol (WEP) encryption with 802-1X authentication. When you test the connection with the APs you receive errors. You need to make sure that the APs are set to broadcast the signals as well as ensuring that the client computers is able to receive the wireless network coverage.

What should you do?

- A. You need to configure the Wi-Fi Protected Access (WPA) on the APs.
- B. You need to configure the WPA2 settings on the APs.
- C. You need to configure every client computer to accept the APs broadcast through Primary DNS server.
- D. You need to configure the RADIUS settings for the primary as well as the secondary RADIUS servers.
- E. You need to configure a group policy object and link it to CERTKILLER-SR01

**Answer: D****Explanation:**

In this scenario, the correct option is D. You should configure the APs to include Remote Authentication Dial-in User service (RADIUS) settings. You should use the settings such as names of primary and secondary RADIUS servers, UDP ports, RADIUS shared secret and failure

detection settings.

Options like configuring Wi-Fi Protected Access and WPA2 settings are not valid because WPA settings are related to Wireless connection security.

### QUESTION NO: 186

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com runs an ISA server as a firewall in order to secure their internal network. You are responsible for setting up remote access for users to the network by means of a Virtual Private Network (VPN) service using Point-to-Point Tunneling Protocol (PPTP). You receive various complaints from users receiving the "Error 721: The remote computer is not responding" message when attempting to connect to the VPN server after the configuration. To ensure productivity you need to make sure that the users are able to logon to the VPN server.

What should you do?

- A. You should open port 1423 on firewall.
- B. You should open port 3389 on firewall.
- C. You should open port 3380 on firewall.
- D. You should open port 1723 on firewall.

**Answer: D**

#### **Explanation:**

To establish VPN connectivity through PPTP, you need to make sure that TCP Port 1723 is opened on the Firewall and IP Protocol 47 (GRE) is configured.

The Error 721 occurs when the VPN is configured to use PPTP, which uses GRE protocol for tunneled data, and the network firewall does not permit Generic Routing Encapsulation (GRE) protocol traffic. To resolve this problem, you need to configure the network firewall to permit GRE protocol 47 and make sure that the network firewall permits TCP traffic on port 1723.

Reference : RAS Error Code / Error 721 :

<http://www.chicagotech.net/raserrors.htm#Error%20721>

Reference : You receive an "Error 721" error message when you try to establish a VPN connection through your Windows Server-based remote access server

<http://support.microsoft.com/default.aspx?scid=KB;EN-US;888201>

**QUESTION NO: 187**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are in the process of deploying a notebook computer that will be used over a wireless network. You configure a group policy and configure profiles using the names of approved wireless networks. Thereafter you link the group policy object (GPO) to the CKNotebook OU. You receive numerous complaints from users using the notebook computer stating that they are unable to connect the wireless network. You decide to make sure that the group policy wireless settings are applied to the notebook computers.

What should you do?

- A. You should connect the notebook computers to the wired network. Thereafter the network computers should be logged off and on again.
- B. You should run the `gpupdate / boot` command on the notebook computers.
- C. You should run the `gpupdate / target: computer` command on the notebook computers.
- D. You should create a Wired Network (IEEE 802.3) Group Policy and then create a GPO and link it to the CKNotebook OU.

**Answer: A**

**Explanation:**

The users cannot connect to the wireless network and the group policy wireless settings are not applied to the notebook computers because the GPO settings always try to get applied on startup before the wireless connects to the network, so it can't update. To resolve this problem, you need to connect the notebook computers to the wired network. Log off the network computers, and then log on again. As soon as the users connect to the domain as a wired network, they will receive the wireless settings. The logging off and logging on would help refreshing the policies on the notebook computers.

Reference : GPO not applied for laptops

<http://techrepublic.com.com/5208-6230->

[0.html?forumID=101&threadID=237624&messageID=2320844](http://0.html?forumID=101&threadID=237624&messageID=2320844)

**QUESTION NO: 188**

You are an Enterprise administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network

run Windows Server 2008 and all client computers run Windows Vista.

The company has Active Directory Certificate Services (AD CS) and Network Access Protection (NAP) deployed on the network. You receive an instruction from the CIO to configure the wireless network to accept smartcards.

What should you do?

- A. This can be accomplished using WPA2, PEAP and MSCHAP v2.
- B. This can be accomplished using WPA2, 802.1X authentication and EAP-TLS.
- C. This can be accomplished using WPA, PEAP, MSCHAP v2 as well as strong user passwords.
- D. This can be accomplished using WEP, PEAP, 802.1X authentication and MSCHAP v2.
- E. This can be accomplished using WPA2, SPAP authentication and PEAP.

**Answer: B**

**Explanation:**

To configure the wireless network to accept smart cards, you need to use WPA2, 802.1X authentication and EAP-TLS.

The use of smart cards for user authentication is the strongest form of authentication in the Windows Server 2003 family. For remote access connections, you must use the Extensible Authentication Protocol (EAP) with the Smart card or other certificate (TLS) EAP type, also known as EAP-Transport Level Security (EAP-TLS).

Reference:

Using smart cards for remote access

<http://technet2.microsoft.com/windowsserver/en/library/c19be042-6b5c-407a-952d-fb6f451b5edd1033.msp?mfr=true>

**QUESTION NO: 189**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

All servers on the CertKiller.com network have Remote Desktop (RDP) enabled with default security settings for server administration. You need to ensure that RDP connections between the Windows Server 2008 servers and Windows Vista client computers are secure.

What should you do?

- A. You should consider setting the security layer for every server to the RDP security Layer. Thereafter the firewall can be configured on every server to block port 3389.
- B. You should consider obtaining user certificates from the internal certificate authority. Thereafter every server should be configured to allow connections only to Remote Desktop client computers that use Network Level Authentication.
- C. You should consider configuring the firewall on every server to block port 3380.
- D. You should consider setting the security layer for every server to the RDP security Layer. Thereafter user certificates should be obtained from the internal CA.
- E. You should consider blocking communications via port 1423 on the firewall.

**Answer: B**

**Explanation:**

To ensure the RDP connections are as secure as possible, you need to first acquire user certificates from the internal certificate authority and then configure each server to allow connections only to Remote Desktop client computers that use Network Level Authentication.

In the pre-W2008 Terminal Server, you used to enter the name of the server and a connection is initiated to its logon screen. Then, at that logon screen you attempt to authenticate. From a security perspective, this isn't a good idea. Because by doing it in this manner, you're actually getting access to a server prior to authentication - the access you're getting is right to a session on that server - and that is not considered a good security practice.

NLA, or Network Level Authentication, reverses the order in which a client attempts to connect.

The new RDC 6.0 client asks you for your username and password before it takes you to the logon screen. If you're attempting to connect to a pre-W2008 server, a failure in that initial logon will fail back to the old way of logging in. It shines when connecting to Windows Vista computers and W2008 servers with NLA configured it prevents the fallback authentication from ever occurring, which prevents the bad guys from gaining accessing your server without a successful authentication.

Reference : Server 2008 Terminal Services Part 2: NLA - Network Level Authentication

[http://www.realtime-windowsserver.com/tips\\_tricks/2007/06/server\\_2008\\_terminal\\_services\\_2.htm](http://www.realtime-windowsserver.com/tips_tricks/2007/06/server_2008_terminal_services_2.htm)

**QUESTION NO: 190**

You are an Enterprise administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com recently directed you to plan the deployment of a wireless network which requires 12 access points for total coverage. CertKiller.com wants you to provide the best wireless

performance possible whilst supporting only 802.11b clients.

What should you do?

- A. You should make use of the 802.11a protocol.
- B. You should make use of the 802.11n protocol.
- C. You should make use of the 802.11g protocol.
- D. You should make use of the 802.11b protocol.
- E. You should make use of Extensible Authentication Protocol (EAP).

**Answer: B**

**Explanation:**

The protocol 802.11n has a performance speed of about 250 mbps. 802.11n is also back ward compatible with clients using the 802.11b protocol.

Incorrect answers:

- A: The protocol 802.11a uses the old standard. This protocol is not compatible with 802.11b.
- C: The protocol 802.11g is compatible with 802.11b, however 802.11n is faster.
- D: The protocol 802.11b is from the older standard, the 802.11g and 802.11n is the newer standard.

Reference:

JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp . 124

**QUESTION NO: 191**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com makes use of a wireless network with several access points. During the Day a CertKiller.com user complained that they are unable to access the wireless network. You later discover that the access point rejects the user's credentials. You check the Access point and determine that it submits authentication requests to a RADIUS server. You are required to determine the exact cause of the authentication failure.

What should you do?

- A. The Security event log should be examined on the Windows Server 2008 computer.
- B. The System event log should be examined on the Windows Server 2008 computer.

- C. The Security event log should be examined on the wireless clients.
- D. The System event log should be examined on the wireless clients.
- E. The Application log for Performance events should be examined on the Windows Server 2008 computer.

**Answer: A**

**Explanation:**

The Windows Server 2008 RADIUS service comes with events that have more detail. It also has the information of identifying the problem and also the user name that submitted it.

**Incorrect Answers:**

B: The System event log does not add events on the local Security event log. The Windows Server 2008 RADIUS service does it.

C: RADIUS does not give detail information about any failures. You should use the Security event log on the RADIUS server.

D: RADIUS does not give detail information about any failures. You should use the Security event log on the RADIUS server.

**QUESTION NO: 192**

You are employed as the enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com has recently decided to configure wireless authentication and encryption throughout the organization. CertKiller.com wants you to configure the most secure authentication mechanism as they will not sacrifice security. You later had all client computers running Windows XP Professional upgraded to the latest Service Pack.

What should you do?

- A. For the wireless network use WPA-EAP.
- B. For the wireless network use 64-bit WEP.
- C. For the wireless network use 128-bit WEP.
- D. For the wireless network use WPA-PSK.
- E. For the wireless network use a Group Policy Object (GPO).

**Answer: A**

**Explanation:**

WPA-EAP uses very flexible authentication. There is no static keys involved in this kind of authentication. It also has the highest level of security.



Incorrect answers:

B: 64-bit WEP is outdated and uses static keys. It can also be easily cracked.

C: 128-bit WEP is not so secure because it is using static keys and it can be easily cracked.

D: WPA-PSK is not so secure because it is using static keys and it can be easily cracked.

Reference:

JC Mackin and Tony Northrup' Self-Paced Training Kit: Configuring Windows Server 2008 Network Infrastructure, MCTS Exam 70-642, pp . 126

Part 5, Configure firewall settings (5 Questions)

### QUESTION NO: 193

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are responsible for a Windows Server 2008 server named CERTKILLER-SR01. CERTKILLER-SR01 is used to store confidential information. During routine monitoring you discover that CERTKILLER-SR01 has been attacked on numerous occasions. To prevent this from occurring again you decide to disable all incoming connections to CERTKILLER-SR01 immediately.

What should you do?

- A. Your best option would be to disable the Net Logon service in the Services snap-in.
- B. Your best option would be to enable the Block all connections option on the Public Profile of Windows Firewall.
- C. Your best option would be to enable the Block all connections option on the Domain Profile in Windows Firewall.
- D. Your best option would be to enable the Block all connections option on the Internal Profile in Windows Firewall.

**Answer: C**

#### Explanation:

To immediately disable all incoming connections to CERTKILLER-SR01, you need to enable the Block all connections option on the Domain Profile from Windows Firewall.

You can configure inbound connections to Block all connections from Windows Firewall by configuring Firewall properties. When Block all connections is configured for a Domain profile, Windows Firewall with Advanced Security ignores all inbound rules, effectively blocking all inbound connections to the domain.

Reference : Configuring firewall properties

<http://technet2.microsoft.com/windowsserver2008/en/library/19b429b3-c32b-4cbd-ae2a-8e77f2ced35c1033.mspx?mfr=true>

#### QUESTION NO: 194

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are responsible for managing a Windows server named CERTKILLER-SR02. You receive an instruction from the CIO to configure the Windows Firewall on CERTKILLER-SR02. This is to stop CERTKILLER-SR02 from establishing communication sessions to other computers by using the TCP port 25.

What should you do?

- A. You should consider creating an inbound rule using the Advanced Security snap-in.
- B. You should consider creating an outbound rule using the Advanced Security snap-in.
- C. You should consider enabling the Block all incoming connections option.
- D. You should consider creating an inbound rule using the Advanced Security snap-in that blocks communication from all ports except port 25.

**Answer: B**

#### Explanation:

To prevent CERTKILLER-SR02 from establishing communication sessions to other computers by using TCP port 25, you need to create an outbound rule from the Windows Firewall with Advanced Security snap-in.

By default, inbound network traffic to a computer that does not match a rule is blocked, but nothing prevents outbound traffic from leaving a computer. To block the network traffic for prohibited programs, you must create an outbound rule that blocks traffic with specific criteria from passing through Windows Firewall with Advanced Security

Reference : Creating Rules that Block Unwanted Outbound Network Traffic / Step 1: Blocking Network Traffic for a Program by Using an Outbound Rule

<http://technet2.microsoft.com/windowsserver2008/en/library/c3bb5b29-b6a8-4fd4-a66d-ddb39767b2ea1033.mspx?mfr=true>

**QUESTION NO: 195**

You are the newly appointed Enterprise administrator for CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com has given you a Windows Vista client computer for this project. CertKiller.com has recently finished installing an automation tool on a Windows Server 2008 computer which acts as a network client accessing a server on the intranet using TCP port 89 and an Internet server using TCP port 270. CertKiller.com later instructs you to install an additional client component to connect to the Windows Server 2008 computer using TCP port 37 on the Windows Vista client. CertKiller.com has informed you that the firewall settings on the computers are default. You are required to make the required changes to the configuration.

What should you do?

- A. Add a firewall rule to allow outbound connections to TCP port 37 on the Windows Vista client.
- B. Add a firewall rule to allow outbound connections to TCP port 270 on the Windows Server 2008 computer.
- C. Add a firewall rule to allow inbound connections to TCP port 270 on the Windows Vista client.
- D. Add a firewall rule to allow inbound connections to TCP port 37 on the Windows Server 2008 computer.

**Answer: D**

**Explanation:**

TCP port 37 does not have a firewall rule, by default. The inbound connections that do not have a firewall rule will be blocked by Windows Server 2008. So you need to add a firewall rule.

Incorrect answers:

- A: Windows Vista clients do allow for outbound connections by default. It is not necessary to create a firewall rule.
- B: In Windows Server 2008, you are using TCP port 270 for outbound connections. The firewall in Windows Server 2008 allows for outbound connections which are by default.
- C: In Windows Server 2008, you are using TCP port 270 for outbound connections. However it does not allow for inbound connections.

**QUESTION NO: 196**

You are an Enterprise administrator for CertKiller.com. CertKiller.com recently finished deploying a Windows Server 2008 application server which accepts incoming connections on TCP port 1028.

CertKiller.com has later informed you that the application on the server does not have access control. CertKiller.com wants you to configure the inbound firewall properties to allow connections from only authorized users in the domain.

What should you do?

- A. You should select these addresses in the Scope tab in the Local IP Address group and add each to the internal network.
- B. You should select Only Allow Connections From These Users in the Users And Computers tab and add the Domain Users group.
- C. You should click these profiles in the Advanced tab and select the Domain.
- D. You should click Allow Only Secure Connection in the General tab.
- E. You should click Deny All Connections in the General tab for the Domain Users group.

**Answer: B,D**

**Explanation:**

To obtain domain authentication, you should select Allow Only Secure Connections, that needs IPsec. Thereafter you can limit the users as needed which are part of the members in a specific group.

**Incorrect Answers:**

- A: This means that users do not have to be a member of the domain. You also should not configure the Local IP Address settings, but the Remote IP Address settings.
- C: You cannot make use of a profile to use for authentication. This will not apply to the users that are not from the domain.

**QUESTION NO: 197**

You are an Enterprise administrator for CertKiller.com. CertKiller.com has recently asked you to configure Group Policy settings which configure firewall settings for the Windows XP Professional client computers. CertKiller.com wants only the Windows Firewall node to be used to configure firewall rules. You are required to inform CertKiller.com which features will not be available when using the Windows Firewall node in Group Policy.

What should you reply?

- A. You will not be able to drop connections originating from a specific subnet.
- B. You will not be able to require using IPsec authentication for a connection.
- C. You will not be able to allow a specific executable to accept incoming connections on any port.
- D. You will not be able to use UTP traffic filtering.
- E. You will not be able to use UDP traffic filtering.

**Answer: B**

**Explanation:**

Windows Server 2008 and Windows Vista support firewall features, however Windows XP Professional does not. So you need to use IPSec.

**Incorrect Answers:**

A: Windows Firewall With Advanced security and the Windows Firewall itself support the configuring of the scope, for a rule.

C: Windows Server 2008 and Windows Vista can be used to create a rule for executables.

D: Windows XP Professional and Windows Vista support UDP traffic filtering.

**QUESTION NO: 198**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are in the process of deploying a file server named CERTKILLER-SR01. A shared folder is located on CERTKILLER-SR01 that is used by CertKiller clients to access the shared files. You receive numerous complaints from users stating that they are unable to access the shared files on CERTKILLER-SR01.

You decide to check the TCP/IP properties for CERTKILLER-SR01 and notice that it is configured to retrieve IP addresses automatically. The client workstations were configured with static IP addresses and subnet masks. To ensure productivity you need to make sure that all CertKiller.com users are able to access the shared files.

What should you do?

- A. You should consider configuring CERTKILLER-SR01 with a static IP address in the TCP/IP properties.
- B. You should consider adding the domain to the DNS suffix on the network interface.
- C. You should consider configuring a default gateway on CERTKILLER-SR01 in the TCP/IP properties.
- D. You should consider configuring the DNS server address in the TCP/IP properties.

**Answer: A**

**Explanation:**

To ensure that users are able to access the shared files, you need to configure a static IP address on CERTKILLER-SR01 because in order for both PC's to be able to communicate the Ethernet adapters will need to be configured with a static IP address and a common Subnet mask. As an example, assign one PC an IP address of 192.198.0.1 and assign the second PC an IP address of

192.198.0.2. Both machines should use the Subnet mask 255.255.255.0.

Reference : need help to setup a lan connection between 2

<http://en.kioskea.net/forum/affich-2335-need-help-to-setup-a-lan-connection-between-2>

### QUESTION NO: 199

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com recently deployed a file server named CERTKILLER-SR01. You receive an instruction from the CIO to create folder named Marketing on CERTKILLER-SR01. You need to configure NTFS permissions on Marketing in order to grant the Domain Users group the Read permission and the Marketing group the Modify permission.

Due to company growth CertKiller.com has employed a new user named Rory Allen. Rory Allen is a member of the Domain Users group as well as the Marketing group. You need to identify the appropriate permissions Rory Allen should have to accomplish his daily tasks.

What should you do?

- A. The user would have Read permission.
- B. The user would have Full Control permission.
- C. The user would have Write permission.
- D. The user would have No Access.
- E. The user would have Shared Folder permissions.

**Answer: C**

#### Explanation:

Rory Allen is a member of the Marketing group as well as the Domain Users group. NTFS permissions are cumulative and least restrictive so Rory Allen is granted READ permission by his membership in the Domain Users Group and Modify permission from his membership in the Finance Group. Read + Modify = Modify. This means that the new user can write to the folder.

Incorrect answers:

- A: Rory Allen has Modified NTFS permissions which permit him to write that means and to read permissions.
- B: Rory Allen does not have Full Control permissions because this will allow him to change permissions.
- D: Rory Allen has write permissions. The permissions assigned to him are Modified NTFS

permissions.

**QUESTION NO: 200**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com.

You completed the deployment of a Windows server 2008 Server Core to the computer. You receive an instruction from the CIO during the course of the day to create shared folders for CertKiller.com users that makes use of the command line.

What should you do?

- A. Use the command share.
- B. Use the command Netsh.
- C. Use the IPconfig tool.
- D. Use the command Net Share.
- E. Use a Network policy.

**Answer: D**

**Explanation:**

You should use the Net Share command. This will allow you to create shared folders.

**Incorrect Answers:**

- A: The Share command will not allow you to create shared folders, but is an executable program. This is used to lock legacy MS-DOS applications.
- B: The Netsh command will not allow you to create shared folders, but is used for network configurations.
- C: The IPconfig tool will not allow you to create shared folders, but is used for the displaying of IP configuration information.

**QUESTION NO: 201**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. You completed the deployment of a Windows server 2008 Server Core to the computer. During the course of the day you receive an instruction From the CIO to create disk quotas for the network users in the domain making use of the command line.

What should you do?



- A. Use the Net command line utility.
- B. Use the Share command line utility.
- C. Use the StorRept command line utility.
- D. Use the DirQuota command line tool.
- E. Use the Netsh command line.

**Answer: D**

**Explanation:**

The DirQuota command line tool is used to configure disk quotas.

Incorrect answers:

- A: The Net command line utility is used for folder sharing, not for disk quotas.
- B: The Share command will not allow you to create disk quotas. It is used to lock legacy MS-DOS applications.
- C: The StorRept command line utility is used to configure storage reports.

**QUESTION NO: 202**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You completed the deployment of a Windows server 2008 Server Core to the computer. You receive an instruction from the CIO to ensure that an e-mail is sent when the domain users utilized 90 MB of space in order to stop them from using more than 100 MB. To accomplish this you decide to configure the disk quotas.

What should you do?

- A. Your best option would be to create a soft quota with a 90 MB limit with a second soft quota of 100 MB limit
- B. Your best option would be to create a hard quota with a 90 MB limit with a second hard quota of 100 MB limit.
- C. Your best option would be to create a single soft quota with a 100 MB limit whilst creating a warning at 90 percent.
- D. Your best option would be to create a single hard quota with a 100 MB limit whilst creating a warning at 90 percent.
- E. Your best option would be to review the Quota Entries list in the properties of each volume.

**Answer: D**

**Explanation:**

A hard quota will prevent the user from exceeding their limit. So you need to create an 80% warning limit that will send to the user an e-mail.

Incorrect answers:

- A: Soft quotas will allow to user to exceed their quota limit.
- B: A hard quotas will prevent the user from exceeding the 80% limit.
- C: Soft quotas will allow to user to exceed their quota limit.

**Part 2, Configure Distributed File System (DFS) (2 Questions)****QUESTION NO: 203**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com which are configured with numerous sites. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The domain consists of a domain-based DFS namespace called \\CertKiller.com\\Management. The hierarchy of this namespace is frequently updated. This results in the PDC emulator being overloaded. You receive an instruction from the CIO to configure the \\CertKiller.com\\Management namespace in order to minimize the workload of the PDC emulator.

What should you do?

- A. This can be accomplished by enabling the Optimize for scalability option.
- B. This can be accomplished by setting the Ordering method option to Random order.
- C. This can be accomplished by setting the Ordering method option to lowest cost.
- D. This can be accomplished by using the Optimize for consistency in the Root Scalability mode.

**Answer: A**

**Explanation:**

To configure the \\CertKiller.com\\Management namespace in order to minimize the workload of the PDC emulator you need to enable the Optimize for scalability option.

The Optimize for scalability mode, also known as root scalability mode, allows organizations to use more than the recommended 16 namespace servers for hosting a domain-based namespace in consistency mode. When root scalability mode is enabled, namespace servers do not send change notification messages to other namespaces servers when the namespace changes, nor do they poll the PDC emulator every hour. Instead, they poll their closest domain controller every hour to discover updates to the namespace.

Root scalability mode reduces network traffic to the PDC emulator at the expense of faster updates to all namespaces servers.

Reference : Polling properties

<http://technet2.microsoft.com/windowsserver/en/library/0f0f3943-fd39-4a27-8b31-3f084f6a77311033.msp?mfr=true>

## QUESTION NO: 204

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com network contains a server named CERTKILLER-SR01. CERTKILLER-SR01 is configured to host the domain-based DFS namespace named \\CertKiller.com\dfs. CertKiller.com users store their information in subfolders within the DFS namespace. You receive an instruction from the CIO to ensure that only administrators are allowed to create new folders or files at the root of the \\CertKiller.com\dfs share.

What should you do?

- A. This can be accomplished by configuring the \\CERTKILLER-SR01\dfs shared folder permissions by setting the permissions for the Authenticated Users group to Reader and the Administrators group to Co-owner.
- B. This can be accomplished by starting the Delegate Management Permissions Wizard for the DFS namespace named \\CertKiller.com\dfs on CERTKILLER-SR01. Thereafter the Full Control permission can be set to Deny for the Administrators group.
- C. This can be accomplished by configuring the NTFS permissions for the C:\DFSroots\dfs folder on CERTKILLER-SR01. Then the Create folders/append data special permission to Deny for the Authenticated Users group should be set. Thereafter the Full Control permission to Allow for the Administrators group can be set.
- D. This can be accomplished by running the dfscmd.exe \\CERTKILLERSR-01\dfs /restore command on CERTKILLER-SR01.

**Answer: A**

### Explanation:

To prevent all users, except administrators, from creating new folders or new files at the root of the \\CertKiller.com\dfs share, you need to configure the \\CERTKILLER-SR01\dfs shared folder permissions by setting the permissions for the Authenticated Users group to Reader and the

Administrators group to Co-owner

Reader is allowed to only view the files and folders and a Co-owner is allowed viewing, adding, changing, and deleting all files.

Reference : Managing Files and Folders in Windows Vista

<http://www.informit.com/articles/article.aspx?p=698129&seqNum=29>

Part 3, Configure shadow copy services (4 Questions)

### QUESTION NO: 205

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com network contains a file server named CERTKILLER-SR01. A CertKiller.com user named Mia Hamm is a junior technician in your department. Mia Hamm restores a large file using the Previous Versions tab. You need to view the progress of the file restoration.

What should you do?

- A. Your best option would be to click on open files on the shared folders node in the Computer Management window that appears in Administrative tools.
- B. Your best option would be to run the shadow.exe /v command from the command prompt.
- C. Your best option would be to run vssadmin.exe query reverts from the command prompt.
- D. Your best option would be to click on sessions on the shared folders node in the Computer Management window that appears in Administrative tools.

**Answer: C**

### Explanation:

To view the progress of the file restoration, you need to run vssadmin.exe query reverts from the command prompt.

The Windows Server 2003 Volume Shadow Copy Service can also be administered from the command line by using the VSSAdmin tool that is included with Windows Server 2003. This tool replicates the features of the Shadow Copies tab of the volume Properties screen and can be called from batch files and scripts. VSSAdmin does not follow the typical "Command /switch" form, but instead uses a list of fixed commands to guide its function. Query Reverts queries the status of in-progress revert operations.

Reference : Rapid Recovery with the Volume Shadow Copy Service / Command-Line Management  
<http://technet.microsoft.com/en-us/magazine/cc196308.aspx>

#### QUESTION NO: 206

You are employed as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are in the process of planning the modification of numerous critical configuration files on a member server named CERTKILLER-SR05. During routine monitoring you discover that important information was lost during the last blackout. You receive an instruction from the CIO to restore these critical files to their previous state.

What should you do?

- A. You should use the DirQuota utility.
- B. You should use the IPconfig tool.
- C. You should use the Share command utility.
- D. You should use the VSSAdmin utility.
- E. You should use the Quota Entries list.

**Answer: D**

#### Explanation:

To restore the file to their previous state, you need to use the VSSAdmin utility. This will initiate a shadow copy with which you can use to restore the files.

#### Incorrect Answers:

- A: You cannot use the DirQuota utility to restore files. The DirQuota utility is used to configure disk quotas.
- B: You cannot use the nslookup command line utility to restore files. It is used to displaying the IP configuration information.
- C: You cannot use the Share command line utility to restore files. This is the used to lock legacy MS-DOS applications.

#### QUESTION NO: 207

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. You completed the deployment of a Windows Server 2008 workstation to the network.

You receive an instruction from the CIO to manually perform a backup of the F: drive for a file server named CERTKILLER-SR02. You decide to make use of the Windows Server Backup utility to accomplish this task. You need to inform the CIO in which location the backup would be stored.

What should do?

- A. The backup should be stored in F:\WindowsFileBackup\CERTKILLER-SR02\.
- B. The backup should be stored in F:\WindowsImageBackup\CERTKILLER-SR02\.
- C. The backup should be stored in F:\CERTKILLER-SR02\WindowsImage\Backup\.
- D. The backup should be stored in F:\WindowsImage\Backup\CERTKILLER-SR02\.
- E. The backup should be stored on a server in a hot site.

**Answer: B**

**Explanation:**

The operating system of CERTKILLER-SR021 will create a WindowsImageBackup folder, which will be in the root of the backup media. It will then create a folder with the computers name.

**QUESTION NO: 208**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You completed the deployment of another Windows Server 2008 computer to the network. You receive an instruction from the CIO to restore information that was lost during the last blackout using the Windows Server Backup utility. You need to determine the appropriate tasks that you will be able to execute.

What should you identify? (Choose all that apply.)

- A. You would be able to restore a non-system volume.
- B. You would be able to restore the system volume.
- C. You would be able to overwrite files that are currently in use.
- D. You would be able to restore individual files.
- E. You would be able to overwrite all files on all disk quotas.

**Answer: A,D**

**Explanation:**

The Windows Server Backup tool will allow you to restore non-system volumes. This will happen while the computer is running. And it can also be used to restore individual files.

Incorrect answers:

B: You cannot override the system file which the computer is on. You need to boot the computer from the installation media, Windows Server 2008.

C: You cannot overwrite files while the files are in use. You need to save the recovered files to a different folder.

Part 4, Configure backup and restore (4 Questions)

### QUESTION NO: 209

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are responsible for a Windows Server 2008 server named CERTKILLER-SR01. The Windows Backup and Restore utility is installed on CERTKILLER-SR01. You receive an instruction from the CIO to create a full backup of all the system state data to the DVD drive (E: drive) without interrupting anyone using CERTKILLER-SR01.

What should you do?

- A. You should run the Wbadmin start backup allCritical backup target:C: /quiet command to create a backup of all system and non-system data.
- B. You should run the Wbadmin start backup allCritical backup target:E: /quiet command to create a backup.
- C. You should run the Wbadmin enable backup -add target:E: command on CERTKILLER-SR01.
- D. You should run the Wbadmin enable backup add target:C: /quiet command on CERTKILLER-SR01.

**Answer: B**

**Explanation:**

:

To create a full backup of all system state data to the DVD drive (E: drive) on CERTKILLER-SR01, you need to run Wbadmin start backup allCritical backup target :E : /quiet command on CERTKILLER-SR01.

Wbadmin enables you to back up and restore your operating system, volumes, files, folders, and applications from a command prompt

Wbadmin start backup runs a one-time backup. If used with no parameters, uses the settings from the daily backup schedule



allCritical Automatically includes all critical volumes (volumes that contain operating system's state). Can be used with the -include parameter. This parameter is useful if you are creating a backup for full system or system state recovery. It should be used only when -backupTarget is specified. Here the backupTarget is DVD drive (E: drive) on the server, so you need to specify backuptarget :E :

/quiet runs the subcommand without any prompts to the user

Reference : Wbadmin start backup

<http://technet2.microsoft.com/windowsserver2008/en/library/4b0b3f32-d21f-4861-84bb-b2eadbf1e7b81033.msp?mfr=true>

### QUESTION NO: 210

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com network consists of a file server named CERTKILLER-SR01. A CertKiller.com user named Kara Lang is a newly appointed technician in your department. Kara Lang was given the assignment to restore a critical large file using the Previous Versions tab. You want to view the progress of the file restoration.

What should you do?

- A. This can be accomplished by clicking on Open Files under the Shared Folders node in the Computer Management.
- B. This can be accomplished by running vssadmin.exe query reverts on the command prompt.
- C. This can be accomplished by running shadow.exe /v on the command prompt.
- D. This can be accomplished by clicking on Sessions under the Shared Folders node in the Computer Management.
- E. This can be accomplished by running the Wbadmin command with the Start Recovery option.

**Answer: B**

#### **Explanation:**

To view the progress of the file restoration, you need to run vssadmin.exe query reverts from the command prompt.

The Windows Server 2003 Volume Shadow Copy Service can also be administered from the command line by using the VSSAdmin tool that is included with Windows Server 2003. This tool replicates the features of the Shadow Copies tab of the volume Properties screen and can be

called from batch files and scripts. VSSAdmin does not follow the typical "Command /switch" form, but instead uses a list of fixed commands to guide its function. Query Reverts queries the status of in-progress revert operations.

Reference : Rapid Recovery with the Volume Shadow Copy Service / Command-Line Management

<http://technet.microsoft.com/en-us/magazine/cc196308.aspx>

### QUESTION NO: 211

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are responsible for managing a server named CERTKILLER-SR01. CERTKILLER-SR01 contains a folder named Research that was created on the D: drive. During routine monitoring you discover that the D:\Research folder has become corrupt. A backup was last executed on 10/15/2009 at 10:00. You receive an instruction from the CIO to restore the files in the Research folder to the last successful backup version. You need to accomplish this without affecting the other folders on CERTKILLER-SR01.

What should you do?

- A. You should consider running the Wbadmin start recovery -backuptarget:D: -version: 10/15/2009-10:00-overwrite \Research command.
- B. You should consider running the Recover d:\ Research command.
- C. You should consider running the Wbadmin restore catalog -backuptarget:D: -version: 10/15/2009-10:00-quiet command.
- D. You should consider running the Wbadmin start recovery -version: 10/15/2009-10:00-itemType:File -items:d:\Research -overwrite -recursive -quiet command.

Answer:D

You should consider running the Wbadmin start recovery -version: 10/15/2009-10:00-itemType:File -items:d:\Research -overwrite -recursive -quiet command.

Answer:D

**Answer: D**

**Explanation:**

To restore all the files in the D:\ Research folder back to the most recent backup version without affecting other folders on the server, you need to run the Wbadmin start recovery -version :10/15/2009-10:00 -itemType:File -items:d:\ Research-overwrite -recursive -quiet command.

Wbadmin start recovery runs a recovery based on the parameters that are specified. In the above query, the -version 10/15/2009-10:00 specifies the version identifier of the backup to recover, -itemtype :File specifies type of items to recover. In this case it is the file that needs to be recovered. The -items :d :\Research specifies that d:\Research folder needs to be recovered. -Overwrite causes Windows Server Backup to overwrite the existing file with the file from the backup. -recursive will only recover files which reside directly under the specified folder. And -quiet runs the subcommand with no prompts to the user.

Reference : Wbadmin start recovery

<http://technet2.microsoft.com/windowsserver2008/en/library/52381316-a0fa-459f-b6a6-01e31fb216121033.mspx?mfr=true>

**QUESTION NO: 212**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are in the process of installing Windows Backup and Restore utility on a server named CERTKILLER-SR10. After the installation you discover that CERTKILLER-SR10 has failed and stopped to respond. You decide to install the Windows Backup and Restore utility on another server named CERTKILLER-SR11 in order to solve the problem. To ensure productivity you need to ensure that the Windows SharePoint Services (WSS) site is restored to CERTKILLER-SR11.

What should you do?

A. You should consider running the Wbadmin start recovery -version: 10/15/2009-10:00-itemType:File -items:d:\Research -overwrite -recursive -quiet command.

Answer:D

You should consider running the Wbadmin start recovery -version: 10/15/2009-10:00-itemType:File -items:d:\Research -overwrite -recursive -quiet command.

Answer:D

B. You should consider running Wbadmin Get Versions on the command line.

Thereafter WSS should be installed.

C. You should consider running Wbadmin Start Recovery on the command line.

Thereafter WSS should be installed.

D. You should consider running Wbadmin in order to restore the application and the sites from backup.

Thereafter WSS should be installed.

E. You should consider running Wbadmin and restore the system state.

Thereafter WSS should be installed.

**Answer: A**

**Explanation:**

:

To restore the company's Windows SharePoint Services (WSS) site to CERTKILLER-SR11, you need to run Wbadmin with the Start Recovery option and then install WSS on the Server.

The Start Recovery option will run a recovery of the volumes, applications, files, or folders specified and will recover the application and sites. However, to run the WSS site, you need WSS on CERTKILLER-SR11 and therefore you need to install WSS on it.

Reference : <http://technet2.microsoft.com/windowsserver2008/en/library/4b0b3f32-d21f-4861-84bb-b2eadbf1e7b81033.msp?mfr=true>

<http://technet2.microsoft.com/windowsserver2008/en/library/4b0b3f32-d21f-4861-84bb-b2eadbf1e7b81033.msp?mfr=true>

Reference: Active Directory Backup and Restore in Windows Server 2008

[http://technet.microsoft.com/en-us/magazine/cc462796\(TechNet.10\).aspx](http://technet.microsoft.com/en-us/magazine/cc462796(TechNet.10).aspx)

Part 5, Manage disk quotas (4 Questions)

## **QUESTION NO: 213**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

You are responsible for managing a server named CERTKILLER-TS01. CERTKILLER-TS01 is configured to host the Terminal Services role. The Terminal server user profiles are located in a folder named Profiles on a server named CERTKILLER-TS02. A Terminal server named CERTKILLER-TS03 contains the home folders for all CertKiller.com users.

During routine monitoring you discover that only 8% of hard disk space is available on

CERTKILLER-TS02. You check and discover that users save their files on their profiles rather than their home folders. You decide to limit the amount of disk space assigned to every user to 225 MB.

What should you do?

- A. You should consider configuring the disk quotas for the volume that hosts Profiles. Thereafter the users should be limited to only use 225 MB of space.
- B. You should consider configuring all profiles by activating disk quota. Thereafter folder redirection settings should be applied in order to redirect the users to save their files on CERTKILLER-TS03.
- C. You should creating an alert that will be triggered when disk space used exceeds 225 MB in the Windows Reliability and Performance monitor.
- D. You should consider creating a new GPO and link it to CERTKILLER-TS01. Thereafter the Profiles folder should be configured in order to limit the disk space quota to 225MB for all users.
- E. You should consider configuring a GPO on CERTKILLER-TS01. Thereafter a default quota limit of 225 MB should be configured and a warning level policy set.

**Answer: A**

**Explanation:**

To limit the amount of disk space assigned to every user to 225 MB, you need to configure the disk quotas for the volume that hosts the Profiles folder and then limit the users to use only 225 MB of space.

Configuring a quota limit through group policy will not help in Terminal services scenario. Also disk quotas cannot be configured for each user profile rather it is configured on a volume or a folder.

Reference : Working with Quotas

<http://technet2.microsoft.com/windowsserver2008/en/library/31790148-eaf1-4115-8a50-4ce7a4503d211033.mspx?mfr=true>

Reference : Setting Up File Sharing Services

[http://safari.phptr.com/9780596514112/setting\\_up\\_file\\_sharing\\_services](http://safari.phptr.com/9780596514112/setting_up_file_sharing_services)

**QUESTION NO: 214**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com network contains file server named CERTKILLER-SR01. CERTKILLER-SR01 is used by CertKiller.com users to store their information. In order to manage the server space you

decide to configure quotas on CERTKILLER-SR01. You need to view the quota usage of all users on a per folder basis.

What should you do?

- A. To view the quota usage you need to review the Quota Entries list from the properties of every volume.
- B. To view the quota usage a Storage Management report should be created from the File Server Resource Manager.
- C. To view the quotas in use you should use the logs in the Windows Reliability and Performance Monitor.
- D. To view the quota usage a File Screen should be created using the File Server Resource Manager.
- E. To view the quota you need to run `dirquota.exe quota list` on the command prompt.

**Answer: B**

**Explanation:**

To view quota usage of every user on a per folder basis, you need to create a Storage Management report from File Server Resource Manager. File Server Resource Manager allows you to create quotas to limit the space allowed for a volume or folder and generate notifications when the quota limits are approached or exceeded. It also allows you to generate storage reports instantly, on demand.

To manage storage resources on a remote computer, you can connect to the computer from File Server Resource Manager. While you are connected, File Server Resource Manager will display the objects created on the remote computer.

Reference : Using the File Server Resource Manager Component / Managing Storage Resources on a Remote Computer

<http://technet2.microsoft.com/windowsserver/en/library/3510fd7c-cbfc-4f67-b4fc-d7de7c13373b1033.msp?mfr=true>

Reference : Introduction to File Server Resource Manager

<http://technet2.microsoft.com/windowsserver/en/library/3510fd7c-cbfc-4f67-b4fc-d7de7c13373b1033.msp?mfr=true>

**QUESTION NO: 215**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com network contains file server named CERTKILLER-SR02. CERTKILLER-SR02 is used by 50 users in the Sales department. These users utilize CERTKILLER-SR02 as well as storing their files on it. In order to manage the disk space you decide to configure it with quotas. To save you time you decide to make use of a quota template in order to apply the quotas to 50 folders. You need to modify the quota settings with the least amount of administrative effort.

What should you do?

- A. Your best option would be to create a file screen template and apply it to the root of the volume containing the folders.
- B. Your best option would be to delete the quota template and create it again. Thereafter apply the file screen template to the root of the volume containing the folders.
- C. Your best option would be to create a new quota template apply it to all the folders. Thereafter the quota should be modified for every folder.
- D. Your best option would be to modify the quota template.

**Answer: D**

**Explanation:**

To modify the quota settings for all 50 folders by using the least amount of administrative effort, you can simply modify the quota template with the new settings that you want for all 50 folders.

If you base your quotas on a template, you can automatically update all quotas that are based on a specific template by editing that template. This feature simplifies the process of updating the properties of quotas by providing one central point where all changes can be made

Reference:

About Quota Templates

<http://technet2.microsoft.com/windowsserver2008/en/library/31790148-eaf1-4115-8a50-4ce7a4503d211033.mspx?mfr=true>

**QUESTION NO: 216**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

The CertKiller.com network contains file server named CERTKILLER-SR02. CERTKILLER-SR02 contains a shared folder that is used by all users to store data. Due to the critical nature of the data you do not want to deny users the ability to store data on the shared folder when it surpasses the 400 MB data storage limit. You want to be notified when a user stores more than 400 MB of



data in the shared folder.

What should you do?

- A. You should create a hard quota to accomplish the task.
- B. You should create a Passive Screening File Screen to accomplish the task.
- C. You should create an indirect quota to accomplish the task.
- D. You should create a soft quota to accomplish the task.
- E. You should create an Active Screening File Screen to accomplish the task.

**Answer: D**

**Explanation:**

To allow users to store more than 400 MB of data in the shared folder and to receive a notification when a user stores more than 400 MB of data in the shared folder, you need to create a soft quota. A soft quota does not enforce the quota limit but generates all configured notifications.

A hard quota cannot be used because it prevents users from saving files after the space limit is reached and generates notifications when the volume of data reaches each configured threshold.

Reference : Working with Quotas

<http://technet2.microsoft.com/windowsserver2008/en/library/fa248320-c5a5-4c40-8237-1bc22eb8253d1033.mspx?mfr=true>

Part 6, Configure and monitor print services (6 Questions)

**QUESTION NO: 217**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

The CertKiller.com domain contains a computer that is configured to run the UNIX operating system as well as a member server named CERTKILLER-SR01. You install the default Print Server role on CERTKILLER-SR01. You receive an instruction from the CIO to ensure that all users run their print jobs through CERTKILLER-SR01 whether they are UNIX clients or Windows clients?

What should you do? (Choose all that apply.)

- A. This can be accomplished by configuring the printers on CERTKILLER-SR01 to make use of Line Printer Remote printing.

- B. This can be accomplished by installing the File Server role as well as activating the services for the NFS Role Service option on CERTKILLER-SR01.
- C. This can be accomplished by installing the Internet Printing server role on CERTKILLER-SR01.
- D. This can be accomplished by installing the Line Printer Daemon (LPD) Services role service on CERTKILLER-SR01.
- E. This can be accomplished by applying a restrictive Print permission in the Default Domain Policy.

**Answer: A,D**

**Explanation:**

:

To provide support to the UNIX users who print on CERTKILLER-SR01, you need to either install the Line Printer Daemon (LPD) Services role service on CERTKILLER-SR01 or configure the printers on CERTKILLER-SR01 to use Line Printer Remote printing.

The Line Printer Daemon (LPD) Service installs and starts the TCP/IP Print Server (LPDSVC) service, which enables UNIX-based computers or other computers that are using the Line Printer Remote (LPR) service to print to shared printers on this server.

You can use Print Services for UNIX to make your Windows computer work as a Line Printer Daemon (LPD) and Remote Line Printer client

Reference: Overview of Print Services/ LPD Service

<http://technet2.microsoft.com/windowsserver2008/en/library/b7ccec81-c84b-4533-9a7b-53bdaed2f7841033.mspx?mfr=true>

Reference: HOW TO: Install and Configure Print Services for UNIX

<http://support.microsoft.com/kb/324078>

**QUESTION NO: 218**

You are the newly appointed network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com has its headquarters in London and a branch office in Paris. The London office contains a printer server named CERTKILLER-PR01 and the Paris office a printer server named CERTKILLER-PR02. CERTKILLER-PR01 is used to manage 10 printers and CERTKILLER-PR02 manages 4 printers. The previous administrator added CERTKILLER-PR02 to the Print Management Console on CERTKILLER-PR01. You need to ensure that an automatic notification is sent to the users when the printer is unavailable.

What should you do?

- A. Your best option would be to configure an e-mail notification for the Printers With Jobs printer filter.
- B. Your best option would be to enable the Show informational notifications for local printers option on CERTKILLER-PR01 as well as CERTKILLER-PR02.
- C. Your best option would be to enable the Show informational notification for network printer option on CERTKILLER-PR01as well as CERTKILLER-PR01.
- D. Your best option would be to configure an e-mail notification for the Printers Not Ready printer filter.
- E. Your best option would be to enable the Show informational notification for the Printers With Jobs printer filter.

**Answer: D**

**Explanation:**

To send an automatic notification to the users when a printer is not available, you need to use the default print filter called Printers Not Ready to sort the filters that are not in working condition and then configure an email notification for the users telling them that the printer is not available. The Printers Not Ready filter can help you to quickly find out which printers are not ready by selecting the Printers Not Ready node and the email notifications can be sent when the filter condition is met, or a script can be specified to be run when the condition is met.

You should not use the With Jobs printer filter because this filter will bring out the filters that already have print jobs and are working.

Reference: Using Printer Filters

[http://www.windowsnetworking.com/articles\\_tutorials/Managing-Printers-Windows-Server-2003-R2.html](http://www.windowsnetworking.com/articles_tutorials/Managing-Printers-Windows-Server-2003-R2.html)

Reference : Create a New Printer Filter

<http://technet2.microsoft.com/windowsserver2008/en/library/0ba8afd8-40fb-440a-8c95-4b3aebd219281033.msp?mfr=true>

**QUESTION NO: 219**

You work as a network administrator at CertKiller.com. The CertKiller.com network currently contains eight printer servers running Windows Server 2008. CertKiller.com has planned the centralization of management of the print servers by moving all printers to a single Windows Server 2008 Server Core computer. You have later exported the printers from individual servers and require importing the servers to the new print server.

What should you do?

- A. You should use the printbrm -r -f <filename> command line utility.
- B. You should use the printui -b -f <filename> command line utility.
- C. You should use the netsh print import <filename> command line utility.
- D. You should use the printbrmengine -r -f <filename> command line utility.
- E. You should use the printbrm -b<filename> command line utility.

**Answer: A**

**Explanation:**

You can use the printbrm -r -f <filename> command line utility to require importing the servers to the new print server. The printbrm can import and export printer settings.

Incorrect answers:

- B: You can use the printui -b -f <filename> command line utility to import the servers to the new print server. This is a graphical interface; however the 'b' can export printer configurations but not import them.
- C: The Netsh command is used to configure network settings.
- D: You can use the printbrmengine -r -f <filename> command line utility to import the servers to the new print server. It is an executable file that is used by the PrintBRM and the PrintBMRUI. However, you cannot use it directly.

**QUESTION NO: 220**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com recently finished deploying several print servers to the network to be used for network printing. CertKiller.com has directed you to write a script which publishes the print servers to Active Directory.

What should you do?

- A. Use the Pubprn.vbs script for publishing
- B. Use the PrnQctl.vbs script for publishing.
- C. Use the PrnMngr.vbs script for publishing.
- D. Use the PrnCnfg.vbs script for publishing.
- E. Use the netsh command line utility for publishing.

**Answer: A**

**Explanation:**

You can use the Pubprn.vbs script to publish the print servers to Active Directory.

**Incorrect Answers:**

B: You cannot use the PrnQctl.vbs script to publish the print servers to Active Directory. It is used to print a test page, pause or to resume the printer.

C: You cannot use the PrnMngr.vbs script to publish the print servers to Active Directory. It is used to add or remove printers.

D: You cannot use the PrnCnfg.vbs script to publish the print servers to Active Directory. It is used to configure printer names, locations, permissions, and other settings.

**QUESTION NO: 221**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com recently finished the deployment of a shared printer named CERTKILLER-PR01 from a member server named CERTKILLER-SR05. The Internet Printing role is installed on CERTKILLER-SR05. You receive an instruction from the CIO to configure a client computer that will be used for printing to the shared printer from behind a firewall that will only allow Web connections.

What should you do?

- A. Use the UNC path \\CERTKILLER-SR05\CERTKILLER-PR01.
- B. Use the UNC path \\CERTKILLER-SR05\Printers\CERTKILLER-PR01\printer.
- C. Use the UNC path http://CERTKILLER-SR05/Printers/CERTKILLER-PR01/printer.
- D. Use the UNC path http://CERTKILLER-SR01/Printers/CERTKILLER-SR05/printer.
- E. Use the UNC path http://CERTKILLER-SR05/CERTKILLER-PR01.

**Answer: C**

**Explanation:**

You can use the UNC path http://CERTKILLER-SR05/Printers/CERTKILLER-PR01/printer to share printer from behind a firewall which only allows Web connections.

Incorrect answers:

A : You need to use the HTTP and specify the URL.

B: There is no need to name the folder or the Printers folder as the UNC path. With the UNC path you cannot bypass the firewall.

E: You can use UNC path http://CERTKILLER-SR05/CERTKILLER-PR01to connect the printer

across a LAN. But you need to use a URL. This will allow you to use Internet printing and to bypass the firewall.

**QUESTION NO: 222**

You work as the network administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008 and all client computers run Windows Vista.

CertKiller.com recently finished the deployment of numerous print servers to the network that will be utilized for network printing. CertKiller.com recently directed you to configure the printers to notify you by e-mail when specific printers run out of paper or suffers a paper jam.

What should you do?

- A. You should consider configuring a notification from the driver properties.
- B. You should consider creating a custom filter.
- C. You should consider configuring e-mail notification using the PrintBRM utility.
- D. You should consider configuring an e-mail notification from the printserver.

**Answer: B**

**Explanation:**

To notify you by e-mail specific printers run out of paper or suffers a paper jam, you should create a custom filter that comprises the criteria that includes the printer name and problem status. After that you can create a notification for the custom filter to send an e-mail.

**Incorrect Answers:**

- A: Configuring a notification from the driver properties will not help. You should first create a custom filter and only then create a notification for the filter.
- C: The PrintBRM utility is used to import and export printer settings.
- D: Configuring a notification from the printer's properties will not help. You should first create a custom filter and only then create a notification for the filter.

**QUESTION NO: 223**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. CertKiller.com has its headquarters in Chicago and a branch office in Dallas.

The branch office at Dallas contains 15 standalone servers that run Windows Server 2008. CertKiller.com also contains a WSUS server named CERTKILLER-SR20. All updates first get

approved and then placed on CERTKILLER-SR20. Consequently all approved updates for the servers at CertKiller.com reside on CERTKILLER-SR20. CertKiller.com wants all servers at CertKiller.com to get approved updates only.

What should you do?

- A. You should consider configuring Automatic Updates on all servers by using the Control Panel.
- B. You should consider configuring the Windows Update Settings on all servers in the local group policy.
- C. You should consider running the wuauctl.exe /reauthorization command on every server.
- D. You should consider running the wuauctl.exe /detectnow command on every server.

**Answer: B**

**Explanation:**

You need to configure the Windows Update Settings on each server by using the local group policy to receive updates from CERTKILLER-SR20. Microsoft suggests the use of Group Policy for setting up computers and WSUS in clients.

**Incorrect Answers:**

- A: To configure the Windows Update Settings on all the servers would be time consuming.
- C: Running these commands will force the update detection and reauthorization respectively and therefore cannot be used for configuration. Reference: What does wuauctl.exe /detectnow do <http://www.wsus.info/forums/lofiversion/index.php?t6505.html> Reference: Adding Computers to WSUS 3.0 SP1 (Windows Server 2008) <http://www.geekzone.co.nz/chakkaradeep/4564>
- D: Running these commands will force the update detection and reauthorization respectively and therefore cannot be used for configuration. Reference: What does wuauctl.exe /detectnow do <http://www.wsus.info/forums/lofiversion/index.php?t6505.html> Reference: Adding Computers to WSUS 3.0 SP1 (Windows Server 2008) <http://www.geekzone.co.nz/chakkaradeep/4564>

**QUESTION NO: 224**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com also contains a server named CERTKILLER-SR21, where you have installed Windows Update Server (WSUS). You also use remote SQL to store the WSUS database. Secure Sockets Layer (SSL) on CERTKILLER-SR21. It is used to encrypt metadata transferred between client computers and downstream WSUS servers. However, you notice that the connection between the SQL server and CERTKILLER-SR21 is not secure. You need to secure the database connection.



What should you do? (Choose all that apply.)

- A. The best option is to use CERTKILLER-SR21 for the database.
- B. The best option is to install SQL and WSUS on different servers and configure them as stand-alone servers.
- C. The best option is to configuring Internet Protocol Security (IPSec) on the connection between SQL server and CERTKILLER-SR21.
- D. The best option is to configure the connection between the two servers by using IPv4 static addresses.

**Answer: A,C**

**Explanation:**

You can place the database on WSUS server and configure IPSec on the network. The SSL protocol enables client computers and WSUS servers to authenticate the WSUS server and pass encrypted metadata. You have to change the URL configured for the clients to connect to WSUS server. The WSUS SSL deployments have some security limitations. You should place the database on the WSUS server to secure the database connection in this scenario. Then you can deploy IPSec between the WSUS and SQL server to encrypt all traffic between them.

Other options like installing both SQL server and WSUS on standalone computers are not valid because their membership in the domain has no effect on the data security exchanged between the two servers.

**QUESTION NO: 225**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains two servers named CERTKILLER-SR22 and CERTKILLER-SR23. Both these servers have WSUS installed. The difference between the two WSUS servers is that only CERTKILLER-SR22 has the approved and tested updates. You have received instructions for the management to allow CERTKILLER-SR23 to get updates from CERTKILLER-SR22 only and not from the official Microsoft website.

What should you do?

- A. You should configure CERTKILLER-SR22 as a proxy server.
- B. You should configure CERTKILLER-SR23 as a proxy server.
- C. You should configure CERTKILLER-SR22 as an upstream server.
- D. You should configure CERTKILLER-SR23 as an upstream server.

**Answer: C**

**Explanation:**

To configure WSUS on CERTKILLER-SR22 so that the CERTKILLER-SR23 receives updates from CERTKILLER-SR22, you need to configure CERTKILLER-SR22 as an upstream server. The WSUS hierarchy model allows a single WSUS server to act as an upstream server and impose its configuration on those servers configured as downstream servers below it.

A WSUS hierarchy supports two modes, autonomous mode and replica mode. In replica mode, the upstream server is the only WSUS server that downloads its updates from Microsoft Update. It is also the only server that an administrator has to manually configure computer groups and update approvals on. All information downloaded and configured on to an upstream server is replicated directly to all of the devices configured as downstream servers.

Reference : Deploying Microsoft Windows Server Update Services / WSUS in a Large LAN  
[http://www.windowsnetworking.com/articles\\_tutorials/Deploying-Microsoft-Windows-Server-Update-Services.html](http://www.windowsnetworking.com/articles_tutorials/Deploying-Microsoft-Windows-Server-Update-Services.html)

**QUESTION NO: 226**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a server named CERTKILLER-SR25 that has WSUS installed. The CertKiller.com security policy states that all traffic on the corporate network should be encrypted. You need to make sure that the traffic between both the WSUS administrative website and their computer is compliant with the security policy.

What should you do?

- A. You should configure NTFS permissions on the CERTKILLER-SR25  
On the content directory you should Deny Full Control permission to the Everyone group.
- B. You should configure IPsec security on CERTKILLER-SR25.
- C. You should configure CERTKILLER-SR25 to require Integrated Windows Authentication (IWA) when users connect to CERTKILLER-SR25.
- D. You should configure SSL encryption on the WSUS server administrative website.

**Answer: D**

**Explanation:**

To ensure that the traffic between the WSUS administrative website and the server administrator's computer is encrypted, you need to configure SSL encryption on the WSUS server website

Now that you have the necessary certificate, you must configure IIS to use it. To do so, expand the Default Web Site in the IIS Manager console and then right click on the WSUSAdmin virtual directory and select the Properties command from the resulting shortcut menu. You will now see the properties sheet for the WSUSAdmin virtual directory. Select the properties sheet's Directory Security tab and then click the Edit button that's found in the Secure Communications section. Select the Require Secure Channel (SSL) check box and click OK, Apply, and OK.

Reference : Applying Certificates to a WSUS Server / Enforcing SSL Encryption

<http://www.windowsecurity.com/articles/Applying-certificates-WSUS-Server.html>

### QUESTION NO: 227

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a non-Active Directory environment. All servers on the CertKiller.com network run Windows Server 2008.

All updates first get approved and then placed on CERTKILLER-SR26. Consequently all approved updates for the servers at CertKiller.com reside on CERTKILLER-SR26. CertKiller.com wants all servers and client computers at CertKiller.com to get approved updates from CERTKILLER-SR26.

What should you do?

- A. You should open the Control Panel of each server and configure the Windows Update Settings.
- B. You should run wuauctl.exe /reauthorization on each server.
- C. You should configure the Windows Update Settings on these servers, in the local group policy.
- D. You should run wuauctl.exe /detectnow on each computer in the CertKiller.com domain.

**Answer: C**

#### **Explanation:**

To configure all the servers on the network to receive updates from CERTKILLER-SR26, you need to configure the Windows Update settings using local group policy on each server on the corporate network.

Windows Server Update Services (WSUS) clients can be configured to provide update installation and reboot behavior best suited to your environment and your business needs. You can use Group Policy or Local Group Policy to modify Automatic Update configuration on your WSUS clients to determine what notification, download, install, and reboot behavior your WSUS managed clients will experience in updating from WSUS.

Reference : Managing the WSUS Automatic Updates Client Download, Install, and Reboot

Behavior with Group Policy

[http://technet.microsoft.com/hi-in/library/cc512630\(en-us\).aspx](http://technet.microsoft.com/hi-in/library/cc512630(en-us).aspx)

### QUESTION NO: 228

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com has headquarters in London and 15 branch offices in the adjacent region with more than 1500 employees strong. The employees at the branch offices are managed by the management staff at CertKiller.com's London office. You have received instruction from the CIO to design the WSUS architecture for CertKiller.com network.

What should you do?

- A. The best option is to deploy a WSUS server at each branch office and configure the WSUS server to be replicas of the WSUS server in London.
- B. The best option is to deploy a WSUS server at each branch office and configure each WSUS server as an upstream server.
- C. The best option is to deploy a WSUS server at the London office and configure the client computers at the branch offices to retrieve updates directly from the WSUS server at the London office.
- D. The best option is to deploy a WSUS server at the London office and configure the client computers to retrieve updates from Microsoft.

**Answer: A**

#### **Explanation:**

The best option is to make use of a WSUS server from where each computer can download the updates.

#### **Incorrect Answers:**

B: All the management staff is at London. It will not be effective if you let the management staff run all the WSUS servers at each branch office. It is best to make use of a WSUS server at the London and let the other computers connect remotely to download updates.

C: CertKiller.com has 1500 users. To let each user connect to Microsoft for updates will be too much and then most of the updates will fail. It will be then best to put a WSUS server at each branch office.

D: CertKiller.com has 1500 users. To let each user connect to Microsoft for updates will be too much and then most of the updates will fail. It will be then best to put a WSUS server at each branch office.

**QUESTION NO: 229**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are busy with the configuration of an update infrastructure at CertKiller.com. You have received instructions from the CIO to configure the user workstations in order to download updates as well as installing updates automatically. To accomplish this task you device to make use of a Group Policy.

What should you do?

- A. You should configure a WSUS and allow Automatic Updates Immediate Installation for all client computers on the Group Policy.
- B. You should have Automatic Updates configured on the Group Policy.
- C. You should enable Client-Side Targeting on the Group Policy.
- D. You should have No Auto-Restart For Scheduled Automatic Updates on the Group Policy.

**Answer: B**

**Explanation:**

You should enable the group policy to have Automatic Updates. By default, the Windows Update Client will prompt the user to do the installation. The group policy can be set to configure updates and when to install them.

**Incorrect Answers:**

- A: If you configure the allow Automatic Updates Immediate Installation, it will immediately download updates. Selecting this option will not allow the computer to reboot.
- C: Client-Side Targeting can be used to configure the computers as member of group. It will have no effect of how the updates are installed.
- D: If you configure the No Auto-Restart For Scheduled Automatic Updates, it will not automatically reboot the system.

**QUESTION NO: 230**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. CertKiller.com contains a server that has WSUS installed. You need to determine which operating systems will not support the WSUS clients.

What should you identify? (Choose all that apply.)

- A. You should identify Windows XP Professional as it will not support WSUS user computers.
- B. You should identify Windows 2000 Professional as it will not support WSUS user computers.
- C. You should identify Windows 95 as it will not support WSUS user computers.
- D. You should identify Windows 98 as it will not support WSUS user computers.
- E. You should identify Windows 98 upgraded to Windows XP Professional as it will not support WSUS user computers.

**Answer: C,D**

**Explanation:**

Windows 95 and 98 do not support WSUS client computers. Only Windows 2000 can act as a WSUS client if it has Service Pack 3 or later. Windows XP Professional can act as a WSUS client.

**QUESTION NO: 231**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You have just completed an audit of the workstations to check if they have their security updates. You are planning to use the MBSA for this task. However, some of the workstations do not have all the security updates. You need to find out why the updates failed.

What should you do? (Choose all that apply)

- A. You should look in the %SystemRoot%\WindowsUpdate.log file.
- B. You should look in the System log on the WSUS server.
- C. You should look in the Applications And Services Logs\Microsoft\Windows\WindowsUpdateClient\Operational on the client computer.
- D. You should look in the System log on the client computer.
- E. You should look in the events log of the Windows Reliability and Performance Monitor.

**Answer: A,C,D**

**Explanation:**

A: To investigate way the updates failed, you need to examine the %SystemRoot%\WindowsUpdate.log file. This will have detailed information which will be produced by the Windows Update Client.

C: To investigate way the updates failed, you need to examine the Applications And Services Logs\Microsoft\Windows\WindowsUpdateClient\Operational. This will have detailed information which will be produced by the Windows Update Client.

D: To investigate way the updates failed, you need to examine the System log. This will have detailed information which will be produced by the Windows Update Client.

Incorrect Answer:

B: The audit of some of the client computers does not have the security updates. This means the information will be available on the WSUS server.

#### **QUESTION NO: 232**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

To make sure that the WSUS updates are distributed successfully, which of the following can be derived from the Update Status Summary report?

- A. It will indicate to you that the WSUS can be used to remove the update.
- B. It will indicate to you systems that failed to install an update.
- C. It will indicate to you which computer group was approved for the update.
- D. It will indicate to you systems that successfully have installed the update.
- E. It will indicate to you that the WSUS is failing according to the Windows Security Health Validator.

**Answer: B,C**

#### **Explanation:**

The Update Status Summary report will have all the updates that were downloaded and the computers that were approved. It will also have the pie chart of the computers where the update failed and where it was successful.

#### **Incorrect Answers:**

- A: The Update Status Summary report will not indicate if the WSUS can be used to remove the update.
- D: It will not show which system has the update installed, however it shows the number of computers that have the update installed.

#### **QUESTION NO: 233**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a server that has WSUS installed. You have just completed the grouping of the systems on the network. You want these systems to be members of different groups for update staggering. You have received instructions from the CEO to set up the computer group for



a computer.

What should you do? (Choose all that apply.)

- A. You should right-click the computer and choose Change Membership in the Update Service console.
- B. You should drag the computers to the appropriate group in the Update Service console.
- C. You should enable the Configure Automatic Updates policy.
- D. You should configure the Enable Client-Side Targeting Group Policy setting.
- E. You should right-click the computer and choose Configure Automatic Updates in the Update Service console.

**Answer: A,D**

**Explanation:**

If you configure the Enable Client-Side Targeting Group Policy setting, it will place all of the computers in the GPO in a specific computer group. Also if you Right-click the computer and select Change Membership in the Update Services console, it will allow you to place a computer in a computer group.

Incorrect answers:

- B: You cannot drag and drop to move the computers in the Update Service console.
- C: You cannot use the Configure Automatic Updates policy to define computer group membership.

**QUESTION NO: 234**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are responsible for a Windows Server 2008 server named CERTKILLER-SR25. CERTKILLER-SR25 has the WSUS services installed. You receive an instruction from the CIO make sure that traffic between the WSUS administrative website and the server administrator's computer is encrypted. You need to determine the best solution that will accomplish this.

What should you do?

- A. The best option is to run the netdom trust /SecurePasswordPrompt command on CERTKILLER-SR25.
  - B. The best option is to configure IPsec security on CERTKILLER-SR25
- Then the content directory to should be configured to Deny Full Control permission to the Everyone group on CERTKILLER-SR25.

- C. The best option is to configure SSL encryption on the WSUS server administrative website.
- D. The best option is to configure CERTKILLER-SR25 to require Integrated Windows Authentication (IWA) as soon as users connect to the WSUS server.

**Answer: C**

**Explanation:**

To ensure that the traffic between the WSUS administrative website and the server administrator's computer is encrypted, you need to configure SSL encryption on the WSUS server website

Now that you have the necessary certificate, you must configure IIS to use it. To do so, expand the Default Web Site in the IIS Manager console and then right click on the WSUSAdmin virtual directory and select the Properties command from the resulting shortcut menu. You will now see the properties sheet for the WSUSAdmin virtual directory. Select the properties sheet's Directory Security tab and then click the Edit button that's found in the Secure Communications section. Select the Require Secure Channel (SSL) check box and click OK, Apply, and OK.

Reference : Applying Certificates to a WSUS Server / Enforcing SSL Encryption  
<http://www.windowsecurity.com/articles/Applying-certificates-WSUS-Server.html>

Part 2, Capture performance data (8 Questions)

**QUESTION NO: 235**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a domain controller named CERTKILLER-DC01. You have installed the Microsoft Network Monitor 3.0 on CERTKILLER-DC01 to do a security audit. During monitoring on the domain controller, while capturing data, you notice that some captured frames display host mnemonic names. These names resides in the Source and the Destination columns. However, some of the frames display IP addresses. You have received instructions from the CEO to display mnemonic host names.

What should you do?

- A. You should consider creating an exclusion policy using a filter and apply the filter to the capture.
- B. You should consider creating a new capture filter and apply the filter to the capture.
- C. You should consider populating the Aliases table and then apply the aliases to the capture.

D. You should consider enabling the Enable Conversations option and then recapture the data to a new file.

**Answer: C**

**Explanation:**

:

To display mnemonic host names instead of IP addresses for all the frames, you need to populate the Aliases table and apply the aliases to the capture. Aliases table display mnemonic host names.

In cases where you'd like to see the real IP address and a resolved name exists, turning off the aliases doesn't show you the real IP address.

Reference : Network Monitor/ SourceNetworkAddress and DestinationNetworkAddress  
<http://blogs.technet.com/netmon/>

#### **QUESTION NO: 236**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a Web server named CERTKILLER-SR11 that hosts shared documents. After you have installed two third party applications on CERTKILLER-SR11, the CertKiller.com employees report of unusual slow response times when using the shared documents. During the investigation you find out that CERTKILLER-SR11's processor is running at a 100 % capacity, when you used the real time monitoring. You need to collect more data to identify why the processors is running 100%.

What should you do?

- A. You should check see the percentage of processor capacity used by each application in Windows Reliability and Performance Monitor.
- B. You should track the processor usage with a counter log to.
- C. You should check the events log in the Windows Reliability and Performance Monitor.
- D. You should create an alert that will be triggered when processor usage exceeds 80 percent.

**Answer: A**

**Explanation:**

To gather additional data to diagnose the cause of the problem, you need to use the Resource View in Windows Reliability and Performance Monitor to see the percentage of processor capacity used by each application.

The Resource View window of Windows Reliability and Performance Monitor provides a real-time graphical overview of CPU, disk, network, and memory usage. By expanding each of these monitored elements, system administrators can identify which processes are using which resources. In previous versions of Windows, this real-time process-specific data was only available in limited form in Task Manager

Reference : Windows Reliability and Performance Monitor  
<http://technet.microsoft.com/en-us/library/cc755081.aspx>

#### QUESTION NO: 237

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. CertKiller.com contains a server named CERTKILLER-SR12.

CERTKILLER-SR12 consists of 10 logical drives, a new Data Collector Set, and is connected to a SAN. You have received instructions from management to automatically run a data archiving script on CERTKILLER-SR12. However, it should be done when the free space on any of the logical drives is below 30 %.

What should you do?

- A. The best option is to add the Performance counter data collector.
- B. The best option is to add the Security Event data collector.
- C. The best option is to add the Performance counter alert.
- D. The best option is to add the System configuration data collector

**Answer: C**

#### Explanation:

To automatically run a data archiving script if the free space on any of the logical drives is below 30 percent and to automate the script execution by creating a new Data Collector Set, you need to add the Performance counter alert.

The Performance counter alert creates an alert if a performance counter reaches a threshold that you specify.

You can configure your data collector set to automatically run at a scheduled time, to stop running after a number of minutes, or to launch a task after running. You can also configure your data collector set to automatically run on a scheduled basis. This is useful for proactively monitoring computers.

Reference : Creating a Snapshot of a Computer's Configuration with Data Collector Sets in Vista /

## How to Create Custom Data Collector Sets

[http://www.biztechmagazine.com/article.asp?item\\_id=241](http://www.biztechmagazine.com/article.asp?item_id=241)

**QUESTION NO: 238**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a network server named CERTKILLER-SR13. During a routine monitoring, you notice a security lapse in the CertKiller.com network. You then want to start a list of all DNS requests that was initiated by CERTKILLER-SR13. You then install the Microsoft Network Monitor 3.0 application on CERTKILLER-SR13 and set up the server to perform a security audit.

The traffic that was captured was saved on a file as CK\_data.cap. However, the size of the file was more than 1 GB. You need to create a file named CK-SR13CK\_data.cap from the existing capture file that contains only DNS -related data.

What should you do?

- A. The best option is to run the following command: `nmcap.exe /inputcapture data.cap /capture DNS /file CK-SR13CK_data.cap`.
- B. The best option is to apply a size restriction using a disk quota on the CK-SR13CK\_data.cap file.
- C. The best option is to capture filter DNS and the displayed frames should be saved as CK-SR13CK\_data.cap file.
- D. The best option is to add a new alias named DNS to the aliases table and thereafter save the file as CK-SR13CK\_data.cap.

**Answer: A**

**Explanation:**

NMCap also allows you to accept a capture file as input. This can be useful for cleansing your traces before you use them. Or you could also parse traffic by different ports or by IP addresses. The below given command allows you to create a file named CK-SR13CK\_data.cap to store only the DNS-related data after filtering it from data.cap file, which is a capture file.

The command `nmcap.exe /inputcapture data.cap /capture DNS /file CK-SR13CK_data.cap` file

Reference : Network Monitor / Cool NMCap trick, using another capture file as the input source  
<http://blogs.technet.com/netmon/Default.aspx?p=2>

**QUESTION NO: 239**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a domain controller named CERTKILLER-DC01. CERTKILLER-DC01 has the Microsoft Network Monitor 3.0 application installed. During the day, you have received a complaint that a workstation named CERTKILLER-WS123 is not able to obtain an IP configuration from the domain controller. On CERTKILLER-DC01, you then enabled P-mode to capture only the DHCP server-related traffic coming from CERTKILLER-DC01 and going to CERTKILLER-WS123. The network interface configuration for CERTKILLER-DC01 and going to CERTKILLER-WS123 is as seen in the exhibit:

You have received instructions from the CEO to capture the DHCP traffic between CERTKILLER-DC01 and CERTKILLER-WS123

What should you do?

- A. You should use IPv4. Address == 192.168.15.84 && DHCP to build a filter in the Network Monitor application.
- B. You should use IPv4 address == 192.168.2.1 && DHCP to build a filter in the Network Monitor application.
- C. You should use Ethernet Address == 0x00155ECD3E83 && DHCP to build a filter in the Network Monitor application.
- D. You should use Ethernet Address == 0x0015F2CD2AFB && DHCP to build a filter in the Network Monitor application.

**Answer: A**

**Explanation:**

:

To build a filter in the Network application to capture the DHCP traffic between CERTKILLER-DC01 and CERTKILLER-WS123, you need to use IPv4.Address == 192.168.15.84 && DHCP.

To define a filter, you need to specify IPv4, period, SourceAddress then the equal mark (twice) and the IP address (source). In order to fine tune a specific filter, you can combine several conditions in a specific filter using the AND (&&) and OR (||) logical operators. In this question you need to find the traffic originating from 192.168.15.84 that is DHCP related. Therefore you would use 192.168.15.84 && DHCP.

Reference : A Guide to Network Monitor 3.1 / Building a complex filter (or defining several

conditions)

<http://blogs.microsoft.co.il/blogs/erikr/archive/2007/08/29/A-Guide-to-Network-Monitor-3.1.aspx>

#### **QUESTION NO: 240**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a server named CERTKILLER-SR14. After you have installed a software application on CERTKILLER-SR14, you notice that the server has intermittent performance problems. You need to find out if the software application was installed.

What should you do?

- A. You should consider using the Network Monitor utility to see if the software application was installed.
- B. You should consider using the Data Collector Sets utility to see if the software application was installed.
- C. You should consider using the Reliability Monitor utility to see if the software application was installed.
- D. You should consider using the Stability Monitor utility to see if the software application was installed.

**Answer: C**

#### **Explanation:**

The Reliability Monitor will allow you to see when the application was installed.

#### **Incorrect Answers:**

- A: The Network monitor allows you to capture network traffic not when the installation was installed.
- B: The Data Collector Sets utility allows you to capture performance and data configuration.
- D: There is no Stability Monitor utility.

#### **QUESTION NO: 241**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

One morning you have received several complaint from the CertKiller.com users that the e-mail services are sluggish during peak and during after hours, the performance would be satisfactory.



You need to find out which resources are limiting performance by having performance data captured during the night and during the day to compare them.

What should you do? (Choose all that apply.)

- A. You should consider using the Network Security Health utility.
- B. You should consider using the Data Collector Sets utility.
- C. You should consider using the Reliability and Performance Monitor utility.
- D. You should consider using the Performance Monitor utility.

**Answer: B,D**

**Explanation:**

The Data Collector Sets utility will record the data performance. There after you can use the Performance Monitor utility to view the info. You can set the Data Collector Sets utility to record at day and at night. With this you can then review the reports with the Performance Monitor utility. The Performance Monitor utility on the other hand will allow you to view real-time data performance.

**Incorrect Answers:**

- A: The Network monitor allows you to capture network traffic.
- C: The Reliability Monitor will allow you to see when the application was installed.

**QUESTION NO: 242**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You are busy with the configuring and utilization of the Reliability Monitor. A CertKiller.com manager wants to know what can be stored in the Reliability Monitor.

What should your reply be to the manager?

- A. You should inform the manager that it contains information of device drivers which failed.
- B. You should inform the manager that it contains information of services which have stopped.
- C. You should inform the manager that it contains information of device drivers that are manually stopped.
- D. You should inform the manager that it contains information of applications which are uninstalled.

**Answer: A,D**

**Explanation:**

The Reliability Monitor will allow you to see when the application was installed and it also records the device driver failures.

**Incorrect Answers:**

B: The Reliability Monitor records the application failures, however not the errors within.

C: The Reliability Monitor will allow you to see when the application was installed and it also records the device driver failures. Part 3, Monitor event logs (6 Questions)

**QUESTION NO: 243**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains two domain controllers named CERTKILLER-DC01 and CERTKILLER-DC02. You then create a default subscription on CERTKILLER-DC01 and CERTKILLER-DC02 to configure Event forwarding and subscription. However, a CertKiller.com manager wants to know what event logs can be used to review the system events for CERTKILLER-DC02.

What should you reply?

- A. You should inform the manager that Performance Events log on CERTKILLER-DC02 can be used.
- B. You should inform the manager that System log on CERTKILLER-DC01 can be used.
- C. You should inform the manager that Forwarded Events log on CERTKILLER-DC01 can be used.
- D. You should inform the manager that Application log on CERTKILLER-DC02 can be used.

**Answer: C****Explanation:**

:

To review the system events for CERTKILLER-DC02, you need to view the Forwarded Events log on CERTKILLER-DC01, which is configured to centrally manage events.

The Event Collector service can automatically forward event logs to other remote systems, running Windows Vista or Windows Server 2008 on a configurable schedule. Event logs can also be remotely viewed from other computers or multiple event logs can be centrally logged and monitored agentlessly and managed from a single computer.

Reference : Event Viewer

[http://en.wikipedia.org/wiki/Event\\_View](http://en.wikipedia.org/wiki/Event_View)er

**QUESTION NO: 244**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com consists of a head quarters and a branch office. The branch office at TesCKig.com contains three server named CERTKILLER-SR11, CERTKILLER-SR12 and CERTKILLER-SR13. You are busy to configure the Event Logs subscription on CERTKILLER-SR11 to monitor CERTKILLER-SR12 and CERTKILLER-SR13. However, you notice that you cannot create a subscription on CERTKILLER-SR11.

What should you do? (Choose all that apply.)

- A. You should consider running the `wecutil cs subscription.xml` command on CERTKILLER-SR11.
- B. You should consider creating an event collector subscription configuration file called `subscription.xml` on CERTKILLER-SR11.
- C. You should consider running the ForwardedEvents log in a custom view and export the custom view to `subscription.xml` file.
- D. You should consider running the `wevtutil im subscription.xml` command on CERTKILLER-SR11.

**Answer: A,B**

**Explanation:**

:

To configure a subscription on CERTKILLER-SR11, you need to first create an event collector subscription configuration file and Name the file `subscription.xml`. You need to then run the `wecutil cs subscription.xml` command on CERTKILLER-SR11.

This command enables you to create and manage subscriptions to events that are forwarded from remote computers, which support WS-Management protocol. `wecutil cs subscription.xml` command will create a subscription to forward events from a Windows Vista Application event log of a remote computer at CertKiller.com to the ForwardedEvents log.

Reference : Wecutil

<http://technet2.microsoft.com/windowsserver2008/en/library/0c82a6cb-d652-429c-9c3d-0f568c78d54b1033.mspx?mfr=true>

**QUESTION NO: 245**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. CertKiller.com consists of a head quarters and a branch office. The branch office at CertKiller.com contains two server named CERTKILLER-SR12 and CERTKILLER-SR13.

You have configured the event subscription on CERTKILLER-SR12 and CERTKILLER-SR13 to collected and transferred events to CERTKILLER-SR12, using the HTTP protocol and choosing the normal option for the event delivery optimization setting. Though, none of the subscriptions worked. You need to make sure that the servers support event collectors?

What should you do?

- A. You should consider running the wecutil qc command on CERTKILLER-SR12  
You should consider running the winrm quickconfig command on CERTKILLER-SR13  
You should consider adding the CERTKILLER-SR12 account to the administrators group on CERTKILLER-SR13
- B. You should consider running the winrm quickconfig command on CERTKILLER-SR12  
You should consider adding the CERTKILLER-SR13 account to the administrators group on CERTKILLER-SR12
- C. You should consider running the wecutil qc command on CERTKILLER-SR13  
You should consider adding the CERTKILLER-SR13 account to the administrators group on CERTKILLER-SR12
- D. You should consider running the wecutil qc command on CERTKILLER-SR13  
You should consider running the winrm quickconfig command on CERTKILLER-SR12  
You should consider adding the CERTKILLER-SR13 account to the administrators group on CERTKILLER-SR12

**Answer: A**

**Explanation:**

: To collect events from CertKillerServer2 and transfer them to CERTKILLER-SR12, you need to first run the wecutil qc command on CERTKILLER-SR12. This command enables you to create and manage subscriptions to events that are forwarded from remote computers.

Then you need to run the winrm quickconfig command on CERTKILLER-SR13. WinRM is required by Windows Event Forwarding as WS-Man is the protocol used by WS-Eventing. Group Policy can be used to enable and configure Windows Remote Management (WinRM or WS-Man) on the Source Computers. With WinRM, Group Policy can be used to configure Source Computers (Clients) to forward events to a collector (or set of collectors).

Finally, you need to add the CERTKILLER-SR12 account to the administrators group on

CERTKILLER-SR13 so that access rights can be granted to the collector system on the forwarding computer.

Reference : Quick and Dirty Large Scale Eventing for Windows

<http://blogs.technet.com/otto/archive/2008/07/08/quick-and-dirty-enterprise-eventing-for-windows.aspx>

Reference : Collect Vista Events

[http://www.prismmicrosys.com/newsletters\\_june2007.php](http://www.prismmicrosys.com/newsletters_june2007.php)

### QUESTION NO: 246

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains two servers named CERTKILLER-DC01 and CERTKILLER-SR13 respectively. You receive instructions from the CIO to set up CERTKILLER-DC01 to collect events from CERTKILLER-SR13.

What should you do?

- A. The best option is to run `net localgroup "Event Log Readers" CERTKILLER-SR13@CertKiller.com /add` at the forwarding computer.
- B. The best option is to run `net localgroup "Event Log Readers" CERTKILLER-DC01@CertKiller.com /add` at the collecting computer.
- C. The best option is to run `winrm quickconfig` at CERTKILLER-DC01.
- D. The best option is to run `wecutil qc` at the collecting computer.

**Answer: D**

#### Explanation:

You should run the command `wecutil qc` at the forwarding computer. You can configure it to automatically configure the computer to collect the events.

#### Incorrect Answers:

- A: You should not add the forwarding computer to the group. That group only consists of the collecting computers.
- B: You cannot run the `net localgroup "Event Log Readers" CERTKILLER-DC01 @CertKiller.com /add` command at the forwarding computer.
- C: You cannot run the `winrm quickconfig` command at the forwarding computer.

**QUESTION NO: 247**

You work as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains two servers named CERTKILLER-DC02 and CERTKILLER-SR17. You need to set up CERTKILLER-DC01 to collect subscription events from CERTKILLER-SR17 and run the selected command on the forwarding system.

What should you do? (Choose TWO.)

- A. The best option is to run net localgroup "Event Log Readers" CERTKILLER-DC01@CertKiller.com /add at the forwarding computer.
- B. The best option is to run net localgroup "Event Log Readers" CERTKILLER-SR13@CertKiller.com /add at the upstream server.
- C. The best option is to run wecutil qc at the forwarding computer.
- D. The best option is to run winrm quickconfig at the forwarding computer.
- E. The best option is to run wecutil cs subscription.xml on the forwarding computer.

**Answer: A,D**

**Explanation:**

You can run the net localgroup "Event Log Readers" CertKillerDC1 @CertKiller.msft /add and the winrm quickconfig command on the collecting computer.

**Incorrect Answers:**

- B: You cannot run the localgroup "Event Log Readers" CertKillerCLIENT1 @CertKiller.msft /add command at an upstream server.
- C: You cannot run the winrm quickconfig command at the forwarding computer.

**QUESTION NO: 248**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

A CertKiller.com manager named Mia Hamm wants to know which configuration tool can be used to configuring event subscription for updating always.

What should you reply?

- A. You should inform the manager that the Wecutil configuration utility can be used.
- B. You should inform the manager that the Net command line utility can be used.
- C. You should inform the manager that the Event collector subscription configuration utility can be used.
- D. You should inform the manager that the Event Viewer console can be used.

**Answer: A**

**Explanation:**

You can use the Wecutil configuration utility to customize a subscription interval.

**Incorrect Answers:**

- B: The Net command line utility is used to stop and start services, not to configure a subscription interval
- C: The WinRM configuration utility is used to configure the forwarding computer.
- D: You can use the Event Viewer to configure aspects of the subscription but not to customize a subscription interval. Part 4, Gather network data (5 Questions)

**QUESTION NO: 249**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a domain controller named CERTKILLER-DC01 that has Microsoft Network Monitor 3.0 installed. You have received instructions from the CEO to execute a security audit on CERTKILLER-DC01 without impacting on the normal business day activities. Consequently you need to execute the audit between 22:00 and 07:00 the following day and save it to the C:\LDAPData.cap file.

You then create a scheduled task and added a new 'Start a program action' to it. You need to put the application name and arguments to the new action.

How can you accomplish it? (Choose TWO.)

- A. You should consider adding netmon.exe as the application name.
- B. You should consider adding nmcap.exe as the application name.
- C. You should consider adding nmconfig.exe as the application name.
- D. You should consider providing the /networks \*/capture LDAP /file C:\LDAPData.cap /stopwhen /timeafter 9 hours as conditions.
- E. You should consider providing the /networks \* /capture LDAP /file C:\LDAPData.cap /stopwhen /timeafter 9 hours as arguments.



**Answer: B,E**

**Explanation:**

:

The "/network", defines which network interface we are capturing on. In this case, we say "\*" for all interfaces. The next parameters "/capture /file %1" tells NMCap what to filter out. In this case it tells to filter LDAP to C:\LDAPData.cap.

The last part of NMCap, the "/stopwhen" directive, that allows it to determine when NMCap should stop capturing. So we pass it a "/frame" parameter which tells it to stop the capturing after 9 hours and exit NMCap.

Reference : Network Monitor/ Stop That Capture: How does NMCap get stopped?

<http://blogs.technet.com/netmon/Default.aspx?p=2>

**QUESTION NO: 250**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains a new server named CERTKILLER-SR20 that has the Web Server (IIS) role installed on it. However, CERTKILLER-SR20 has no Reliability Monitor data at present; furthermore the system stability share is outdated. You need to set up CERTKILLER-SR20 to collect the reliability monitor data.

What should you do?

- A. The best option is to run Network Security Health Validator on the CERTKILLER-SR20.
- B. The best option is to configure the Remote Registry service to start automatically on the CERTKILLER-SR20.
- C. The best option is to configure the Task scheduler service to start automatically on the CERTKILLER-SR20.
- D. The best option is to configure the Windows Reliability and Performance Monitor to start automatically on the CERTKILLER-SR20.

**Answer: C**

**Explanation:**

To configure the CertKillerServer1 to collect the reliability monitor data, you need to configure the Task scheduler service to start automatically.

Reliability Monitor uses data provided by the RACAgent scheduled task, a pre-defined task that

runs by default on a new installation of Windows Vista. The seamless integration between the Task Scheduler user interface and the Event Viewer allows an event-triggered task to be created with just five clicks.

In addition to events, the Task Scheduler in Windows Vista / Server 2008 supports a number of other new types of triggers, including triggers that launch tasks at machine idle, startup, or logon. Because you need Task Scheduler to collect reliability monitor data, you need to you need to configure the Task scheduler service to start automatically.

Reference : Network Monitor 3.1 OneClick ... now what? / Task Scheduler Changes in Windows Vista and Windows Server 2008 - Part One

<http://blogs.technet.com/askperf/>

Reference : What allows the Reliability Monitor to display data?

[http://www.petri.co.il/reliability\\_monitor\\_windows\\_vista.htm](http://www.petri.co.il/reliability_monitor_windows_vista.htm)

#### QUESTION NO: 251

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

CertKiller.com contains two workstations named CERTKILLER-WS201 and CERTKILLER-WS202. You have received instructions from the CIO to capture the communications between the two workstations with the Network Monitor.

What should you do?

- A. The best option is to use the Network Monitor with enable P-Mode on CERTKILLER-WS202. You should also connect CERTKILLER-WS201 to the same hub as CERTKILLER- WS202 and CERTKILLER- WS203 to a Layer 2 switch on a separate network.
- B. You should use the Network Monitor with enable P-Mode on CERTKILLER-WS202. You should also connect CERTKILLER-WS201 to the same hub as CERTKILLER- WS203 and CERTKILLER- WS202 to a different network.
- C. You should run Network monitor on CERTKILLER-WS201 as CERTKILLER- WS202 has no Network Monitor installed.
- D. You should use the Network Monitor with enable P-Mode on CERTKILLER-WS202. You should also connect CERTKILLER-WS201 to the same Layer2 switch as CERTKILLER- WS203 and CERTKILLER- WS202 on a test network.

**Answer: B,C**

**Explanation:**

You can capture communications despite of the kind of network infrastructure. Furthermore, the computers that are connected to the hub can see the other communications. If the P-Mode enabled, the computer that is running the Network Monitor will capture the communications that are sent to CERTKILLER-WS201.

**Incorrect Answers:**

A: The Layer 2 switches will not send the computer that is running the Network Monitor communications to CERTKILLER-WS201 and CERTKILLER-WS202. The port of the Network Monitoring computer must be connected as a network monitoring port.

D: You need to connect the computer that is running the Network Monitor, to the same hub.

**QUESTION NO: 252**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008. You received instructions from the CIO to investigate the performance of the network. Consequently you need to create a Network Monitor capture file with a command prompt to monitor the performance of the Windows Server 2008 network.

What should you do?

- A. You should use NMCap.
- B. You should use Nmconfig.
- C. You should use Netmon.
- D. You should use PerfMon.

**Answer: A****Explanation:**

You should use the NMCap command line utility. This will allow you to capture communication from a 'run as' and save as a .CAP file.

**Incorrect Answers:**

B: You should not use the Nmconfig command line utility. This installs and uninstalls the Network Monitor.

C: You should not use the Netmon command line utility. This is a Network Monitor executable file and it cannot be run from the command prompt.

D: You should not use the Nmwifi command line utility. This configures wireless scanning options.

**QUESTION NO: 253**

You are employed as an enterprise administrator at CertKiller.com. The CertKiller.com network consists of a single Active Directory domain named CertKiller.com. All servers on the CertKiller.com network run Windows Server 2008.

You have received complaints from a CertKiller.com user named Mia Hamm her workstation, 169.254.15.84, does not retrieve Web pages from the CertKiller.com server. During the investigation the problem, you instruct Mia Hamm to submit a request. Doing this, you can capture traffic using the network monitor. However, you captured hundreds of other requests. However, you only want Mia Hamm's submitted request.

What should you do?

- A. You should consider using the display filter HTTP || IPv4.Address == 169.254.15.84.
- B. You should consider using the display filter HTTP || ipv4.SourceAddress == 169.254.15.84.
- C. You should consider using the display filter HTTP && IPv4.SourceAddress == 169.254.15.84.
- D. You should consider using the display filter HTTP && IPv4.Address == 169.254.15.84.

**Answer: D**

**Explanation:**

To filter the display to view communications sent from the client computer, you should use the display filter HTTP && IPv4.Address == 169.254.15.84. This will show the HTTP communications and the other communications from 169.254.15.84.

**Incorrect Answers:**

- A: The filter will only show all the HTTP communications to and from 169.254.15.84 and where it came from.
- B: This will only show the HTTP communications from 169.254.15.84.
- C: The filter will only show all the HTTP communications to and from 169.254.15.84.