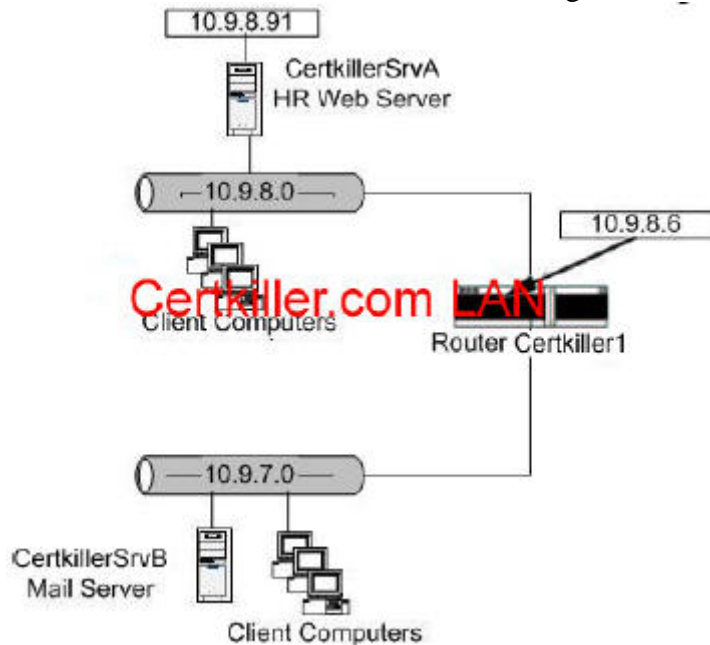


## QUESTION 1

You are the network administrator for Certkiller.com. A server named CertkillerSrvA functions as an intranet Web server for the human resources (HR) department. A server named CertkillerSrvB is a Microsoft Exchange 2000 Server mail server. The network configuration is shown in the exhibit.



CertkillerSrvA contains confidential documents that must be accessed daily by users on only the 10.9.8.0 subnet. All users must be able to connect to CertkillerSrvB. You want to configure the TCP/IP properties of CertkillerSrvA to prevent any computer in the 10.9.7.0 subnet from establishing a session with CertkillerSrvA. What should you do?

- A. Configure CertkillerSrvA port filtering to block TCP port 80.
- B. Use Internet Connection Firewall (ICF) with no services selected.
- C. Configure CertkillerSrvA with a default gateway address of 10.9.8.6.
- D. Configure CertkillerSrvA with no default gateway address.

Answer: D

Explanation:

We have a routed subnet here. For clients in the 10.9.7.0 network to communicate with CertkillerSrvA, they must be configured with a default gateway address (the address of the router), which they have. However, to establish a session with CertkillerSrvA, CertkillerSrvA must also be configured with a default gateway address (the address of the router), so that CertkillerSrvA can communicate with the clients in the 10.9.7.0 network. By removing the default gateway from CertkillerSrvA, we can disable this communication. CertkillerSrvA will still be able to communicate with clients on the 10.9.8.0 network.

Incorrect Answers:

- A: Port 80 is used by the web server. We shouldn't block it, otherwise clients in the 10.9.8.0 network will not be able to communicate with the server on the default port.
- B: This won't prevent any internal network communications.
- C: 10.9.8.6 is the correct default gateway for the server. We need to remove the default gateway setting.

---

## QUESTION 2

You are the network administrator for Certkiller. The network consists of a single Active Directory domain

Certkiller.com. The domain contains 25 Windows server 2003 computers and 5,000 Windows 2000 Professional computers. You install and configure Software Update Services (SUS) on a server named CertkillerSrv. All client computer accounts are in the Clients organizational unit (OU). You create a Group Policy object (GPO) named SUSupdates and link it to the Clients OU. You configure the SUSupdates GPO so that client computers obtain security updates from CertkillerSrv. Three days later, you examine the Windowsupdate.log file on several client computers and discover that they have downloaded Windows security updates from only ndowsupdate.microsoft.com. You need to configure all client computers to download Windows security updates from CertkillerSrv. What should you do?

- A. Open the SUSupdates GPO and configure the Configure Automatic Update policy to assign the Auto download and notify for install setting for Windows security updates.
- B. Open the SUSupdates GPO and configure the Configure Automatic Update policy to assign the Auto download and schedule the install setting for Windows security updates.
- C. Create software distribution policy for the SUSupdates GPO that assigns the package WUAU22.msi to all client computers. Restart all client computers.
- D. On all client computers, configure the UseWUSever registry value to enable Automatic Updates to use CertkillerSrv.

Answer: D

Explanation:

The Windows 2000 clients aren't able to use the GPO setting that configures which server they should receive their updates from. You can import a template file to correct this problem, but that isn't listed as an answer. The only answer that will work is to edit the registry of the client computers to configure them to receive their updates from CertkillerSrv.

Incorrect Answers:

- A: This won't affect which server the clients download the updates from.
- B: This won't affect which server the clients download the updates from.
- C: WUAU22.msi is the automatic updates client software. The clients in this case already have this installed (it comes as part of Windows 2000 Service Pack 3).

Reference:

<http://www.jsiinc.com/SUBL/tip5800/rh5809.htm>

---

### QUESTION 3

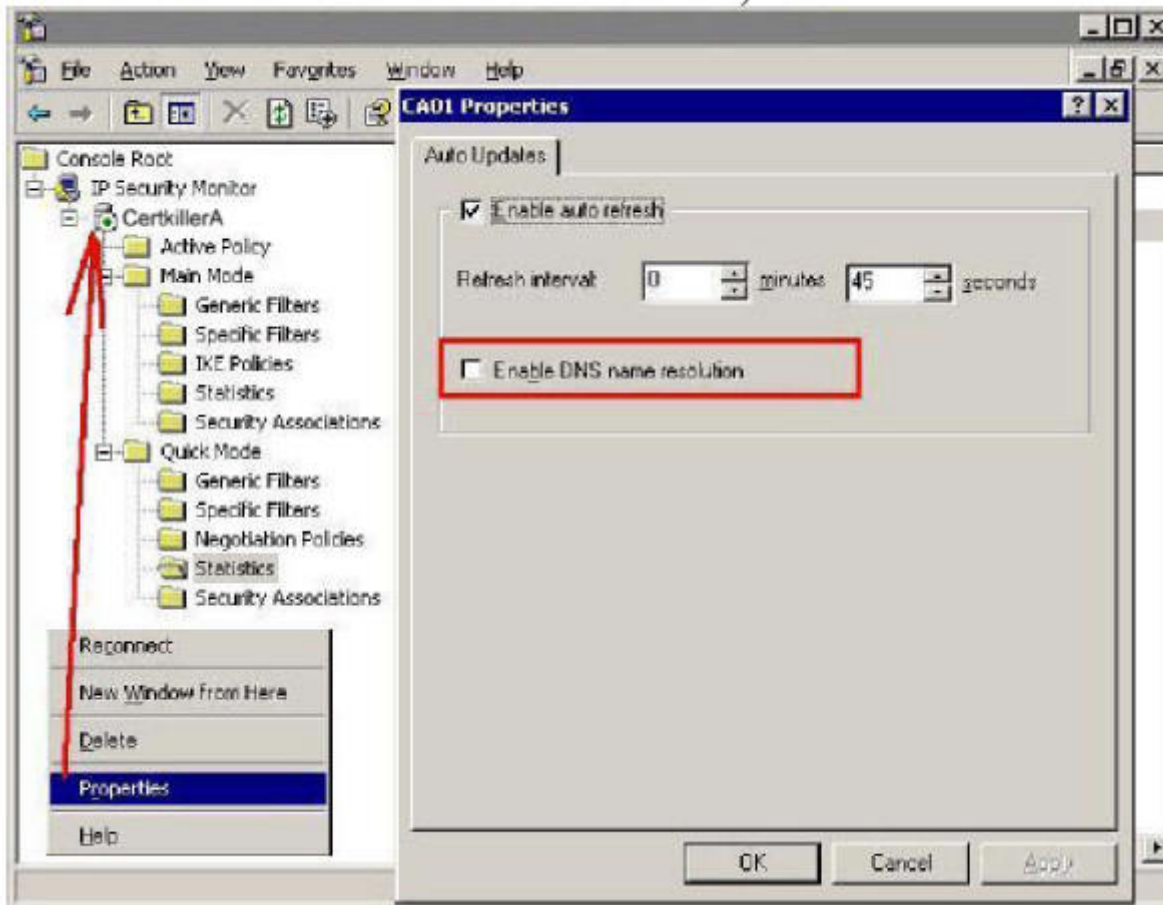
You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. The domain contains Windows Server 2003 computers, Windows XP Professional computers, and Windows 2000 Professional computers. An IPSec policy is assigned to a server named CertkillerA. By using the IP Security Monitor console on CertkillerA, you verify the IPSec communication connections, and you notice that all computers that have established security associations (SAs) with CertkillerA are displayed by their IP addresses. You want computers that have established SAs with CertkillerA to be displayed in IP Security Monitor by a fully qualified domain name (FQDN). What should you do on CertkillerA?

- A. In the assigned policy, add a new rule that filters all TCP and UDP traffic on port 53. Configure the filter action to permit unsecured IP packets to pass through.
- B. Open the IP Security Monitor console and configure the properties of CertkillerA to enable the Enable DNS name resolution option.
- C. From a command prompt, run the netsh ipsec static show all command.
- D. From a command prompt, run the netsh ipsec dynamic show all command.

Answer: B

Explanation:

We need to check the Enable DNS Resolution on the Server properties of IPSEC Monitor (the PTR records in DNS will resolve the IP addresses to host names).

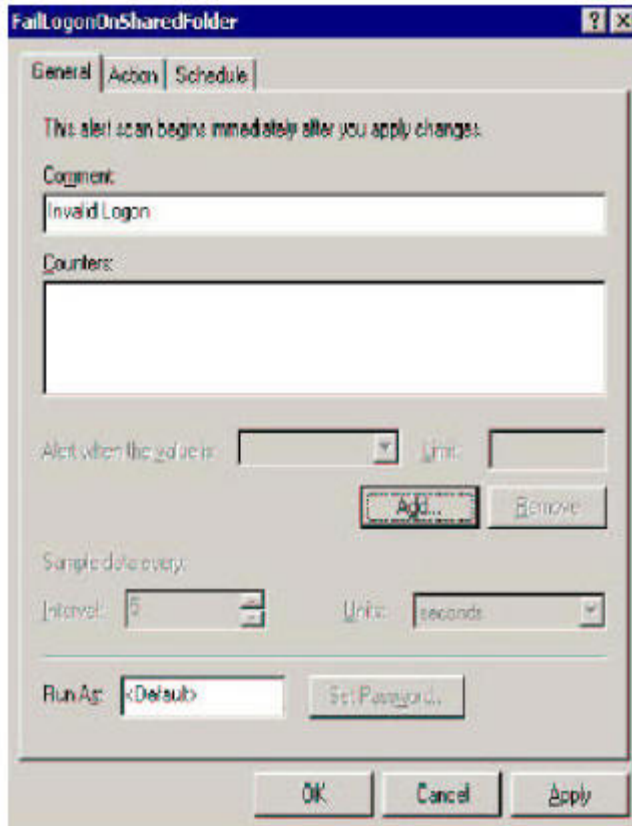


---

#### QUESTION 4

You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. The domain contains Windows Server 2003 domain controllers and Windows XP Professional computers. A server named CertkillerSrv7 hosts a shared folder. You want to use System Monitor to configure monitoring of the server performance object to alert you when invalid logon attempts are made to the shared folder. You want to monitor only events that are associated with invalid logons. How should you configure the alert?

To answer, drag one or more appropriate instances of the server performance object to the alter interface.



## Server Counter Objects

Sessions Forced Off

Errors Logon

Errors System

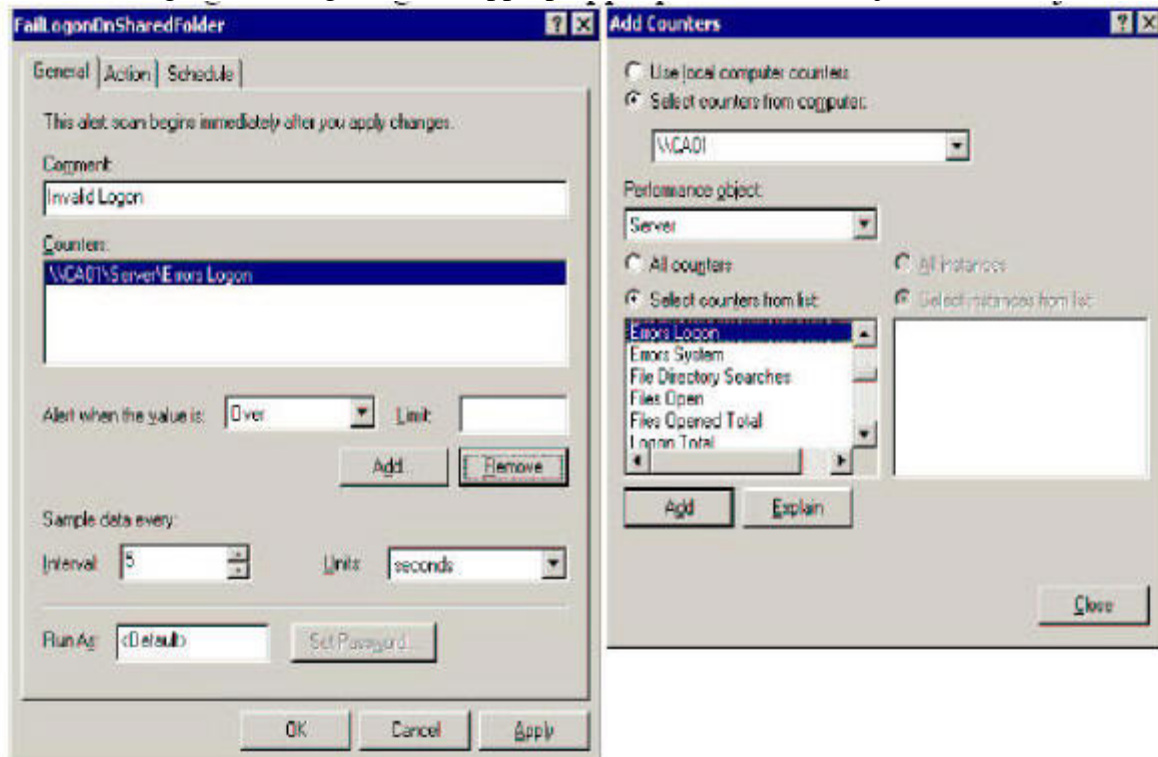
Errors Acces Permissions

Errors Granted Access

Sessions Errored Out

Error Access Permissions

Answer: Drag "Errors Logon" to the appropriate location. Server Object and Counter Errors Logon



Explanation:

When a remote network resource is connected to by using a UNC name, the user's credentials must be validated.

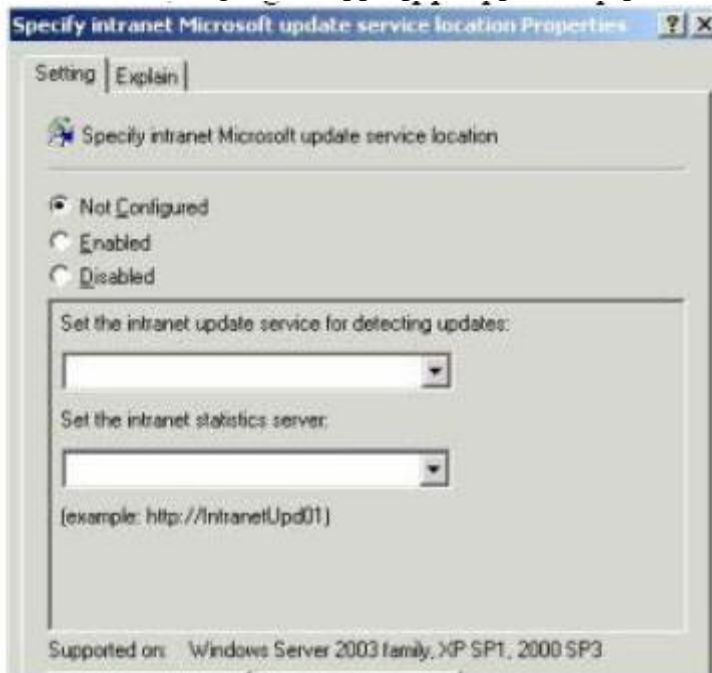
A UNC connection works through Multiple UNC Provider (MUP) by using Server Messaging Blocks (SMBs). An SMB called SESSION SETUP and X is used for the connection, and at that time the user's credentials are passed to the network resource. If the resource is a domain controller that maintains the user account, then the validation will occur locally on that computer. However, if the resource must use pass-through authentication to validate the user, the secure channel mechanism listed earlier in this article is used. The network resource will request a validation of the user from its domain controller, and if the user's credentials are not valid, the domain controller will return an error to the network resource. Also, the domain controller will increment its usri3\_bad\_pw\_count for that user. This will all take place transparently to the client workstation that originated the request. The network resource will return a message to the client workstation. That message will have the NT status code 0xC000006D, STATUS\_LOGON\_FAILURE

---

### QUESTION 5

You are the network administrator for Certkiller. The network contains Windows Server 2003 computers and Windows XP Professional computers. You install Software Update Services on a server named Certkiller3. You create a new Group Policy object (GPO) at the domain level. You need to properly configure the GPO so that all computers receive their updates from Server1. How should you configure the GPO?

To answer, configure the appropriate option or options in the dialog box.



Answer: Select the "Enabled" radio button. In the "Set the intranet update service for detecting updates" box, enter the name of the server; in this case you would enter http://CertkillerA. You should also enter http://CertkillerA as the address of the intranet statistics server.

---

### QUESTION 6

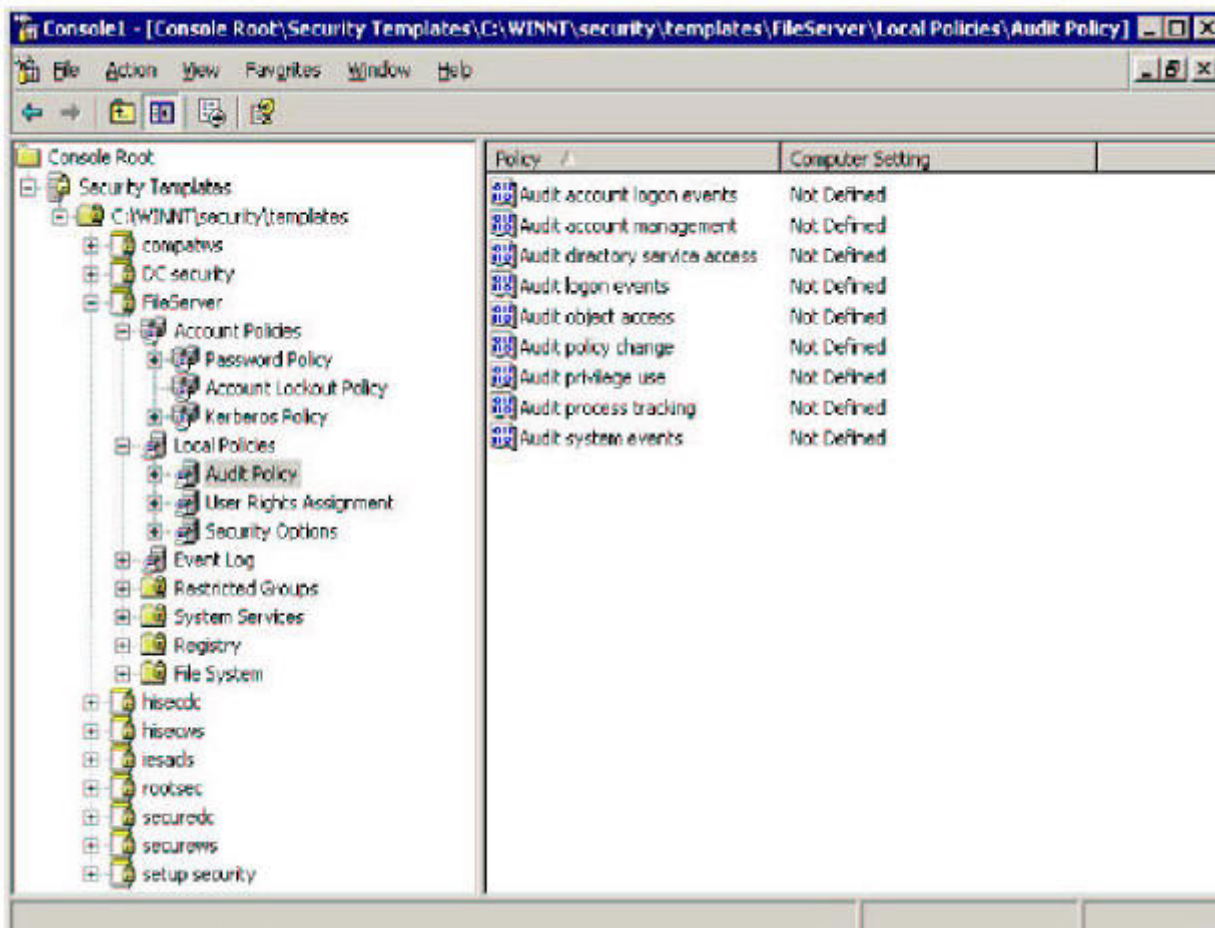
You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. The domain contains Windows Server 2003 computers and Windows XP Professional computers. The written company security policy states that the audit policy on all file servers in the domain must have the ability to audit failure events for user access to files and folders. You create a custom security template named fileserver.

You need to configure the fileserver security template to enforce the written security policy of Certkiller for all

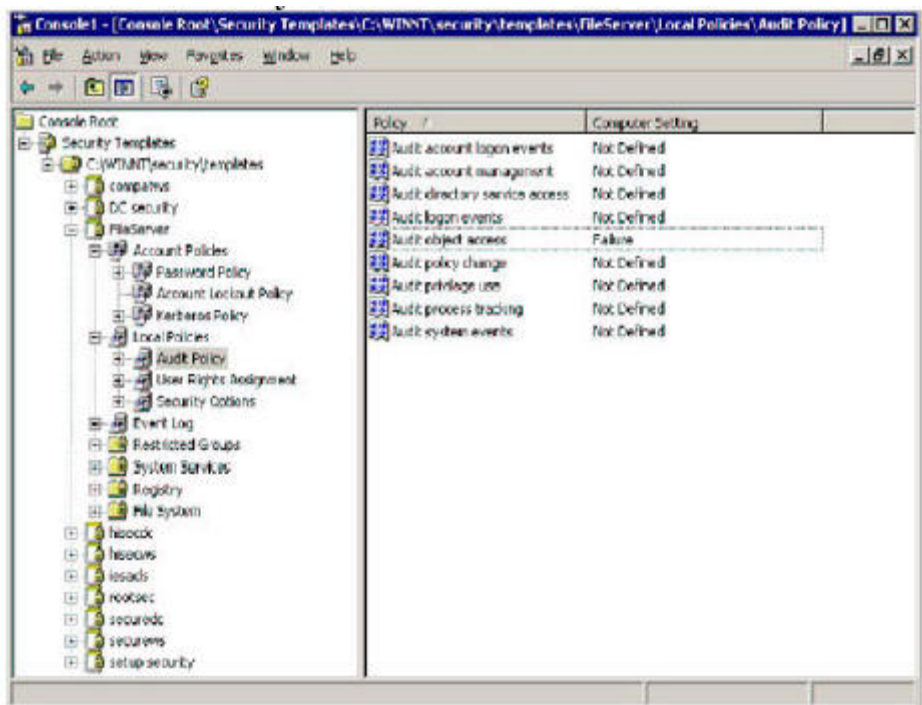


file servers. Which policy or policies should you modify?

To answer, select the appropriate audit policy or policies in the list of audit policies.



Answer: Audit object access.



## Explanation

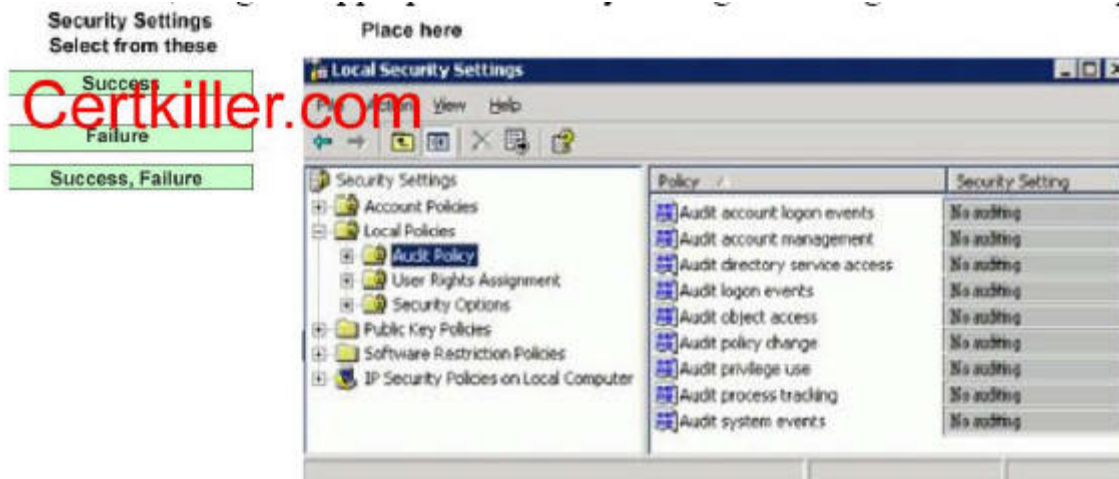
### Audit object access

This security setting determines whether to audit the event of a user accessing an object -for example, a file, folder, registry key, printer, and so forth-that has its own system access control list (SACL) specified. If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified. To set this value to No auditing, In the Properties dialog box for this policy setting, select the Define these policy settings check box and clear the Success and Failure check boxes. Note that you can set a SACL on a file system object using the Security tab in that object's Properties dialog box. Default: No auditing.

## QUESTION 7

You are the network administrator for Certkiller. A server named CertkillerSrvC functions as a local file server. CertkillerSrvC contains several extremely confidential files. The company's security department wants all attempts to access the confidential files on CertkillerSrvC to be recorded in a log. You need to configure the local security policy on CertkillerSrvC to give you the ability to comply with the security department's requirements. No other auditing should be configured. What should you do?

To answer, drag the appropriate security setting or settings to the correct policy or policies.



Answer:



Explanation:

Audit object access

This security setting determines whether to audit the event of a user accessing an object -for example, a file, folder, registry key, printer, and so forth-that has its own system access control list (SACL) specified. If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified. We should audit success and failure to log all attempts to access the files.

## QUESTION 8

You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The domain contains 10 Windows Server 2003 computers. The domain controllers are also configured as DNS server. Each DNS server hosts an Active Directory- integrated forward lookup zone named Certkiller.com. The DNS servers are also configured with a reverse lookup zone named 192.168.1.x Subnet. The DHCP server is configured with a scope that has the following properties:

- An IP address range from 192.168.1.1 - 192.168.1.254
- A subnet mask of 255.255.255.0
- An exclusion range from 192.168.1.1 - 192.168.1.55
- Scope options that include the assignment of a DNS server and a WINS server. The existing servers have



static IP addresses within the range of 192.168.1.1 - 192.168.1.10. You assign a static IP address to a new UNIX server named Server1. You need to create a new host (A) resource record for Server1. In addition, you need to ensure that the DNS servers will respond to reverse lookup queries against the IP address for Server1. You also need to maximize the security and availability of the A record for CertkillerSrv13. What should you do?

To answer, configure the appropriate option or options in the dialog box, and drag the appropriate IP address to the correct location.

IP Addresses Select from these	Dialog Box Place here
<div>192.168.1.0</div> <div>192.168.1.1</div> <div>192.168.1.25</div> <div>192.168.1.58</div> <div>192.168.1.255</div>	 <p>The 'New Host' dialog box is shown. The 'Name' field contains 'CertkillerSrv13'. The 'Fully qualified domain name (FQDN)' field contains 'CertkillerSrv13 Certkiller.com'. The 'IP address' field is empty. The 'Create associated pointer (PTR) record' checkbox is checked.</p>

Answer:

IP Addresses Select from these	Dialog Box Place here
<div>192.168.1.0</div> <div>192.168.1.1</div> <div>192.168.1.58</div> <div>192.168.1.255</div>	 <p>The 'New Host' dialog box is shown. The 'Name' field contains 'CertkillerSrv13'. The 'Fully qualified domain name (FQDN)' field contains 'CertkillerSrv13 Certkiller.com'. The 'IP address' field contains '192.168.1.25', which is highlighted with a green box. The 'Create associated pointer (PTR) record' checkbox is checked.</p>

Explanation:

192.168.1.0 & 192.168.1.255 are broadcast addresses, and would not be used.

192.168.1.1 - existing servers are 1-10, so this address is already in use.

192.168.1.58 - is already in the scope (remember that 1-55 are excluded, so 56-254 are dynamic and can't be used unless a reservation is set).

192.168.1.25 - is the only usable & available address left!

---

## QUESTION 9

You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. All domain controllers have the DNS service installed. You configure a new UNIX server to act as a secondary DNS server that is authoritative for the DNS zone. You create a host (A) record for the UNIX

server in the DNS zone. You configure the DNS zone to allow zone transfers to all servers. You need to configure the DNS zone to accommodate the new UNIX server. What should you do?

- A. Add a name server (NS) resource record for the UNIX server to the DNS zone.
- B. Add the UNIX server to the start of authority (SOA) resource record for the DNS zone.
- C. Add a global service locator (SRV) resource record that includes the UNIX server as a host.
- D. Add a LDAP service locator (SRV) resource record that includes the UNIX server as a host.

Answer: A

Explanation:

When adding DNS servers to the domain, you must add an NS (Name Server) record to the zone. NS.

Description: Used to map a DNS domain name as specified in owner to the name of hosts operating DNS servers specified in the name\_server\_domain\_name field. Syntax: owner ttl IN NS name\_server\_domain\_name.

Example: example.microsoft.com. IN NS nameserver1.example.microsoft.com.

---

### QUESTION 10

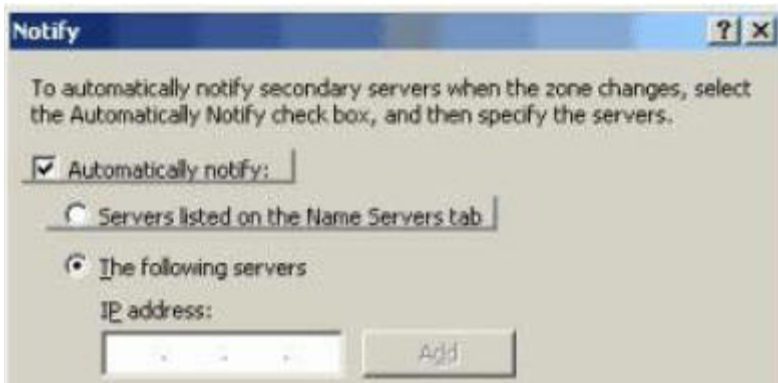
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The domain DNS servers are configured as shown in the following table.

Server name	IP address	Server operating system	Server role	DNS role
Certkiller1	10.10.1.222	Windows Server 2003	Domain Controller	Standard primary
Certkiller2	10.10.3.126	Windows 2000 Server	Member server	Standard secondary
Certkiller3	10.10.2.241	Windows Server 2003	Domain controller	Standard secondary
Certkiller4	10.10.4.192	UNIX	Not applicable	Standard secondary
Certkiller5	10.10.6.245	Windows Server 2003	Domain controller	Standard secondary

You uninstall DNS from Certkiller2 and reconfigure Certkiller2 as a file server. Then you reconfigure Certkiller4 as a caching-only server. Next, you reconfigure the domain controllers to use Active Directory-integrated DNS zones. You need to eliminate unnecessary zone transfer activity on the network.

What should you change in the Notify dialog box?

To answer, select the setting or settings that need to be changed. Select the IP address of addresses that need to be removed from the list.





Answer: Remove all the addresses.

Explanation:

The remaining servers are domain controllers hosting active directory integrated zones. The information in an active directory integrated zone is automatically replicated to every domain controller in the domain.

Note:

You may need to uncheck the Automatically notify: box since notification is no longer required. Zone transfers are no longer performed when ALL the servers are Active Directory Integrated zones. This is because zone transfer is now done via Active Directory replication.

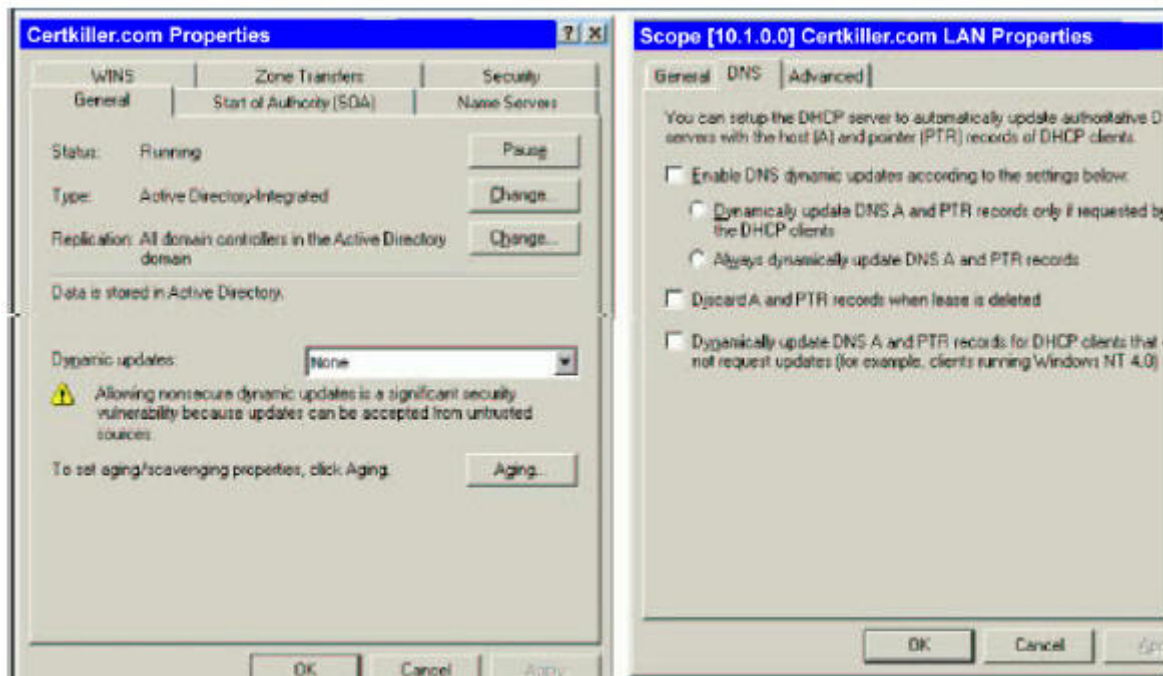
---

### QUESTION 11

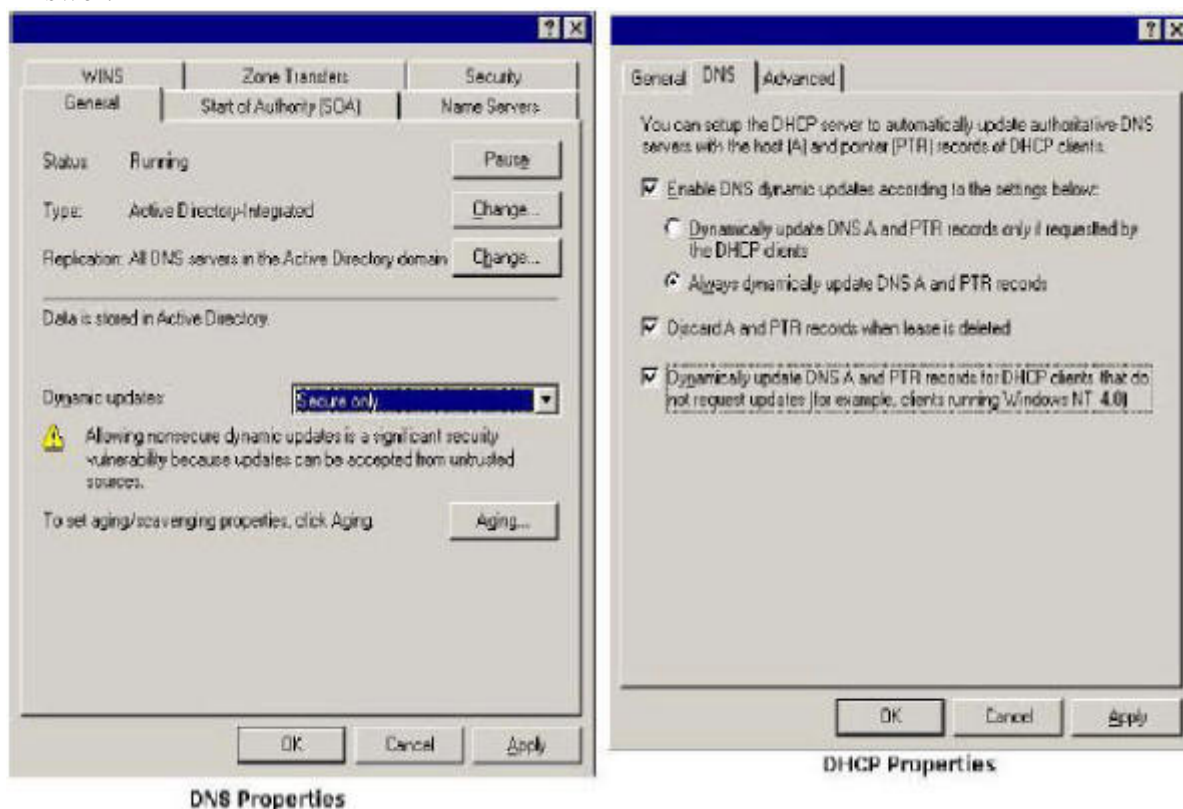
You are the network administrator for Certkiller. All network servers run either Windows Server 2003, Windows 2000 Server, or Windows NT Server 4.0. All client computers run either Windows XP Professional, Windows 2000 Professional, Windows NT Workstation 4.0, or Windows 98. The network consists of an Active Directory domain named Certkiller.com. All domain controllers in the domain run Windows Server 2003. All domain controllers also have the DNS service installed and host and Active Directory-integrated zone named Certkiller.com. A Windows Server 2003 member server assigns IP addresses to all computers in the company. All IP addresses are assigned from the 10.1.0.0/24 scope. All computers in the company must always be registered automatically in the Certkiller.com zone, regardless of the local TCP/IP configuration settings. Only computers that have valid computer accounts in the Active Directory domain must be able to register host (A) records in the zone. If a computer is removed from the network, the associated name registration must be removed from DNS. You are configuring the Certkiller.com DNS zone and the 10.1.0.0/24 DHCP scope to comply with the stated requirements.

Which configuration settings should you use?

To answer, configure the appropriate option or options in the dialog boxes.



Answer:

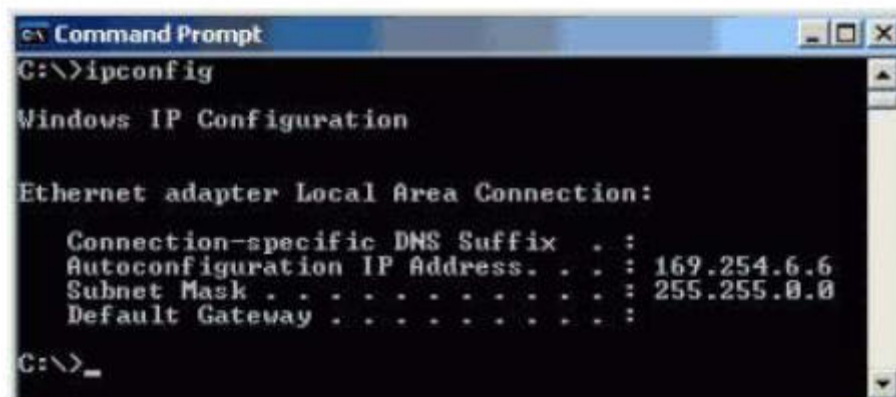


## QUESTION 12

You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. You configure a new Windows Server 2003 file server named CertkillerSrv1. You restore user files from a tape backup, and you create a logon script that maps drive letters to shared files on



CertkillerSrv1. Users report that they cannot access CertkillerSrv1 through the drive mappings you created. Users also report that CertkillerSrv1 does not appear in My Network Places. You log on to CertkillerSrv1 and confirm that the files are present and that the NTFS permissions and share permissions are correct. You cannot access any network resources. You run the ipconfig command and see the following output.



```
Command Prompt
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.6.6
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

C:\>_
```

You need to configure the TCP/IP properties on CertkillerSrv1 to resolve the problem. What should you do?

- A. Add Certkiller.com to the DNS suffix for this connection field.
- B. Configure the default gateway.
- C. Configure the DNS server address.
- D. Configure a static IP address.

Answer: D

Explanation:

The IP address shown in the exhibit is an APIPA (automatic private IP addressing) address. This means that the server is configured to use DHCP for its IP configuration but is unable to contact a DHCP server (a likely cause for this is that there isn't a DHCP server on the network). We can fix the problem by configuring a static IP address in the same IP range as the rest of the network.

Incorrect Answers:

- A: A DNS suffix isn't necessary.
- B: A default gateway isn't necessary unless this is a routed network.
- C: The server not having a DNS server address wouldn't prevent clients connecting to the server.

---

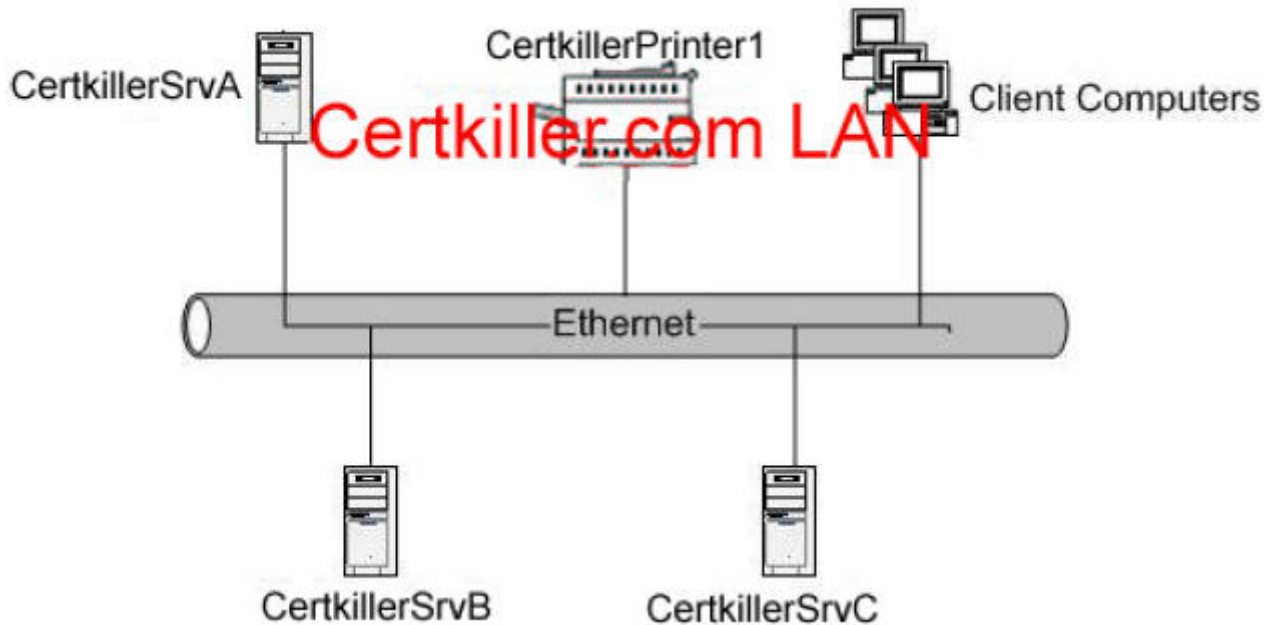
### QUESTION 13

You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The network contains 100 Windows 2000 Professional computers and three Windows Server 2003 computers. Information about the three servers is shown in the following table.

Name	Operating system	Roles
CertkillerSrvA	Windows Server 2003	Domain controller, primary DNS server
CertkillerSrvB	Windows Server 2003	Domain controller, WINS server
CertkillerSrvC	Windows 2000 Advanced Server	Member server, DHCP server

You add a network interface print device named CertkillerPrinter1 to the network. You manually configure the IP address for CertkillerPrinter1. CertkillerPrinter1 is not currently registered on the DNS server. The relevant portion of the network is shown in the exhibit.





You need to ensure that client computers can connect to CertkillerPrinter1 by using its name. What should you do?

- A. On CertkillerSrvA, add an alias (CNAME) record that references CertkillerPrinter1.
- B. In the Hosts file on CertkillerSrvC, add a line that references CertkillerPrinter1.
- C. On CertkillerSrvA, add a service locator (SRV) record that reference CertkillerPrinter1.
- D. On CertkillerSrvA, add a host (A) record that references CertkillerPrinter1.
- E. In the Hosts file on CertkillerSrvB, add a line that references CertkillerPrinter1.

Answer: D

Explanation:

The clients' printer software needs to know the IP address of the printer. For this, we can simply enter a host (A) record in the DNS zone. An A record maps a hostname to an IP address.

Incorrect Answers:

A: An alias (CNAME) can only point to an A record. We need to create the A record. B: We should use DNS, not a hosts file.

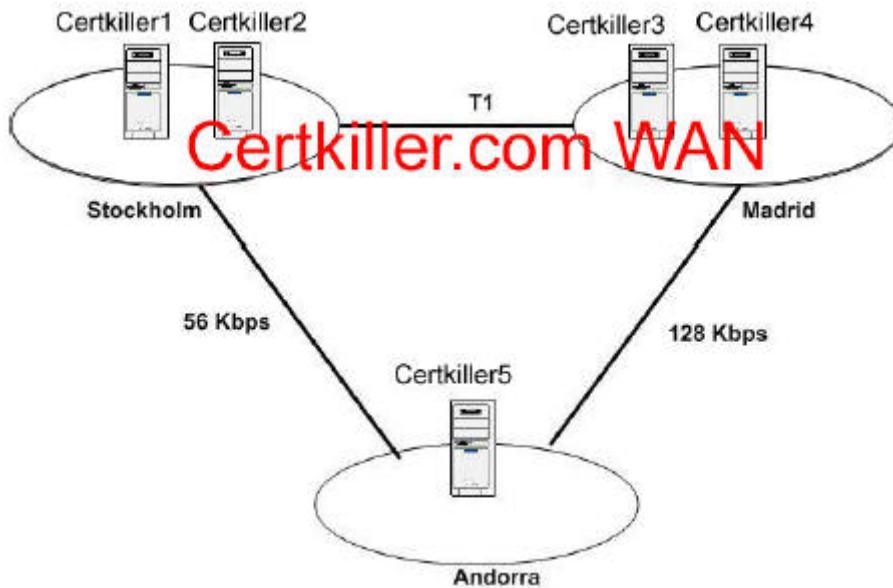
C: We don't need an SRV record for a printer. SRV records are used for computers providing a service, like a domain controller for example.

E: We should use DNS, not a hosts file.

---

### QUESTION 14

You are the network administrator for Certkiller. The network consists of a single Windows Server 2003 domain named Certkiller.com. The functional level of the Certkiller.com domain is Windows 2000 mixed. The network configuration is shown in the exhibit.



The servers are configured as shown in the following table.

Server Name	IP address	Server role	Operating system	Services and applications installed
Certkiller1	10.10.2.5	Domain controller	Windows Sever 2003	DNS, WINS
Certkiller2	10.10.28	File and print server	Windows 2000 Server	WINS, DHCP
Certkiller3	10.10.22.1	Domain controller	Windows 2000 Server	DNS
Certkiller4	10.10.22.6	Application server	Windows 2000 Server	Winds, DHCP, Microsoft Exchange Server 5.5
Certkiller5	10.10.64.3	Domain controller	Windows Server 2003	DNS, WINS, DHCP

Certkiller1 is the replication hub for the other WINS servers You need to reduce the lookup traffic between client computers and the WINS servers within each office. In addition, you need to optimize all network traffic between offices and within each office. You also need to ensure redundancy if the WINS service fails on any one of the servers. How should you configure WINS forward lookups on Certkiller1?

To answer, configure the appropriate option or options in the dialog box, and drag the two appropriate IP addresses to the correct locations.

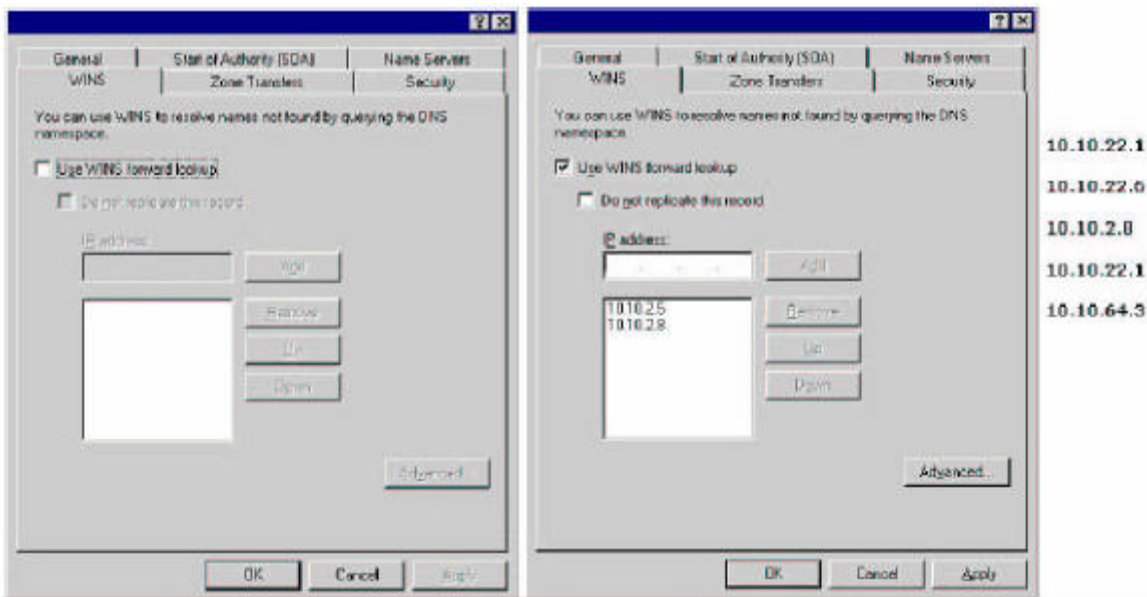
IP Addresses  
Select from these

Dialog Box  
Place here

- 10.10.2.5
- 10.10.2.8
- 10.10.22.1
- 10.10.22.6
- 10.10.2.8
- 10.10.22.1
- 10.10.22.6
- 10.10.64.3



Answer:



Explanation:

In order to avoid wins lookup traffic across the WAN links, we must just configure wins forward lookups to Certkiller1 and Certkiller2 because they are local to the DNS server. We can configure the other WINS servers to replicate with Certkiller1 out of office hours.

## QUESTION 15

You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. All servers run either Windows Server 2003 or Windows 2000 Server. All client computers run either Windows XP Professional, Windows 2000 Professional, or Windows NT Workstation 4.0. All the computers are members of the domain. All servers have static IP addresses, and all client computers are assigned addresses by a DHCP server that runs Windows Server 2003. The DNS service is installed on three

Windows Server 2003 computers that are configured as domain controllers. Company network management standards state that a DNS domain must be created for each department in the company. A new department named Market Research has been organized. You need to create a corresponding DNS zone named marketresearch.Certkiller.com. The network management standards contain the following requirements.

- All computers must be registered in a DNS zone.
- All DNS records must be kept up-to-date at all times, and any changes to the host name or IP address must be updated on the DNS record.
- Only computers that have valid accounts in the domain must be allowed to dynamically register records in the DNS zone.
- To reduce administrative effort, all possible administrative tasks should be automated.

You must configure the marketresearch.Certkiller.com zone to meet these requirements. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

- A. Create a standard primary zone named marketresearch.Certkiller.com.
- B. Create an Active Directory-integrated zone named marketresearch.Certkiller.com.
- C. Configure the Dynamic updates settings on the marketresearch.Certkiller.com zone to be Secure only.
- D. Configure the Dynamic updates settings on the marketresearch.Certkiller.com zone to be Secure and nonsecure.
- E. Configure the Dynamic updates setting on the marketresearch.Certkiller.com zone to be None.
- F. Manually create and update DNS records for all hosts in the marketresearch.Certkiller.com zone.
- G. Configure the DHCP server to register client computers that have received IP configuration from the DHCP server in the marketresearch.Certkiller.com zone.

Answer: B, C, G

Explanation:

Create an Active Directory-integrated zone named marketresearch.Certkiller.com. Configure the Dynamic updates settings on the marketresearch.Certkiller.com zone to be Secure only. This will ensure the replication will be automated and the records can be secured. Configure the DHCP server to register client computers that have received IP configuration from the DHCP server in the marketresearch.Certkiller.com zone. The DHCP will register the A and PTR records in behalf of the clients.

Incorrect Answers:

A: We need an Active Directory integrated zone for the secure updates.

D: We should not allow non-secure updates.

E: We need to automate the processes. Dynamic updates should be enabled. F: We need to automate the processes. Dynamic updates should be enabled.

---

## QUESTION 16

You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. A Windows Server 2003 computer named CertkillerC functions as the DNS server for the domain. Wingtip Toys is a division of Certkiller. The Wingtip Toys network consists of a single Active Directory domain named wingtiptoy.com. CertkillerC is a secondary zone server for wingtiptoy.com. You are monitoring notification traffic between the two domains. You need to keep a record of when the primary DNS server for wingtiptoy.com informs CertkillerC if available changes in the wingtiptoy.com zone. What should you do?

- A. Use the Performance console to create a log of the DNS performance counter Notification Received on CertkillerC.
- B. Enable debug logging on CertkillerC.

Configure the log to record Notification events.

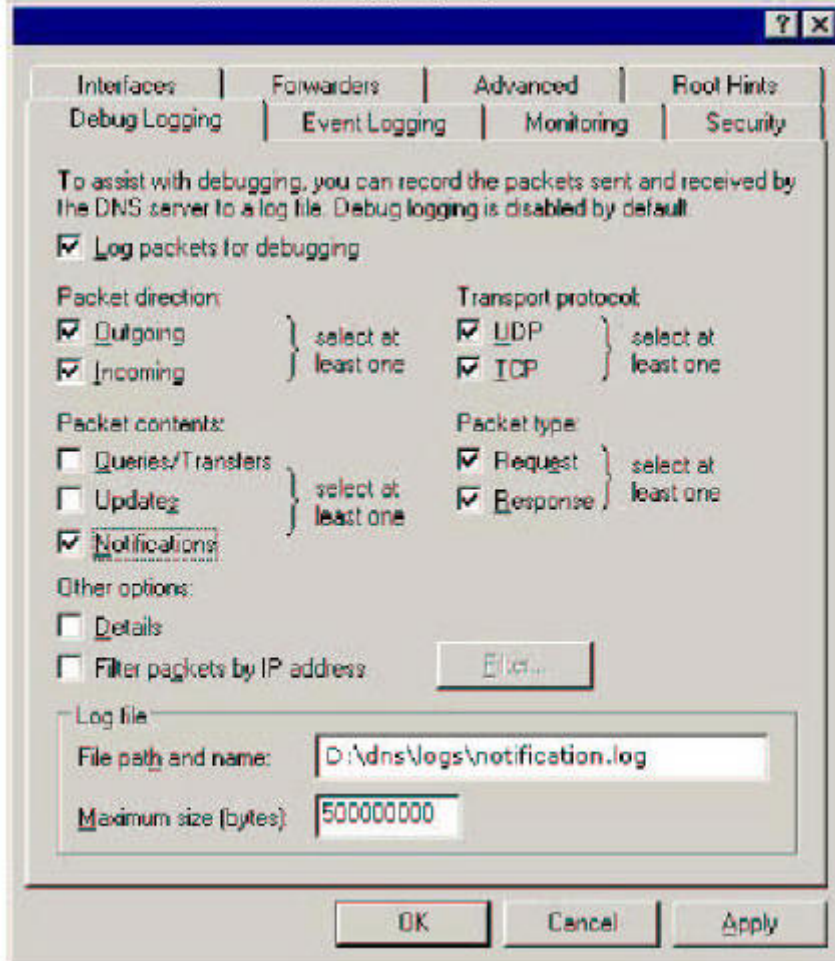
C. Run the replmon command to monitor replication events on CertkillerC.

D. Run the dcdiag command to check DNS registration on CertkillerC.

Answer: B

Explanation:

To set the debug logging options, you must first select Log packets for debugging. To get useful debug logging output you need to select a Packet direction, a Transport protocol and at least one more option. In addition to selecting events for the DNS debug log file, you can specify the file name, location, and maximum file size for the file. Using debug logging options slows DNS server performance.



---

### QUESTION 17

You are the network administrator for Certkiller. The network consists of two DNS domains named Certkiller.com and south.Certkiller.com. A Windows Server 2003 computer named CertkillerSrvA is a domain controller and DNS server for Certkiller.com. CertkillerSrvA is also a secondary zone server for south.Certkiller.com. A Windows 2000 Server computer named CertkillerSrvB is a domain controller and the DNS server for south.Certkiller.com. The two DNS domains are connected through an ISDN line. You need to monitor the successful incremental zone transfers from south.Certkiller.com to Certkiller.com.

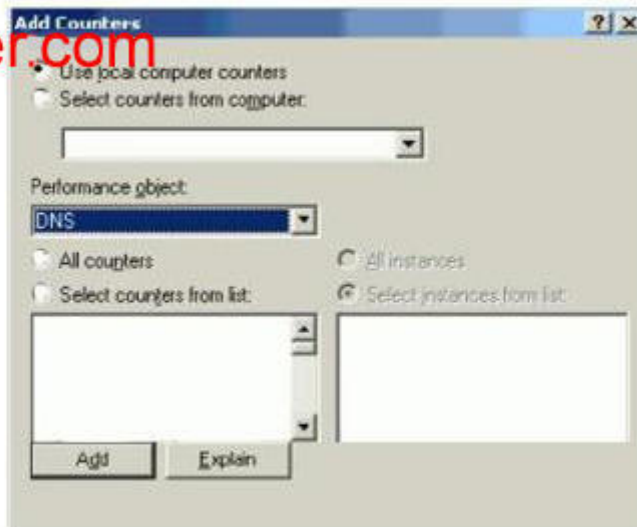
What should you do?



### Computers

CertkillerSrvA  
CertkillerSrvB

### Dialog Box Place here



### Counters

AXFR Success  
Received

IXFR Success  
Received

Dynamic Update  
Received

Secure Update  
Received

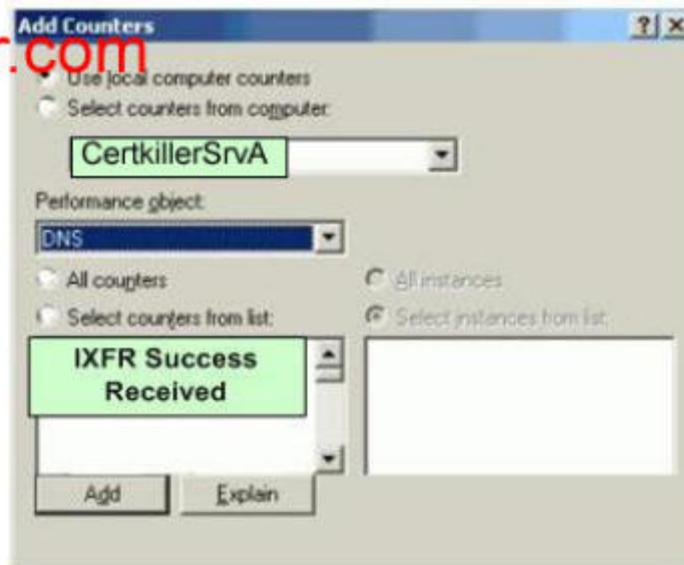
WINS Reverse  
Lookup

Answer:

### Computers

CertkillerSrvB

### Dialog Box Place here



### Counters

AXFR Success  
Received

Dynamic Update  
Received

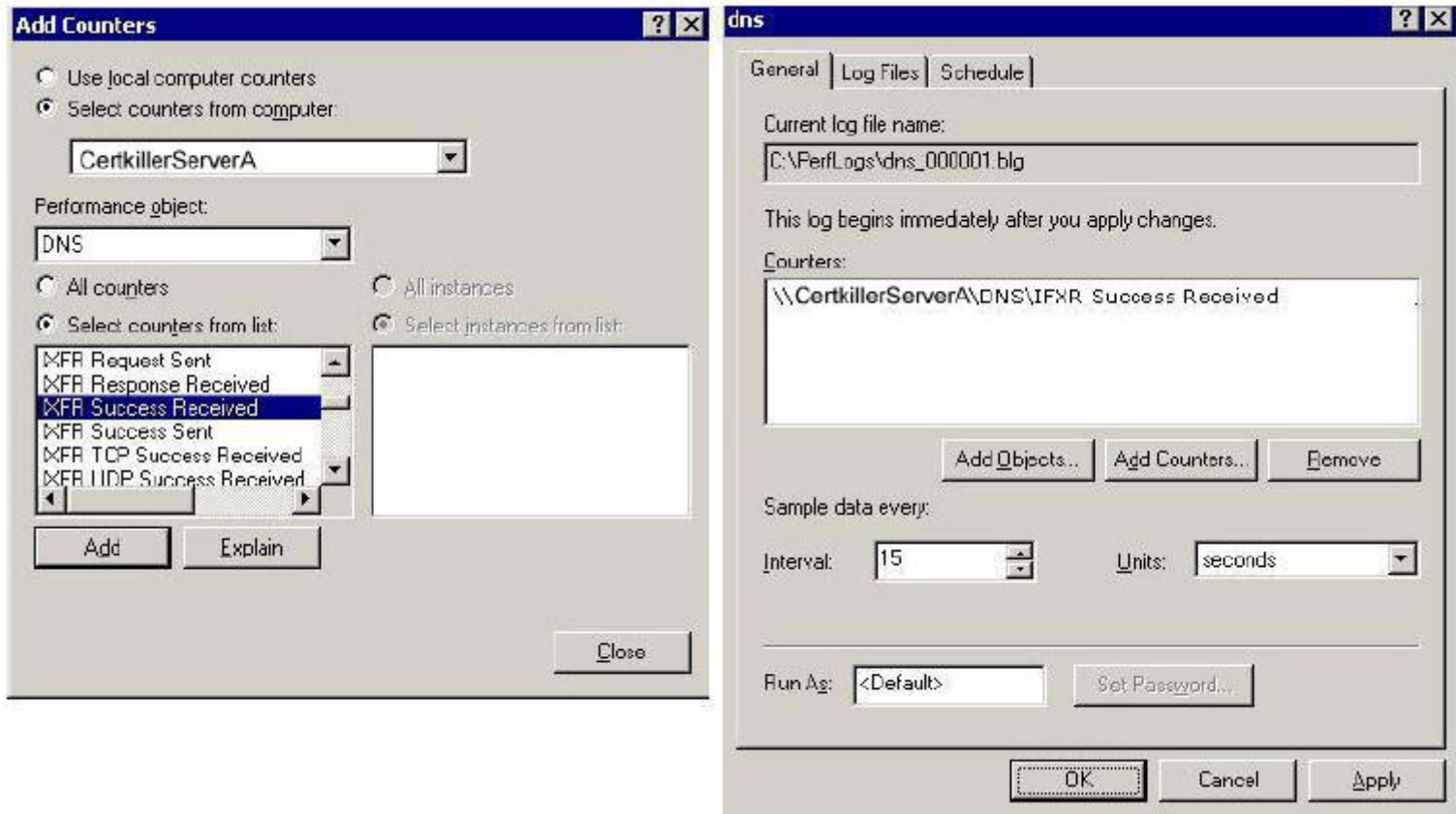
Secure Update  
Received

WINS Reverse  
Lookup

Explanation:

The incremental update for a DNS record is determined by the IXFR counter, incremental DNS transfer. The AXFR is a full replication.

The dynamic updated is a computer registering to DNS. The secure updated is a computer member of the domain who is registering his record. Wins has nothing to do with this, we are talking about DNS.



Note:

Remember to change your radio buttons and not just do the drag and drop. Not shown in the answer above, the following radio buttons should be set:

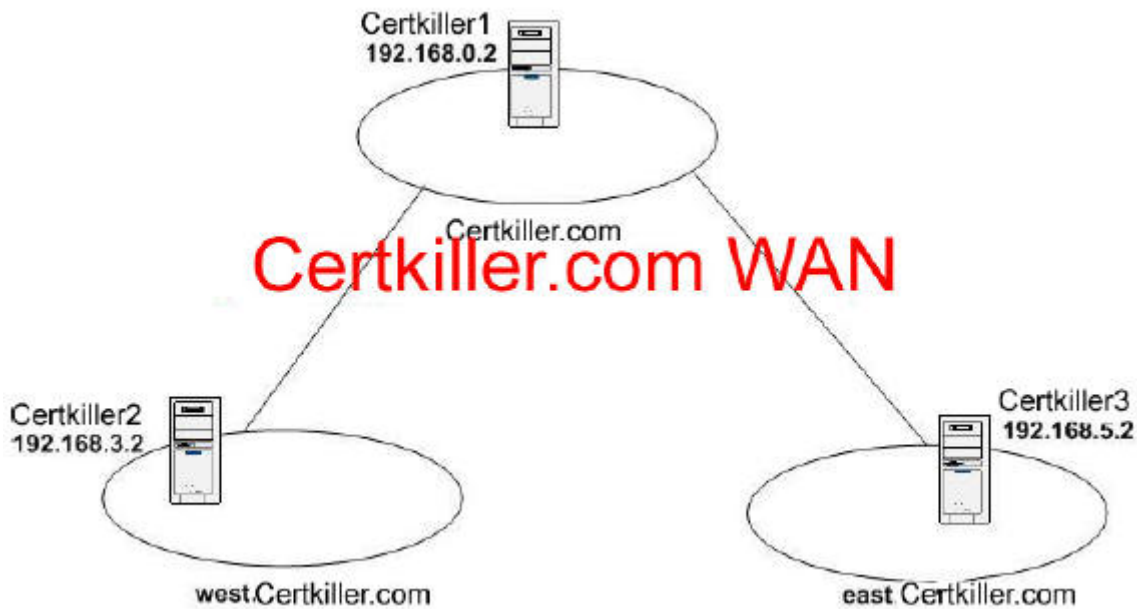
- Select counters from computer
- Select counters from list

### QUESTION 18

You are the network administrator for Certkiller. The network consists of two DNS domains named Certkiller.com and west.Certkiller.com. The company opens a new branch office. The network in the new office is configured as the east.Certkiller.com DNS domain. The three domains now contain the Windows Server 2003 computers that are described in the following table.

Server name	Domain	Server roles
Certkiller1	Certkiller.com	Domain controller, DNS server, start of authority (SOA)
Certkiller2	west.Certkiller.com	Domain controller, DNS server
Certkiller3	east.Certkiller.com	Domain controller, primary DNS server

The relevant portion of the network is shown in the exhibit.



You start the New Delegation wizard to create a new delegation resource record for the east.Certkiller.com domain to the Certkiller.com domain. How should you configure the delegation resource record?

To answer, drag the appropriate server name and IP address to the correct locations in the dialog box.

**Server Names**      **Dialog Box**  
**Place here**

Certkiller3.Certkiller.com  
Certkiller3.east  
Certkiller3.east.Certkiller.com  
Certkiller1.Certkiller.com  
Certkiller1.east  
Certkiller1.east.Certkiller.com

**IP Addresses**

192.168.0.2      192.168.3.2      192.168.5.2

Answer:

**Server Names**

Certkiller3.Certkiller.com

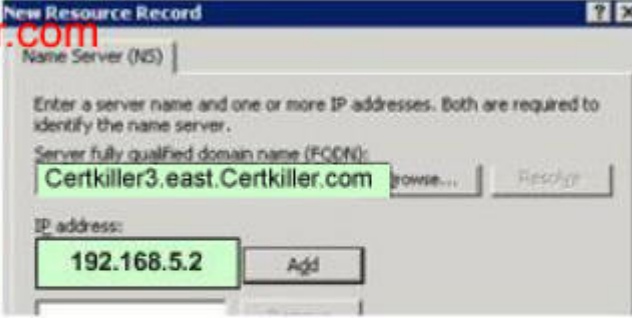
Certkiller3.east

Certkiller1.Certkiller.com

Certkiller1.east

Certkiller1.east.Certkiller.com

**Dialog Box Place here**



**IP Addresses**

192.168.0.2

192.168.3.2

Explanation:

When creating a delegation, you must enter the fully qualified domain name of the DNS server that is authoritative for the delegated domain. In this case, the server's name is Certkiller3.east.Certkiller.com. You must also enter the IP address of the DNS server; in this case 192.168.5.2.

### QUESTION 19

You are the network administrator for Certkiller. The network consists of a single Active Directory forest. The forest contains three domains named Certkiller.com, sales.Certkiller.com, and marketing.Certkiller.com. The relevant portion of the forest is shown in the work area below. The current Master Operation roles held by each domain controller are shown in the following table.

Domain controller	Roles
Certkiller1	PDC emulator, RID master, infrastructure master
Certkiller2	Schema master, domain naming master
Certkiller3	PDC emulator, RID master, infrastructure master
Certkiller4	PDC emulator, RID master, infrastructure master

Users in the sales.Certkiller.com report that they are unable to access resources in marketing.Certkiller.com. The network security administrator discovers that Kerberos authentication is failing because of a time synchronization error. You need to identify the servers that are providing time synchronization services to the client computers in each child domain. Which servers should you identify?

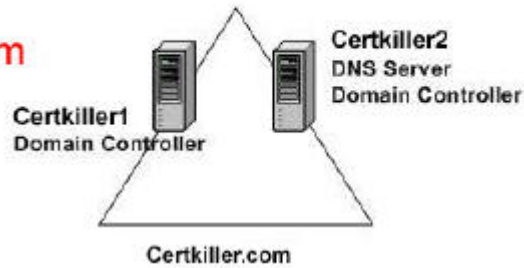
To answer, drag the appropriate server to the corresponding child domain. You can use a server name more than once.

Servers  
Select from these

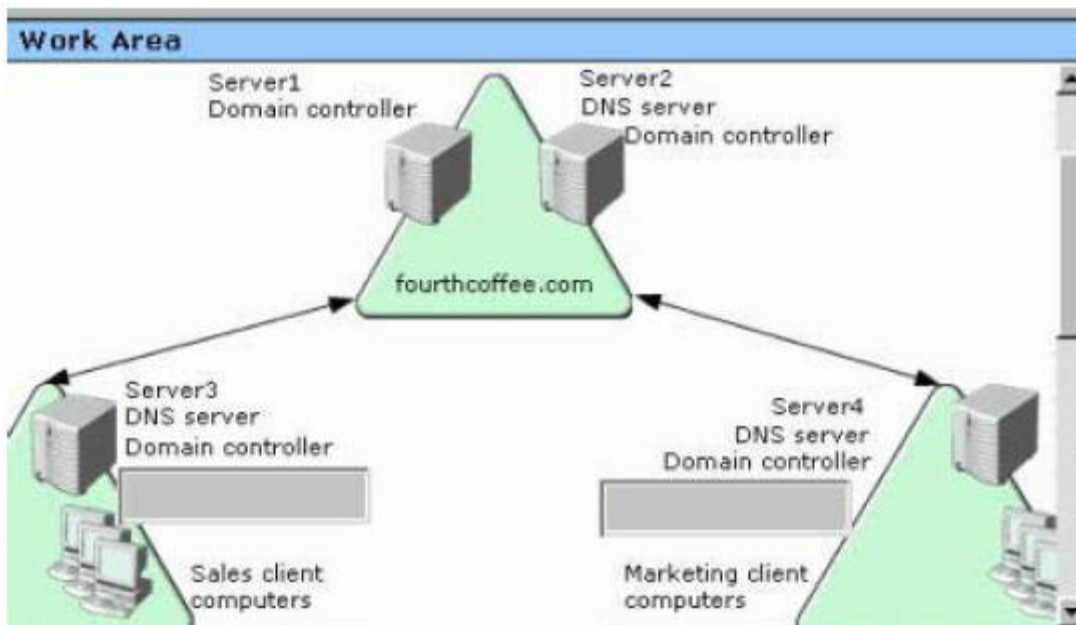
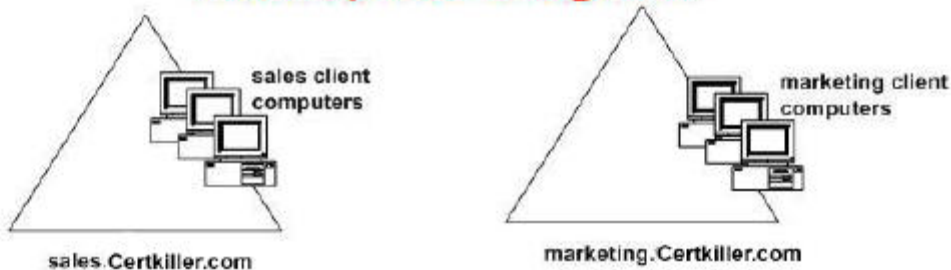
- Certkiller1
- Certkiller2
- Certkiller3
- Certkiller4

Certkiller.com

Work area  
Place here



**\*\* Incomplete Diagram \*\***



Answer: Drag the PDC Emulators to the appropriate domains.

In the two lower triangles there is a space for the drag and drop on each triangle. The question is asking which server provides time sync for Sales and which one for Marketing.

Explanation:

By default if you are out of the timing, Kerberos will reject your authentication; the default time is 5 minutes. By default the first domain controller on each domain is the NTP server for that domain. The first domain controller in a domain is also the PDC emulator by default, so we know that Certkiller1 is the NTP server for



the Certkiller.com domain. You can configure the domain controllers in each child domain to synchronize the time with the root domain.

```
net time \\server2 /domain:contoso.com /setsntp:server1.Certkiller.com.
```

```
net time \\server3 /domain:sales.contoso.com /setsntp:server1.Certkiller.com.
```

```
net time \\server4 /domain:marketing.contoso.com /setsntp:server1.Certkiller.com.
```

Also you can provide a list to provide a fault redundant configuration.

---

### QUESTION 20

You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. The domain contains Windows Server 2003 computers and Windows XP Professional computers. You configure a server named CertkillerSrv as a print server. The name of the print queue is \\CertkillerSrv\\laserprinter. You assign the Everyone group the Allow - Print permissions. Three days later, you discover that print jobs submitted to \\CertkillerSrv\\laserprinter are not being printed. You log on to the client computer named Client1. Client1 is configured to use \\CertkillerSrv\\laserprinter as its default printer. You submit several print jobs, but none of them print and no error message is displayed. In Printers and Faxes on Client1, you open \\CertkillerSrv\\laserprinter. You see the following status of the print queue: "laserprinter on CertkillerSrv is unable to connect". You are able to connect to CertkillerSrv by running the ping command. You need to ensure that print jobs submitted to \\CertkillerSrv\\laserprinter will be printed. What should you do?

- A. Create a shared printer object in Active Directory for \\CertkillerSrv\\laserprinter.
- B. From a command prompt on Client1, run the Net Print \\CertkillerSrv\\laserprinter command.
- C. On Client1, open the Services console and restart the Print Spooler service.
- D. On Client1, open the Services console and connect to CertkillerSrv . Restart the Print Spooler service.

Answer: D

Explanation:

If print jobs aren't being printed and no errors are received, then the problem is often a stalled print spooler service. This can be on the client or the server. In this case, different people are having the same problem, so the problem is likely to be with the server. From a client computer, you can connect to the server and restart the spooler service.

Incorrect Answers:

A: The printer is already shared. Creating another share won't help. B: This command is incomplete. If it were complete, it wouldn't fix the printing problem. C: Different people are having the same problem, so the problem is likely to be with the server rather than the client.

---

### QUESTION 21

You are the network administrator for Certkiller. A new Windows Server 2003 computer named Certkiller6 is located in a small branch office. Certkiller6 runs third-party update software and needs to connect to the Internet to download software updates. Certkiller6 distributes the updates to Windows XP Professional client computers in the branch office. You configure Certkiller6 so that when you double-click the Internet Explorer icon, a VPN dial-up connection to the main office automatically starts. You want Certkiller6 to access the Internet through a Microsoft Internet Security and Acceleration (ISA) Server computer named ISA1 in the main office. ISA1 uses IP address 131.107.68.92 on the Internet and is also the Routing and Remote Access server to the LAN. The ISA1 LAN interface uses IP address 10.10.0.1. Inbound VPN connections receive 10.10.0.0 IP addresses. Client computers can connect to the Internet only through ISA1. ISA1 has dynamically updates host (A) resource records for both ISA1 interfaces. On Certkiller6, you double-click the Internet Explorer icon to initiate an Internet connection. Certkiller6 successfully establishes a VPN connection to ISA1, but cannot connect to the Internet. The Internet Explorer settings for the VPN dial-up connection are shown in the exhibit.



Some users on other VPN connections to ISA1 report that they can connect to the Internet, and other users report that they cannot. You want Certkiller6 and all other VPN connections to ISA1 to consistently connect to the Internet. What should you do?

- A. In the Internet Explorer settings for the VPN dial-up connection on Certkiller6, select the Bypass proxy server for local addresses check box.
- B. In the Internet Explorer settings for the VPN dial-up connection on Certkiller6, enter 10.10.0.1 for the proxy server address.
- C. In the Internet Explorer settings for the VPN dial-up connection on Certkiller6, select the Automatically detect settings check box.
- D. On the network properties for the 131.107.68.92 connection on ISA1, clear the Register this connection's addresses in DNS check box.

Answer: D

Explanation:

The address of the proxy server is ISA1. This address will need to be resolved using DNS. The question states that ISA1 has dynamically updated host (A) resource records for both ISA1 interfaces. This means that when you query DNS for the IP address of ISA1 you could get one of two answers - the IP address of the external interface or the IP address of the internal interface. We want the IP address of the internal interface only, so we should clear the Register this connection's addresses in DNS check box for the external interface of ISA1.

Incorrect Answers:

- A. Bypass proxy server for local addresses removes the workload on the ISA server and only sends data to the ISA server when the data is for an external address. This option in this scenario will reduce further the traffic to the ISA server and will not correct the issue.
- B. This only works for Certkiller6. The question states: "Certkiller6 and all other VPN connections to ISA1 to consistently connect to the Internet" and the other clients are not covered.
- C. Like answer B above, with the correct settings, this still only works for Certkiller6 and not the other clients.

---

**QUESTION 22**

You are a network administrator for Certkiller. A Windows Server 2003 computer named CertkillerSrvA is exhibiting connectivity problems. You monitor CertkillerSrvA by using System Monitor and Network Monitor. While monitoring, you notice that CertkillerSrvA has approximately 4 MB of available memory, and the average CPU utilization is running at 95 percent. When you investigate the Network Monitor capture, you notice that some network packets sent to CertkillerSrvA during the capture have not been captured. You need to ensure that the impact of monitoring on CertkillerSrvA is reduced and that all packets sent to the computer are captured. What should you do?

- A. From a command prompt, run the diskperf command.
- B. Run Network Monitor in dedicated capture mode.
- C. Configure a Network Monitor capture filter.
- D. Increase the buffer size in Network Monitor.

Answer: B

Explanation:

Dedicated capture mode,

Network Monitor does not display or refresh capture statistics when frames are copied to the temporary capture file. This frees more resources for capturing data. Use dedicated capture mode if Network Monitor drops frames due to a lack of resources. If we do not change that dedicated capture will start in:

Normal Mode

Click to turn off Dedicated Capture Mode and return to the Network Monitor Capture window. Dedicated capture mode, Frame capture continues until you explicitly stop the capture process.

Capture filters

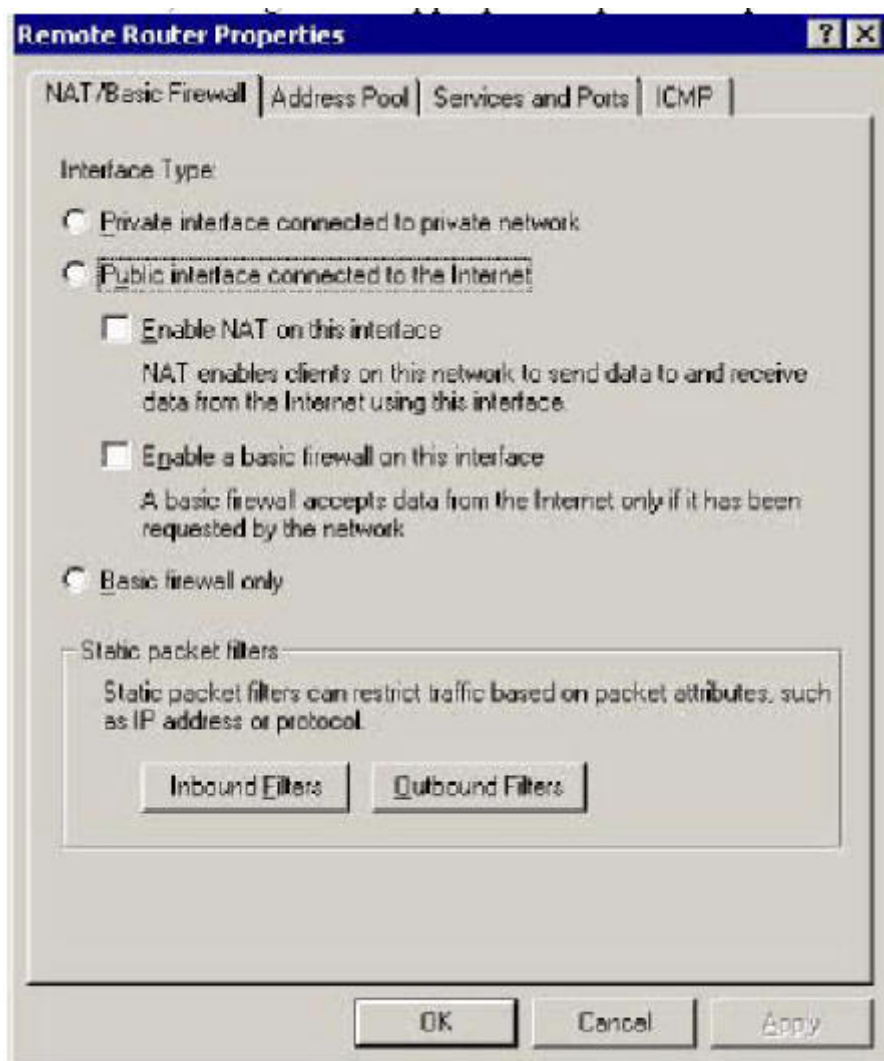
A capture filter functions like a database query that you can use to specify the types of network information you want to monitor. For example, to see only a specific subset of computers or protocols, you can create an address database, use the database to add addresses to your filter, and then save the filter to a file. By filtering frames, you save both buffer resources and time. Later, if necessary, you can load the capture filter file and use the filter again.

---

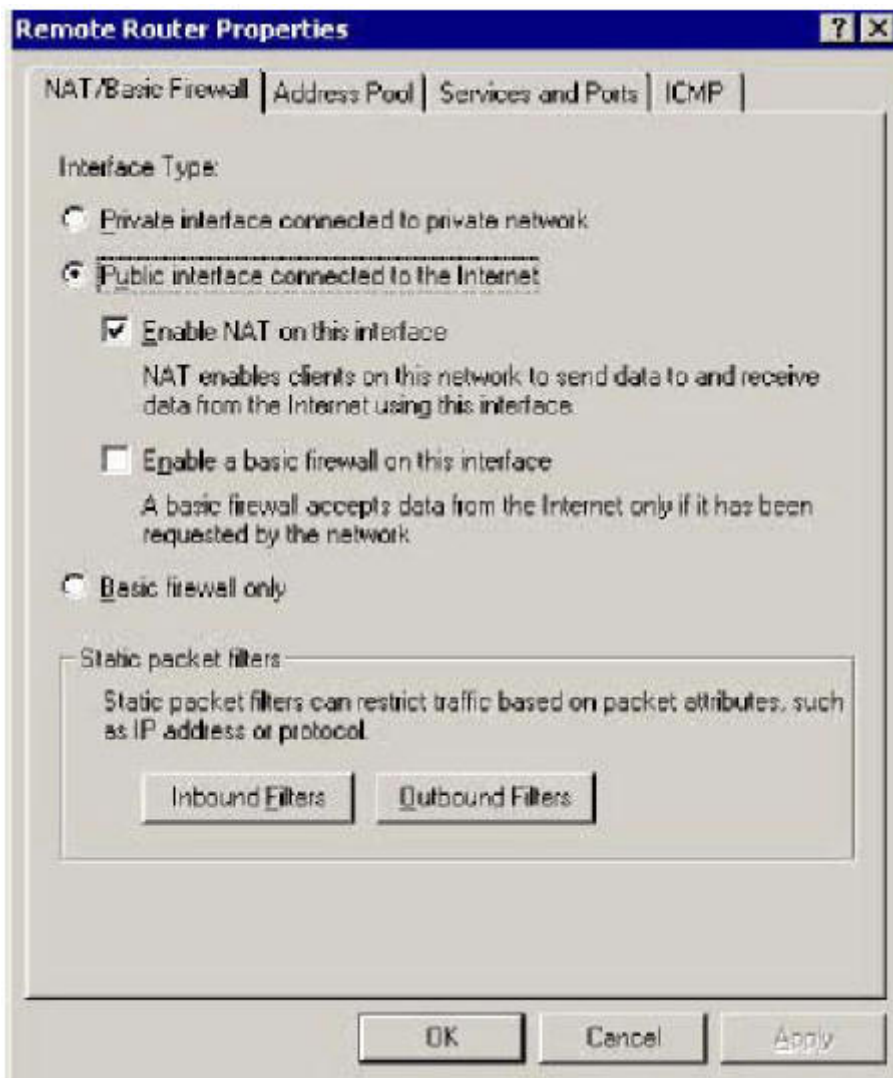
**QUESTION 23**

You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. The domain contains 10 Windows Server 2003 computers and 1,000 Windows XP Professional computers. You configure a server named CertkillerSrv as a Network Address Translator (NAT) server. CertkillerSrv is used to connect all computers on the company network to the Internet. You remove both of the old 10-Mbps network adapters in CertkillerSrv, and you replace them with 10/100-Mbps network adapters. All users now report that they are not able to connect to computers on the Internet. On CertkillerSrv, you confirm that the network adapter connected to the Internet has a public IP address, but you cannot connect to computers on the Internet. You can connect to computers that are on the company network. You need to ensure that computers on the company network can connect to the Internet through CertkillerSrv. On CertkillerSrv, you open the Routing and Remote Access console, and you open the properties of the network adapter that is connected to the Internet. What should you do next?

To answer, configure the appropriate option or options in the dialog box.



Answer:



Explanation:

We must check the NAT check box in order to convert the Public IP address to our internal private IP. We need to select public interface connected to the internet because this is the interface that is connected to our ISP.

---

### QUESTION 24

You are the network administrator for Certkiller. All client computers on the network run Windows NT Workstation 4.0. The new written company network policy requires you to change all network computers from static IP configuration to dynamically assigned IP configuration. The network policy requires a Windows Server 2003 DHCP server to dynamically assign the addresses. You anticipate the possibility that some of the client computers in the company will be overlooked and will continue to use static IP configuration. If this occurs, you want to ensure that the DHCP server will not lease an address that is already statically configured on another computer. You want to configure the DHCP servers to lease only IP addresses that are not already in use. Also, you do not want to increase network traffic any more than necessary, and you want to minimize the amount of time DHCP clients wait for an IP address lease. What should you do?

- A. Configure the DHCP server Conflict detection attempts to 1.
- B. Configure the DHCP server Conflict detection attempts to 3.
- C. Configure client reservations for each client computer MAC address.



D. Activate and reconcile the scopes.

Answer: A

Explanation:

When conflict detection attempts are set, the DHCP server uses the Packet Internet Groper (ping) process to test available scope IP addresses before including these addresses in DHCP lease offers to clients. A successful ping

means the IP address is in use on the network. Therefore, the DHCP server does not offer to lease the address to a client. If the ping request fails and times out, the IP address is not in use on the network. In this case, the DHCP server offers to lease the address to a client. Each additional conflict detection attempt delays the DHCP server response by a second while waiting for the ping request to time out. This increases the load on the server. A value of no greater than two (2) for ping attempts is recommended.

---

### QUESTION 25

You are the network administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. The domain contains a Windows Server 2003 member server named CertkillerA, which contains confidential information. CertkillerA also runs IIS and functions as a Web server for the company intranet. You want to secure the Web traffic to and from CertkillerA. You configure IIS to require only secure communications. Users must be authenticated on CertkillerA by using a domain user name and password. CertkillerA has been functioning properly for five months. Now, when users attempt to connect to CertkillerA by using Internet Explorer, an error message appears. CertkillerA responds to the ping command by host name and IP address. You view the services on CertkillerA, some of which are shown in the following window.

Name	Status	Startup Type	Log On As
Computer Browser		Automatic	Local System
HTTP SSL		Automatic	Local System
Net Logon		Automatic	Local System
Secondary Logon	Started	Automatic	Local System
WebClient	Started	Automatic	Local Service

You need to enable users to access the intranet Web content on CertkillerA. Which two actions should you perform on CertkillerA? (Each correct answer presents part of the solution. Choose two)

- A. Start the Computer Browser service.
- B. Start the HTTP SSL service.
- C. Start the Net Logon service.
- D. Restart the Secondary Logon service.
- E. Restart the Web Client service.

Answer: B, C

Explanation:

Answers A, B and C list the only services that are not running, so D and E are incorrect. We need to start the net logon to provide authentication. (C) We need to start the http SSL service for IIS in order to use SSL encryption. (D)

Note:

if we would like to have the browsing service we will need to start Computer Browser service.

---

### QUESTION 26

You are the network administrator for Certkiller. The network consists of two Active Directory domains. One domain is named Certkiller.com. A subsidiary company named Acme has a domain named acme.com. Both domains are in a single forest. A primary DNS server for Certkiller.com is located in the company's Berlin office. A primary DNS server for acme.com is located in the company's Prague office. Both DNS servers are Windows Server 2003 computers. Each domain has three regional offices. Each regional office contains the following computers:

- A secondary DNS server in its respective domain.
- A DHCP server.
- A recently installed Microsoft Internet Security and Acceleration (ISA) Server computer that connects the LAN to the Internet. Company sales representatives visit the Berlin office, the Prague office and all regional offices several times each month. All sales representatives use Windows XP Professional portable computers that are members of the Certkiller.com domain. You create an appropriate wpad.dat script file on each of the ISA servers in each regional office. On each DHCP server you configure the 252 Proxy Autodiscovery option and the corresponding `http://ISAServerName/wpad.dat` string value. Sales representatives report that they cannot access to the Internet by using Internet Explorer when they visit an office that is in the acme.com domain. You need to ensure that all users can access the Internet at all times. You want to use the minimum amount of administrative effort. What should you do?

- A. Configure Windows XP Professional portable computers with the primary DNS suffix of acme.com.
- B. Configure the Advanced TCP/IP Settings on the Windows XP Professional portable computers with a DNS suffix for this connection setting of acme.com.
- C. On each DHCP server that is a member of the acme.com domain, configure the 015 DNS Domain Name option to be acme.com.
- D. On the primary DNS server for the acme.com domain, add a `_http._service` service locator (SRV) resource record for each ISA server in the acme.com domain.

Answer: C

Explanation:

015 DNS Domain Name will automatically set the "DNS Suffix for this connection" string.

Incorrect answers:

- A. This is only the DNS suffixes to be tried when resolving names during a lookup
- B. This would work, but would need to be done manually and changes each time the portable computer changed locations. The constraint for minimum amount of administrative effort would not be achieved.
- C. This is correct
- D. There is no such SRV record in use

---

### QUESTION 27

You are the network administrator for Certkiller. The network contains 12 Windows Server 2003 computers and 300 Windows XP Professional computers.

Three servers named Certkiller4, Certkiller5, and Certkiller6 run a critical business application. When performing performance baselining on these three servers, you notice that Certkiller6 has a larger number of concurrently connected users at any given moment than Certkiller4 or Certkiller5. The additional workload is causing performance problems on Certkiller6. You need to identify which client computers are connected to Certkiller6. You plan to run Network Monitor on Certkiller6 to capture all packets sent to Certkiller6. The capture task must be configured to meet the following requirements:

- To reduce the size of the captured data, you want to capture only the packet headers.
- If a large number of packets are captured, the packets must be retained on the server. Captured packets must

not overwrite previously captured packets.

Which two tasks should you perform to configure Network Monitor? (Each correct answer presents part of the solution. Choose two)

- A. Configure the Network Monitor display filters.
- B. Configure the Network Monitor capture filters.
- C. Increase the Network Monitor buffer size setting.
- D. Decrease the Network Monitor buffer size setting.
- E. Increase the Network Monitor frame size setting.
- F. Decrease the Network Monitor frame size setting.

Answer: C, F

Explanation:

After installing Network Monitor, users can capture to a file all the frames sent to, or retained by the network adapter of the computer on which it is installed. These captured frames can then be viewed or saved for later analysis. Users can design a capture filter so that only certain frames are captured. This filter can be configured to capture frames based on criteria such as source address, destination address, or protocol. Network Monitor also makes it possible for a user to design a capture trigger to initiate a specified action when Network Monitor detects a particular set of conditions on the network. This action can include starting a capture, ending a capture, or starting a program.

Capture filters

A capture filter functions like a database query that you can use to specify the types of network information you want to monitor. For example, to see only a specific subset of computers or protocols, you can create an address database, use the database to add addresses to your filter, and then save the filter to a file. By filtering frames, you save both buffer resources and time. Later, if necessary, you can load the capture filter file and use the filter again.

Dedicated capture mode,

Network Monitor does not display or refresh capture statistics when frames are copied to the temporary capture file. This frees more resources for capturing data. Use dedicated capture mode if Network Monitor drops frames due to a lack of resources. If we do not change that dedicated capture will start in:

Normal Mode

Click to turn off Dedicated Capture Mode and return to the Network Monitor Capture window. Dedicated capture mode, Frame capture continues until you explicitly stop the capture process.

Capture Buffer Settings

Use this dialog box to adjust the size of the data frame and the total amount of frames you want to capture.

Buffer Size (MB)

The size of your capture buffer. By default, the buffer size is set to 1.0 MB. You can reduce the amount of data you capture by shrinking the capture buffer.

Frame Size (bytes)

The number of bytes that you want Network Monitor to capture from each frame. By default, the frame size is Full (65,535). The drop-down list contains numbers in increments of 64, up to 65,472. You can select one of these numbers, or you can type a specific number between 32 and 65,535, inclusive.

---

## QUESTION 28

You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The functional level of Certkiller.com is Windows Server 2003. The sales division has 500 users. These users belong to global groups as shown in the following table.

Group name Users Member of

Sales Users All sales personnel None

Internal Sales Internal sales personnel Sales Users

All sales personnel with the exception of the employees in the Internal Sales group, are roaming users who require access to the network from remote locations. You configure a server named Certkiller13 to function as a Routing and Remote Access server. In the properties of all user accounts, you enable the Control access through remote access policy setting. You need to configure remote access policies on Certkiller13. You also need to ensure that only roaming users are able to connect to Certkiller13 from remote locations. What should you do?

A. 1. Create a remote access policy named Policy1.

On Policy1, add the policy condition Windows-Groups matches "Certkiller.com\Sales Users".

Configure Policy1 to allow access based on this policy condition.

2. Create a remote access policy named Policy2.

On Policy2, add the policy condition Windows-Groups matches "Certkiller.com\Internal Sales".

Configure Policy2 to deny access based on this policy condition.

3. Assign Policy2 an order of 2.

Assign Policy1 an order of 1

B. 1. Create a remote access policy named Policy1.

On Policy1, add the following condition Windows s-Groups matches "Certkiller.com\Sales Users".

Configure Policy1 to allow access based on this policy condition.

2. Create a remote access policy named Policy2.

On Policy2, add the policy condition Windows s-Groups matches "Certkiller.com\Internal Sales".

Configure Policy2 to deny access based on this policy condition.

3. Assign Policy2 an order of 1. Assign Policy1 an order of 2.

C. 1. Create a remote access policy named Policy1.

On Policy1, add the policy condition Windows s-Groups matches "Certkiller.com\Sales Users".

2. On Policy1, add the second policy condition Windows s-Groups matches "Certkiller.com\Internal Sales".

3. Configure Policy1 to deny access based on these policy conditions.

D. 1. Create a remote access policy named Policy1.

On Policy1, add the following condition Windows s-Groups matches "Certkiller.com\Sales Users".

2. On Policy1, add the second policy condition Windows s-Groups matches Windows s-Groups matches "Certkiller.com\Internal Sales".

3. Configure Policy1 to allow access based on these policy conditions.

Answer: B

Explanation:

We need to allow remote access to Sales group who are not members of the Internal Sales group. Therefore, we need to check that the user is a member of the Internal Sales group first; if the user is a member of this group, the user will be denied access. Then we can check if the user is a member of the Sales group; if so, the user is permitted access.

Incorrect Answers:

A: Part of the answer is missing.

C: This will deny access to members of the Sales group and members of the Internal Sales group.

D: This will allow access to members of the Sales group and members of the Internal Sales group.

---

## QUESTION 29

You are the network administrator for Certkiller. The network contains 400 Windows XP Professional computers and a Windows Server 2003 computer that runs Microsoft Internet Security and Acceleration (ISA) Server. Three hundred employees work from remote locations. These users dial in to the company LAN to

establish an Internet connection and then using a VPN connection to connect to a Windows Server 2003 computer named Certkiller RAS. Internet access speeds among the dial-in users range from 28.8 Kbps to 3 Mbps. The proxy server logs a higher level of Internet activity when the dial-in users connect. The DNS server forwards DNS queries to two Internet service provider (ISP) DNS servers. Regardless of Internet access speed, dial-in users report that local Web browsing for public Internet pages slows dramatically whenever they establish a VPN connection to Certkiller RAS. You run a network monitoring utility and verify that the LAN bandwidth utilization is within acceptable limits. You need to resolve the slow Internet performance issue. You plan to use the Connection Manager Administration Kit wizard to configure all the dial-in user connections. What should you do?

- A. Configure the Internet Explorer LAN settings to Automatically detect settings.
- B. In the TCP/IP settings for each VPN client connection, add the DNS IP addresses of the two DNS servers hosted by the ISP as the primary DNS address.
- C. In the TCP/IP settings for each VPN client connection, add the DNS IP address of Certkiller's DNS server as the primary DNS address.
- D. In the TCP/IP settings for each VPN client connection, clear the Make this connection the client's default gateway check box.

Answer: D

Explanation:

When the users dial into the network, they use the LAN router as their default gateway, so they can access the internet. However, when they connect to the VPN server, the VPN server becomes the clients' default gateway. This means that all internet traffic is going through the VPN server. We can prevent this by going into the TCP/IP settings for each VPN client connection and clearing the Make this connection the client's default gateway check box.

---

### QUESTION 30

You are the network security administrator for Certkiller. The network consists of a single Active Directory domain Certkiller.com. The domain contains Windows Server 2003 computers and Windows XP Professional computers. The human resources department stores confidential data on a server named CertkillerB. The written company security policy states that TCP/IP traffic sent to and from CertkillerB must be encrypted. You need to encrypt all TCP/IP traffic that is sent between CertkillerB and the client computers in the human resources department. What should you do?

- A. Use auto enrollment to request and install an IPSec certificate on all client computers in the human resources department and on CertkillerB.
- B. Use auto enrollment to request and install a Computer certificate on all client computers in the human resources department and on CertkillerB.
- C. Use Encrypting File System (EFS) to encrypt all human resources data that is stored on CertkillerB.
- D. Assign the Secure Server IPSec policy to CertkillerB. Assign the Client IPSec policy to all client computers in the human resources department.

Answer: D

Explanation:

IPSEC for High security Computers that contain highly sensitive data are at risk for data theft, accidental or malicious disruption of the system (especially in remote dial-up scenarios), or any public network communications. Secure Server (Require Security), A default policy, requires IPSec protection for all traffic being sent or received (except initial inbound communication) with stronger security methods. Unsecured communication with a non-IPSec-aware computer is not allowed. Assigning the Client IPSec policy to all client computers in the human resources department will enable the clients to communicate with CertkillerB using



IPSec.

Incorrect Answers:

A: Providing certificates does not automatically provide encryption.

B: Providing certificates does not automatically provide encryption

C: EFS encrypts and protects data at rest, the requirement is protecting data in transit.