QUESTION 601

You are the network administrator for Certkiller . A Windows Server 2003 computer named Certkiller 11 is used to connect the network to the Internet.
You find out that some computers on the network are infected with a worm, which occasionally sends out traffic to various hosts on the Internet. This traffic always uses a certain source TCP port number.
You need to identify which computers are infected with the worm. You need to configure a solution on Certkiller 11 that will perform the following two tasks:
Detect and identify traffic that is sent by the worm.
Immediately send a notification to a network administrator that the infected computer needs to be repaired.
What should you do?

A. Configure a WMI event trigger.
B. Configure a Network Monitor capture filter.
C. Configure a Network Monitor trigger.
D. Configure a System Monitor Alert.

Answer: C

Explanation: Network Monitor captures and displays network packets at byte-level. This is too much information, and view and capture filters can be configured so that you can either view only the traffic that you are interested in, or capture only that traffic. You can create a view filter by specifying source or destination IP address, or protocol. Capture filters can be triggered by a pattern match, for example, so that you can specify when the capture starts.
Incorrect answers:
A: WMI Control is a Windows Server 2003 utility that provides an interface for monitoring and controlling system resources. WMI stands for Windows Management Instrumentation. This is not what is required, you need a Network Monitor trigger.
B: Capturing the filter is not enough; you need to configure a trigger.
D: A System Monitor Alert is not going to comply with the Certkiller 11 requirements as set out in the question.
Reference:
J.C. Mackin, Ian McLean MCSA/MCSE Self-paced training kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft Press, Redmond, 2003, pp. 17: 4-10

QUESTION 602

You are the administrator of a Windows Server 2003 computer named Certkiller 1. The network contains another Windows Server 2003 computer named Certkiller 2 that has the DNS and WINS services installed. Two hundred Windows 2000 Professional computers regularly connect to Certkiller 1 to access file and print resources.
Administrators report that network traffic has increased and that response times for requests for network resources on Certkiller 1 have increased.
You need to identify whether Certkiller 1 is receiving requests for resources through NetBIOS broadcasts.
What should you do?

A. Use Network Monitor to capture traffic between Certkiller 1 and all client computers.
B. Use Network Monitor to capture traffic between Certkiller 1 and Certkiller 2.
C. Monitor Event Viewer for Net Logon error or warning events.
D. Run the tracert command on Certkiller 1.

Answer: A

Explanation: Network Monitor captures and displays network packets at byte-level. This is too much information, and view and capture filters can be configured so that you can either view only the traffic that you are interested in, or capture only that traffic. You can create a view filter by specifying source or destination IP address, or protocol. Capture filters can be triggered by a pattern match, for example, so that you can specify when the capture starts. If you capture traffic between Certkiller 1 and all client computers then you will be able to view the proper information to see whether Certkiller 1 is receiving requests for resources through NetBIOS broadcasts.
Incorrect answers:
B: Capturing traffic between Certkiller 1 and Certkiller 2 will not yield the information necessary in this case.
C: Monitoring Net Logon error or warning events using Event Viewer will not yield the information that you need.
D: Tracert reveals breaks in connectivity but does not provide statistics about router performance. Tracert is a route-tracing utility that allows you to track the path of a forwarded packet from router to router for up to 30 hops. Running tracert on Certkiller 1 will not yield thei formation that you need.
Reference:
J.C. Mackin, Ian McLean MCSA/MCSE Self-paced training kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft Press, Redmond, 2003, pp. 17: 4-10

QUESTION 603
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003.
The network configuration is shown in the exhibit.
MISSING
You need to configure a redundant secure Internet connection between the two offices. You install and enable Routing and Remote Access on a Windows Server 2003 computer in each office. You configure the servers to use L2TP ports for the connection.
You need to ensure that the communication between the two servers is authenticated and encrypted.
You must also ensure that the computer authentication attempts do not fail.
What should you do next on each of the two servers?

A. Install one certificate that has the server extensions and another certificate that has the client extensions.
B. Install a single certificate that has the client extensions and the server extensions.
C. Create a remote access policy that filters on tunnel type and enforces 128-bit MPPE encryption.
D. Create a remote access policy that filters on tunnel type and enforces SPAP as the authentication method.

Answer: B

Explanation: By installing a single certificate with both the client and the server extensions on both of the servers, would provide the redundancy between the two offices with regard to a secure Internet connection whilst ensuring authenticated and encrypted communication between the two.
Incorrect answers:
A: By having separate certrificates for the server and the client extensions, you will not comply with with is required.
C: MPPE is a 128-bit key or 40-bit key encryption algorithm using RSA RC4 that provides for packet confidentiality between the remote access client and the remote access or tunnel server, and it is useful where Internet Protocol Security (IPSec) is not available. But it cannot be utilized in this case.
D: SPAP does not support encryption of connection data.
Reference:
J.C. Mackin, Ian McLean MCSA/MCSE Self-paced training kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft Press, Redmond, 2003, pp. 10:11, 15:16

QUESTION 604
You are the network administrator for Certkiller .com. A Windows Server 2003 computer named Certkiller F runs Routing and Remote Access.
Certkiller sales representatives use Windows XP Professional portable computers. You need configure Certkiller F to allow the sales representatives to dial in to the network.
For security purposes, you want to implement mutual authentication for all connection attempts and to require all dial-in users to use smart cards for both local and dial-up logon.
Which authentication protocol should you use?

A. CHAP
B. MS-CHAP
C. MS-CHAP v2
D. EAP-TLS

Answer: D

Explanation: 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 EAP with the Smart card or other certificate (TLS) EAP type, also known as EAP-TLS. EAP-TLS is the only authentication method supported when smart cards are used for remote authentication. A public key infrastructure (PKI) is required to implement EAP-TLS.
A trusted certification authority verifies the user's identification based on the key the user provides. A trusted certificate authority also verifies the identity of the remote access server, to secure both ends of the communication channel. EAP is supported on Windows
2000, Windows XP, as well as Windows Server 2003 Standalone remote access servers or those that belong to a workgroup cannot use EAP-TLS; only remote access servers that belong to a domain can do so.
Incorrect Answers:
A: CHAP will not solve the dilemma of the need to use smart cards for logon purposes.
B: MS-CHAP is not a mutual authentication process.

C: MS-CHAP v2 does provide mutual authentication, but in this case EAP-TLS would be more appropriate because the question also states a need to make use of smart cards for both local and dial-up logon.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 591, 594-595

QUESTION 605
You configure the Routing and Remote Access service on a server named Certkiller 1. Certkiller 1 is connected to a modem pool and support eight simultaneous inbound connections. You instruct remote users to dial on to Certkiller 1 from their home computers.
Certkiller .com's written business policy states that the only client computer operating systems that should be supported for dial-up access are Windows 95, Windows 98, Windows 2000 Professional, and Windows XP Professional.
You need to configure the remote access policy to support the most secure authentication methods possible. You want to enable only the necessary authentication methods based on the supported client computers that will be connecting.
Which authentication method or methods should you enable? Choose all that apply.

A. PAP
B. SPAP
C. CHAP
D. MS-CHAP Version 1
E. MS-CHAP Version 2

Answer: D, E

Explanation: MS-CHAP v2 is a mutual authentication method offering encryption of both authentication data and connection data. New cryptographic key is used for each connection and each direction of transmission. It is enabled by default in Windows 2000, Windows XP, and Windows Server 2003.
MS-CHAP v1 is a one-way authentication method offering encryption of both authentication data and connection data. Same cryptographic key is used in all connections. It supports older Windows clients such as Microsoft Windows 95 and Microsoft Windows 98. These two options represent the most secure authentication methods to employ.
Incorrect answers:
A: PAP is a generic authentication method that does not encrypt authentication data. User credentials are sent over the network in plaintext. It does not support encryption of connection data.
B: SPAP is a weakly encrypted authentication protocol offering interoperability with Shiva remote networking products. It does not support encryption of connection data.
C: CHAPis a generic authentication method offering encryption of authentication data through the MD5 hash ing scheme. It provides compatibility with non-Microsoft clients. The group policy applied to accounts using this authentication method must be configured to store passwords using reversible encryption. (Passwords must be reset after this new policy is applied.) It does not support encryption of connection data.
Reference:
J.C. Mackin, Ian McLean MCSA/MCSE Self-paced training kit (exam 70-291): Implementing, Managing,

and Maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft Press, Redmond, 2003, pp. 10: 10-11

QUESTION 606
You are the network administrator for Certkiller .com. 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 Certkiller 13 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 polices on Certkiller 13. You also need to ensure that only roaming users are able to connect to Certkiller 13 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: You should allow remote access to members of the Sales group who are not members of the Internal Sales group. Thus, you initially have to determine whether a user is a member of the Internal Sales group; and deny those users access if the user is a member of this group. Following this, you need to verify that the user is a member of the Sales group; and if so, allow the user access.
Incorrect Answers:
A: Part of the answer is missing. This does not represent a complete solution to the problem.
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.
Reference:
James Chellis, Paul Robichaux and Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 383-386

QUESTION 607
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com, and two subnets. The network contains a Windows Server 2003 computer named Certkiller 6. On Certkiller 6, Routing and Remote Access is enabled and is configured as a dial-up server. A Windows Server 2003 computer named Certkiller 7 functions as a DHCP server.
Certkiller 7 is authorized in the domain and leases 192.168.1.0/24 addresses to desktop client computers on the LAN and to Certkiller 6 for dial-up user connections.
On Thursday, several dial-up users report that they cannot connect to Certkiller 6. You open DhcpSrvLogThu.log and notice several lines that are partially shown in the following list.

```
15,...NACK,192.168.1.107, Certkiller 6
15,...NACK,192.168.1.103, Certkiller 6
15,...NACK,192.168.1.104, Certkiller 6
15,...NACK,192.168.1.105, Certkiller 6
15,...NACK,192.168.1.106, Certkiller 6
15,...NACK,192.168.1.108, Certkiller 6
15,...NACK,192.168.1.110, Certkiller 6
```

You want the dial-up users to have successful connections, and you want to avoid disrupting the LAN.
What should you do?

A. Delete the scope and create one in the 10.0.0.0 class
B. On Certkiller 7, configure the Conflict detection attempts setting to 2.
C. For the default Routing and Remote Class, create a 051 Lease scope option lease duration that uses a longer lease duration than the LAN.
D. Configure a static address pool on Certkiller 6 for the dial-up client computers.

Answer: D

Explanation: Static routing provides predefined routes in a static routing table. Static routing systems don't make any attempt to discover other routers or systems on their networks. Thus if you configure a static address pool on Certkiller 6 for the dial-up client computers it will result in the dial-up users having successful connection without disrupting the local area network. This should work since Certkiller 7 is

configured as the DHCP server.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, pp. 342, 415

QUESTION 608
You are the administrator of an Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
The domain contains two domain controllers named DC1 and DC2. The domain also contains two servers that run Routing and Remote Access named Certkiller 1 and Certkiller 2. Certkiller 1 and Certkiller 2 provide users with dial-up access to the corporate network.
You install a new server named Certkiller 3. You configure Certkiller 3 with Internet Authentication Service (IAS).
You want to centrally manage Routing and Remote Access authentication.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

A. On Certkiller 1, use the Routing and Remote Access console to set the authentication provider to Windows authentication.
B. On Certkiller 1, use the Routing and Remote Access console to set the authentication provider to RADIUS authentication.
C. On Certkiller 2, use the Routing and Remote Access console to set the authentication provider to Windows authentication.
D. On Certkiller 2, use Routing and Remote Access console to set the authentication provider to RADIUS authentication.
E. Configure all remote access policies on Certkiller 3.
F. Export the local security settings from Certkiller 3 to a security template. Import the security template into the local security settings on Certkiller 1 and Certkiller 2.
G. Install the Routing and Remote Access service on DC1 and DC2.

Answer: B, D, E

Explanation: RADIUS Authentication allows you to send all authentication requests heard by your server on to a RADIUS server for approval or denial. You manage remote access policies through the Remote Access Policies folder in the RRAS snap-in.
To manage Routing and Remote Access authentication centrally, you should make have the authentication provider use of RADIUS authentication on Certkiller 1 and Certkiller 2 and then configure all the remote access policies as described in options D and E.
Incorrect answers:
A: Windows Authentication is a built-in authentication suite included with Windows Server 2003. You need an authentication that will work with RADIUS. If you want the local machine to authenticate your remote access users, then you make use of Windows authentication, but not in this case.
C: Certkiller 1 should have the authentication provider set up and not Certkiller 2. Furthermore you would need to make use of RADIUS authentication and not Windows authentication.
F: Local Security settings being exported and imported to the different servers will not result in central

management of authentication.
G: This is not necessary as it will not help in centrally managing authentication.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, pp. 394-398

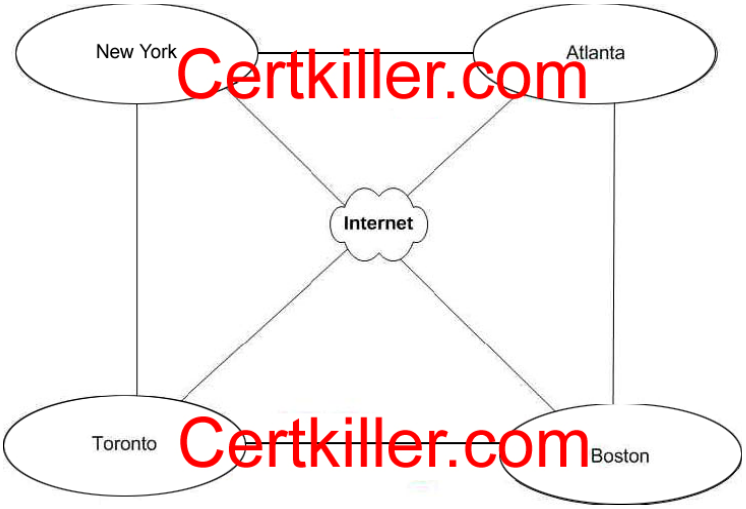
QUESTION 609
You are the administrator for Certkiller .com. All servers run Windows Server 2003.
Certkiller has a main office and three branch offices. A server named Certkiller 2 in one of the branch offices is configured with Routing and Remote Access. Certkiller 2 connects the branch office to the main office by using a demand-dial connection. The demand-dial connection is used primarily to allow users to access a custom application by using port 9000 on a server in the main office.
Certkiller 2 is configured with two network interfaces, as shown in the exhibit.
MISSING
You want to conserve costs by controlling what causes the demand-dial connection to be established.
You only want Certkiller 2 to use the demand-dial connection when a user requires access to the custom application by using port 9000. After the demand-dial connection is established, you will allow all traffic to be routed over the connection. You want to accomplish this by using Routing and Remote Access on Certkiller 2.
What should you do?

A. Create an inbound filter on the demand-dial connection to drop all traffic except for port 9000.
B. Create an outbound filter on the demand-dial connection to drop all traffic except for port 9000.
C. Create a demand-dial filter on the demand-dial connection to drop for all traffic except for port 9000.
D. Create an inbound filter on the Local Area Connection to drop all traffic except for port 9000.
E. Create an outbound filter on the Local Area Connection to drop all traffic except for port 9000.

Answer: C

Explanation: Configuring a demand-dial filter on the demand-dial connection to drop all traffic except for port 9000 would ensure that your ISDN connection is only being used when necessary. Thus keeping costs to the minimum.
Incorrect Answers:
A, B: An inbound or outbound filter on the demand-dial connection will still have to deal with all traffic before it can prohibit the connection. This means that the ISDN connection is used constantly. The best way to keep costs low would be to create a filter to drop ALL traffic except for port 9000.
D, E: Whether in- or outbound filters, traffic on the local area network does not mean that you have to make use of routing and remote access. This makes these options irrelevant in this scenario.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 9, p. 502

QUESTION 610
Network topology Exhibit



You work as a network administrator at the Certkiller main office in Toronto. Certkiller have several offices spread across North America. Each office has a Windows Server 2003 computer that is configured as a router. These servers relay network traffic on the internal network by using only IPSec to ensure secure delivery of network packets. Twenty ports are currently available for this network traffic.
Certkiller 's network connections are shown in the exhibit.
You plan to configure a new secure direct network connection between the New York office and the Toronto office by using the Internet. For this secure connection, you also plan to use the same tunneling protocol that is used on the internal company network.
You need to configure the server in the New York office to route traffic to the Toronto office an to the offices. You need to ensure the fastest possible transmission of information over the new connection.
What should you do?

A. Create a new demand-dial interface that uses PPTP.
B. Create a new demand-dial interface that uses L2TP.
C. Configure an inbound IP filter for the IGMP (Internet Group Management Protocol) protocol.
D. Configure an outbound IP filter fore the IGMP (Internet Group Management Protocol) protocol.

Answer: B

Explanation: Because each office already has a Windows Server 2003 computer that is configured as a router, you can configure a demand-dial interface on each computer. These computers would then operate as a demand-dial router with the demand-dial interfaces building connections between the remote routers in the branch offices. Windows Server 2003 servers include built in L2TP/IPSec support. Using this implementation would provide the highest level of security by ensuring authentication, data confidentiality, data integrity and data origin.
Incorrect Answers:
A: Although PPTP-based VPN connections do provide data confidentiality (captured packets cannot be interpreted without the encryption key), they do not provide data integrity (proof that the data was not modified in transit) or data origin authentication (proof that the data was sent by the authorized user). Thus making this option unwanted.
C: Configuring a filter on inbound traffic only as suggested in this option is not advisable when you want fast transmission of information for a secure IPSec connection with the same tunnelling protocol as the

internal network.

D: Same as above. This option would also only represent half of a possible solution.

Reference:

J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, p. 10:57

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, Chapters 9 & 10

QUESTION 611

Exhibit

Setting	**Certkiller Branch1 demand dial interface**	**Certkiller Branch2 demand dial interface**
Operation mode	Periodic update mode	Periodic update mode
Outgoing packet protocol	RIP version 2 broadcast	RIP version 2 broadcast
Incoming packet protocol	RIP version 1 and 2	RIP version 1 and 2

You are the network administrator for Certkiller .com. Certkiller .com has six branch offices named Certkiller Branch1 through Certkiller Branch6.

You plan to create redundant demand-dial connections between all branch offices. You will begin the implementation by configuring a demand-dial connection between Certkiller Branch1 and Certkiller Branch2.

You create one demand-dial interface on a Windows Server 2003 computer in Certkiller Branch1 and another on a Windows Server 2003 computer in Certkiller Branch2. The servers are named Certkiller 1 and Certkiller 2. You add each demand-dial interface to the RIP protocol and configure the RIP properties for each interface as shown in the exhibit.

When you test the connection, you discover that neither server is inheriting the routes from the other server.

You need to ensure that the routes are inherited when you enable the interfaces. You also need to ensure that the routes persist on each server if a link failure occurs or if either server restarts. You need to reduce convergence time between the routers.

What should you do?

A. Configure both routers to use auto-static update mode. Configure the outgoing packet protocols as RIP version 2 broadcast. Configure the incoming packet protocols with RIP version 2 only.

B. Configure both routers to use auto-static update mode. Configure the outgoing packet protocols as RIP version 2 broadcast. Configure the incoming packet protocols with RIP version 1 only.

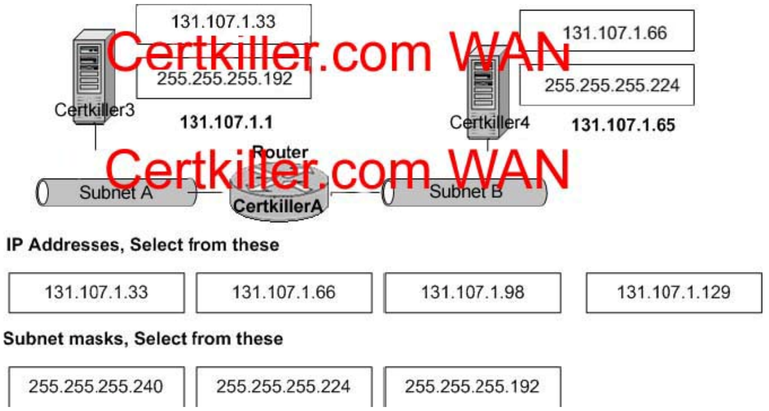
C. Configure both routers to use periodic update mode. Configure the outgoing packet protocols as RIP version 2 broadcast. Configure the incoming packet protocols with RIP version 2 only.

D. Configure both routers to use periodic update mode. Configure the outgoing packet protocols as RIP version 2 broadcast. Configure the incoming packet protocols with RIP version 1 only.

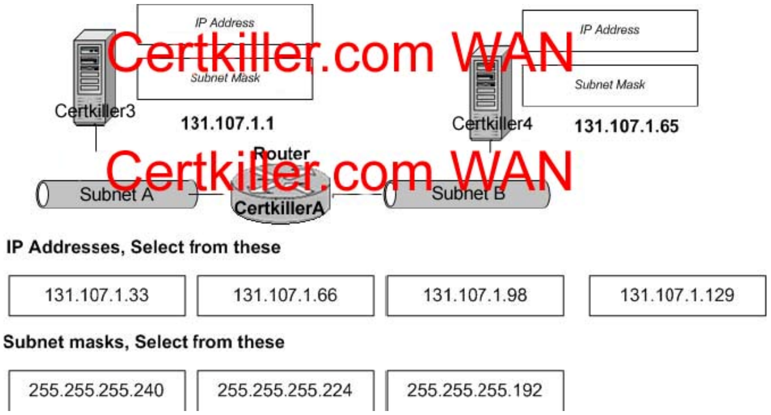
Answer: A

Explanation: In auto-static update mode, the RRAS router only broadcasts the contents of its routing table when a remote router asks for it. The routes that the RRAS router learns from its RIP neighbors are marked as static routes in the routing table, and they persist until you manually delete them-even if the router is stopped and restarted or if RIP is disabled for that interface. Auto-static mode is the default for demand-dial interfaces.
The primary difference between RIPv1 and RIPv2 is the manner in which updates are sent; RIPv1 uses broadcasts every 30 seconds, and RIPv2 uses multicasts only when routes change. RIPv2 also supports simple (e.g., plain text) username/password authentication, which is handy to prevent unwanted changes from cluttering your routing tables. RIPv2 routers also add the ability to receive triggered updates.
SO, if you want to ensure that routes are inherited when you enable interfaces and that these routes persist on each server in case of link failure whilst minimizing convergence time, then option A is the solution.
Incorrect answers:
B: Making use of auto-static update mode would be correct. However the incoming packet protocol should be configured with RIP version 2 only.
C: Periodic update mode is a RIP update mode in which routing table updates are automatically sent to all other RIP routers on the internetwork. This is the wrong update mode to use when you want to satisfy the requirements of this question.
D: In this option both the update mode and the incoming packet protocol configuration that is suggested is wrong.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, pp. 417- 418

QUESTION 612
You are a network administrator for Certkiller .com.
You need to change the IP addresses and subnet masks for two Windows Server 2003 domain controllers named Certkiller 3 and Certkiller 4. You have been allocated the public IP network address 131.107.1.0/24. You want the subnet mask on Subnet A to support 58 hosts. You want the subnet mask on Subnet B to support 28 hosts.
Because you want to conserve IP addresses, you want the subnet mask for each network to allow for subnets that are close in size to the number of required hosts. You have been assigned a default gateway of 131.107.1.1 for subnet A and a default gateway of 131.107.1.65 for subnet B.
Which IP address and subnet mask should you configure for each of the domain controllers?
Drag and Drop



Answer:



Explanation: A 255.255.255.224 subnet mask gives five host address bits, so the maximum number of host addresses is 2 ^ 5 - 2 = 30 host addresses. Thus this option suggests the only subnet mask that will allow for sufficient IP addresses in case of further growth, whilst still conserving as many current addresses as possible.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, p. 62

QUESTION 613
Exhibit, Network topology

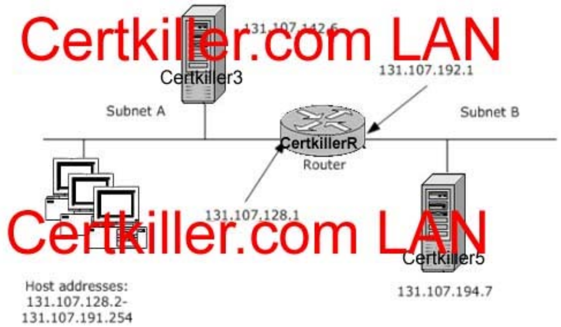
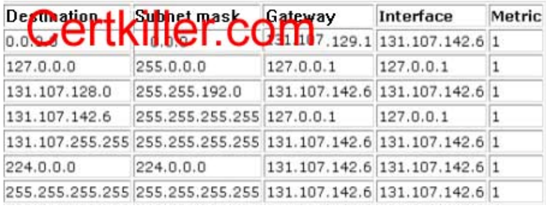


Exhibit #2



Destination	Subnet mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	131.107.129.1	131.107.142.6	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
131.107.128.0	255.255.192.0	131.107.142.6	131.107.142.6	1
131.107.142.6	255.255.255.255	127.0.0.1	127.0.0.1	1
131.107.255.255	255.255.255.255	131.107.142.6	131.107.142.6	1
224.0.0.0	224.0.0.0	131.107.142.6	131.107.142.6	1
255.255.255.255	255.255.255.255	131.107.142.6	131.107.142.6	1

You are the network administrator of Certkiller .com. The Certkiller .com network contains two subnets that are connected by a router. All servers run Windows Server 2003.
All network hosts are manually configured with TCP/IP information. The network is configured as shown in the exhibit.
A developer named Sandra users a computer named Certkiller 3 for testing. Sandra reports that she cannot access resources on a server named Certkiller 5. All other hosts on subnet A are able to access resources on Certkiller 5.
From Certkiller 3 you successfully ping the IP address of the router interface on the local subnet. However, you cannot ping the IP address of Certkiller 5 or the IP address of the router interface on subnet B. You run the route print command on Certkiller 3 and receive the output shown in exhibit #2.
You need to ensure that Certkiller 3 can connect to Certkiller 5 and any other hosts on Subnet B.
What should you do?

A. Change the IP address on Certkiller 3 to 131.107.142.128.
B. Change the subnet mask on Certkiller 3 to 255.255.0.0.
C. Change the default gateway on Certkiller 3 to 131.107.128.1
D. Change the IP address of the router interface connecting to subnet A to 131.107.142.1
E. Change the IP address of the router interface connecting to subnet A to 131.107.194.1

Answer: C

Explanation: The default gateway is used to route traffic between your computer and computers on different subnets. Each gateway has an IP address (to which the client sends outbound packets). When deciding where to send packets bound for other networks, Windows Server 2003 will examine its internal TCP/IP routing table to see whether it already knows how to get packets to the destination network. If so, it uses that route. If not, it uses the default gateway. In the exhibit one sees that Certkiller 3 must go through the router (131.107.128.1) to connect to Certkiller 5.
Incorrect answers:
A: Changing the IP address on Certkiller 3 is not going to enable connection to Certkiller 5. The default gateway has to be changed.
B: It is not a subnet mask problem that is preventing Sandra from connecting to Certkiller 5.
D, E: There is no need to change the IP address of the router interface when all that is needed is to change the Certkiller 3 default gateway so as to enable Sandra to connect to Certkiller 5 under the given circumstances.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, MCSA/MCSE: (Exam: 70-291) Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 75
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 49

QUESTION 614

You are the network administrator for Certkiller .com. The network contains seven hardware routers and seven Windows Server 2003 routers. Each of the current hardware routers supports RIP version 1, RIP version 2.0, and OSPF.

You are process of upgrading the network hardware. During the upgrade, network routes will fluctuate. You expect the final upgrades to be completed in six months. A static route connects a network stub where network hardware and software testing takes place.

You need to ensure that convergance will occure in less than five minutes as you upgrade network hardware.

Which routing protocol should you use?

A. Use RIP version 2.0. Configure the outgoing packet protocol to be RIP version 1 broadcast and the incoming packet control to be RIP version 1 and version 2.

B. Use RIP version 2. Configure the outgoing packet protocol to be RIP version 2 broadcast and the incoming packet protocol to be RIP version 2 only.

C. Use the IGMP Router and Proxy protocol.

D. Use the OSPF routing protocol and configure an area number of 0.0.0.0.

Answer:

QUESTION 615

You are the network administrator for Certkiller .com. All servers run Windows Server 2003.

You configure a server named Certkiller 2 as a Network Address Translation (NAT) server. Certkiller 2 has a single network adapter and a modem. Certkiller 2 connects to the Internet through a demand-dial connection.

Users report that when they attempt to connect to Internet Web sites, they intermittently receive the following error message: "Page not found". After waiting for several minutes, they can connect to the Web sites. These errors occur throughout the day.

You need to configure Certkiller 2 to allow users to always connect to Internet Web sites.

What should you do?

A. Set the demand-dial connection to Persistent.

B. Set the dial-out hours on the demand-dial connection to any day and any time.

C. Set a demand-dial filter.

Configure the filter for Only allow the following traffic.

Specify a new filter outbound port 80.

D. Configure the demand-dial interface as the private interface.

Answer: A

Explanation: Demand-dial connection is a connection, typically using a circuit-switched wide area network (WAN) link that is initiated when data needs to be forwarded. The demand-dial connection is typically terminated when there is no traffic. To allow users to always successfully connect to the Internet you need to configure the demand-dial connection as persistent as this will prevent the problem they are currently experiencing.

Incorrect answers:
B: Setting dial-out hours does not ensure consistent connectivity.
C: TCP port 80 is used for HTTP traffic. When one sets a demand-dial filter it is just to prohibit certain types of traffic over certain ports. This is not what is required in this scenario.
D: The Internet is a Public interface and this option suggests that the demand-dial be configured as the private interface. This will not do.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE : Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 651-652
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 616
You are the network administrator for Certkiller .com. The company has a high-speed Internet connection. A Windows Server 2003 computer named Server5 has Routing and Remote Access installed.
Some company employees use Windows XP Professional portable computers to connect to Server5. If these users open Internet Explorer, a dial-up connection starts and automatically connects to Server5.
All portable computers and user accounts are in the Laptops organizational unit (OU). A Group Policy object (GPO) named LaptopGPO is linked to the Laptops OU.
The network contains the additional servers shown in the following in the following table.

Server name	**Role**
Certkiller 3	DHCP server
Certkiller 4	DNS server
Certkiller 5	Internet Web serer

Certkiller .com purchases two other companies. Portable computer users from the two other companies report that when they open Internet Explorer, a dial-up connection starts, but does not connect, to server5. You find out that the portable computers are attempting to connect to old servers from the previous companies. You add the new portable computer and user accounts to the Laptops OU.
You want all portable computer users to immediately connect to Server5 through a single dial-up connection when they open Internet Explorer. You want to accomplish this configuration with the minimum amount of administrative effort.
What should do?

A. Add an alias (CNAME) resource record named wpad that points to Certkiller 5. On Certkiller 5 configure a wpad.dat automatic configuration file the points to a .ins configuration file. Edit the LaptopGPO GPO and select Automatically detect configuration settings in the Automatic Browser Configuration policy.
B. Edit the LaptopGPO GPO and select Enable Automatic Configuration in the Automatic Brower Configuration policy.
C. Configure a dial-up connection to Server5. Edit the LaptopGPO GPO and in the Connection Settings policy, select Import the Current Connection Settings from this machine and Delete existing Dial-up Connection Settings.
D. Configure dial-up connection settings to server5. Export the settings to a .ins file in a shared folder for which the portable computer users have Read access. On the portable computers, import the .ins file a logon script.

Answer: B

Explanation: To cut down on administrative effort a group policy modification that will enable automatic configuration will have the desired effect. Thus all you need to is to select Enable Automatic Configuration in the Automatic Brower Configuration policy on Server5.
Incorrect Answers:
A: An Alias (CNAME) record specifies another DNS domain name for a name that is already referenced in another resource record. This is not what the question asks for. Only the latter part of the option is correct.
C: The problem is not so much the connection settings from the machine, but rather a case of old nonexistent servers of the previous company. You do not need to configure a dial-up connection to server5.
All that is necessary is to edit the LaptopGPO and enabling automatic configuration. Everything else that is needed is already in place.
D: This option suggests too much administrative effort. All that is needed is to edit the LaptopGPO and enabling automatic configuration.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 3

QUESTION 617
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
The network contains a server named Certkiller 7 that runs the Routing and Remote Access service.
Users connect to Certkiller 7 by using VPNs through the Internet at any time of day.
The company's written security policy states that you must collect information about all VPN connections to the network. This information includes when users logged on, how long they were connected, and how much data was sent across the VPN connection.
You need to configure Certkiller 7 to collect the required information.
What should you do?

A. Configure RRAS login on Certkiller 7 to log all events. Archive the system log on Certkiller 7.
B. Configure an audit policy on the Domain Controllers OU. Audit all successful logon connections to the network.
C. Use the Routing and Remote Access console to monitor the remote access client list.
D. Use the Routing and Remote Access console to monitor the ports list.

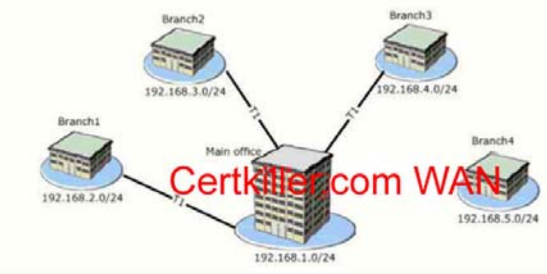
Answer: A

Explanation: The scenario described above mentions that server Certkiller 7 runs RRAS and since users make use of Certkiller 7 through VPN to connect to the Internet, you should configure RRAS login to log all events and archive the system log on Certkiller 7.
Incorrect answers:
B: Configuring audit policy and auditing all successful logon connections to the network will only yield half of the information that is requested.
C& D: The Routing and Remote Access console will yield information regarding routing. The information required in this question is for information about the VPN connections.

Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows
Server 2003, Sybex Inc. Alameda, 2003, p. 262

QUESTION 618

You are the network administrator for Certkiller .com. Certkiller has a main office and four branch offices. Certkiller 's network is configured a shown in the exhibit.



You need to establish network connectivity between the main office and Branch4. In the main office, you configure a server named Certkiller 1, which has Routing and Remote Access installed, to be a demand-dial router. You need to ensure that computers in only the main office can initiate a connection to Branch4 on Certkiller 1.

You configure the input IP packet filters on Certkiller 1 to drop all traffic except traffic from Branch4.

You analyze the network traffic to Certkiller 1 and discover that Certkiller 1 is still initiating connections from servers in other branch offices.

You need to ensure that Certkiller 1 does not initiate any connections from servers in the other branch offices.

What should you do?

A. For the demand-dial interface, set a filter that has a source address of 192.168.1.0 and a subnet mask of 255.255.255.255.

B. For the demand-dial interface, set a filter that has a source address of 192.168.1.0 and a subnet mask of 255.255.255.0.

C. Add the demand-dial interface to the NAT/Basic Firewall object.
Add an address pool of 192.168.1.0 192.168.1.254 with a subnet mask of 255.255.255.255.

D. Add the demand-dial interface to the NAT/Basic Firewall object.
Add an address pool of 192.168.1.0 192.168.1.254 with a subnet mask of 255.255.255.0

Answer: B

Explanation: You need to prevent Certkiller 1 from initiating any connections from servers in the other branch offices and only computers in the main office can initiate a connection to Branch4 on Certkiller 1. Since there is already a filter on input IP packets on Certkiller 1 to drop all traffic except from Branch4, you only need to set a filter with source address of 192.168.1.0 and a subnet mask of 255.255.255.0.

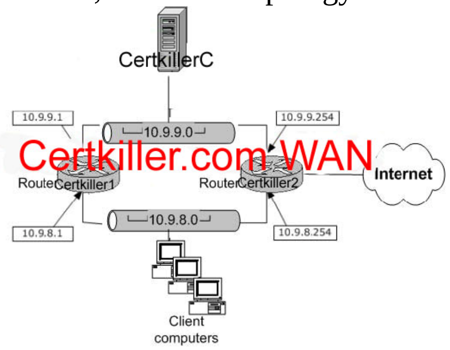
Incorrect answers:

A: The filter has to be set for source address of 192.168.1.0 and a subnet mask of 255.255.255.0 on the demand-dial interface and not for the 255.255.255.255 subnet mask.

C, D: This will not prevent Certkiller 1 from initiating any connections from servers in the other branch offices to Branch4.

Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE self-paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, 2003, Chapter 9, p. 72

QUESTION 619
Exhibit, Network Topology



You are the network administrator for Certkiller .com. The network consists of two subnets and two routers as shown in the exhibit.
While monitoring the network, you notice that the network utilization on router Certkiller 2 is near capacity. The network utilization on router Certkiller 1 is very low.
You need to configure Certkiller C to ensure that it can still communicate with hosts on the Internet while using minimum number of hops. You also need to ensure that Certkiller C will communicate with the client computers in the 10.9.8.0 subnet by using router Certkiller 1.
Which two actions should you perform on Certkiller C? (Each correct answer presents part of the solution. Choose two)

A. From a command prompt, type:
route -p add 10.9.8.0 mask 255.255.255.0 10.9.9.254 metric 1
B. From a command prompt, type:
route -p add 10.9.8.0 mask 255.255.255.0 10.9.9.1 metric 1
C. From a command prompt, type:
route -p add 0.0.0.0 mask 0.0.0.0 10.9.9.254 metric 1
D. From a command prompt, type:
route -p add 0.0.0.0 mask 0.0.0.0 10.9.9.1 metric 1

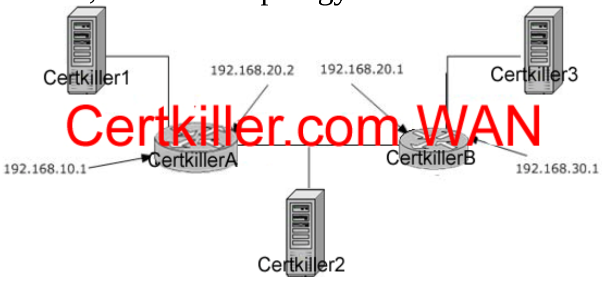
Answer: B, C.

Explanation: When adding routes, it's important to remember that these are temporary additions to the routing table.When the computer is rebooted, these additions are erased.To make a permanent or persistent entry in the routing table, use the -p parameter. Adding the -p switch to the Route Add command makes the static route persistent, which means it remains even after the router is rebooted. It makes the route permanent. Making use of options B and C will ensure that Certkiller C can communicate with client computers in the 10.9.8.0 subnet by using the Certkiller 1 router and still communicate with hosts on the Internet.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing,

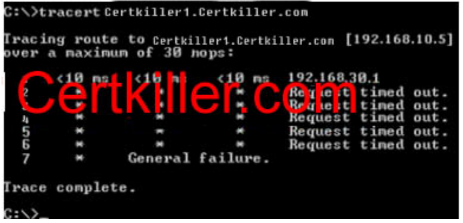
Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 15, p. 9:27

QUESTION 620

Exhibit, Network Topology



Exhibit, Tracert output



```
C:\>tracert Certkiller1.Certkiller.com

Tracing route to Certkiller1.Certkiller.con [192.168.10.5]
over a maximum of 30 hops:

  1    <10 ms   <10 ms    <10 ms  192.168.30.1
  2     *        *         *      Request timed out.
  3     *        *         *      Request timed out.
  4     *        *         *      Request timed out.
  5     *        *         *      Request timed out.
  6     *        *         *      Request timed out.
  7     *     General failure.

Trace complete.

C:\>_
```

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

The Certkiller .com network consists of three subnets. The subnets are connected by two Cisco hardware routers. Each subnet contains one Windows Server 2003 computer with the Routing and Remote Access service enabled and configured. The relevant portion of the network is configured as shown in the Topology exhibit.

Users in the 192.168.30.0/24 subnet report that they cannot access resources on Certkiller 1. You verify that Certkiller 1 and Certkiller 2 can connect to each other. You run the tracert command on Certkiller 3 and view the output shown in the Tracert exhibit.

You need to ensure that users on all three segments of the network can access resources on Certkiller 1.

What should you do?

A. Modify the route to the 192.168.30.0 network in the routing table on router Certkiller A.
B. Modify the route to the 192.168.10.0 network in the routing table on router Certkiller B.
C. Modify the route to the 192.168.30.0 network in the routing table on server Certkiller 1.
D. Modify the route to the 192.168.10.0 network in the routing table on server Certkiller 2.
E. Modify the route to the 192.168.10.0 network in the routing table on server Certkiller 3.

Answer: B

Explanation:

When deciding where to send packets bound for other networks, Windows Server 2003 will examine its internal TCP/IP routing table to see whether it already knows how to get packets to the destination network. If so, it uses that route. If not, it uses the default gateway. In this case however, you need to route 192.168.10.1 in the routing table of the Certkiller B router. That will ensure that all three segments will have accessibility to resources on Certkiller 1.

Incorrect answers:

A: The modification to the routing table should be on the router of Certkiller B and not Certkiller A.
C, D & E: You should be modifying the route (irrespective of the various options posted by these three options) in the routing table on the Certkiller B router and not on the server Certkiller 1, Certkiller 2 or Certkiller 3.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 49

QUESTION 621
You are the network administrator for Certkiller .com. Certkiller has a main office and several branch offices. You work in the main office.
The network contains Windows Server 2003 computers and Windows XP Professional computers.
A user named Katherine works in a branch office. She reports that her client computer cannot connect to a remote VPN server. You suspect that her client computer did not receive a recent hotfix.
You need to verify which hotfixes are installed on Katherine's computer.
What should you do?

A. From a command prompt, run the update.exe command.
B. From a command prompt, run the wmic qfe command.
C. View the History-synch.xml file.
D. View the History-approve.xml file.

Answer: B

Explanation: WMIC extends WMI for operation from several command-line interfaces and through batch scripts. WMI is a WBEM-compliant utility for accessing management information in a network. Its command line interface is WMIC. WMIC uses aliases, switches, verbs and parameters to obtain information from a computer system. Because WMIC can connect to any computer remotely, Administrators can perform remote administration with WMI and WMIC. This is the ideal solution to determine which hotfixes are installed on Katherine's computer.
Incorrect Options:
A: Running the update.exe command installs hotfixes; it will not allow you to see which hotfixes has already been installed.
C: Viewing the History-synch.xml file does not necessarily synchronize the server and have connecting ability with the VPN server. It just gives you the ability to view the synchronization log.
D: Viewing the History-approve.xml file will not enable Katherine to connect to the VPN server. It is the approval log that you will be viewing.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 207
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, 2003, Chapter 12, p. 495

QUESTION 622

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest named Certkiller .com. The functional level of the forest is Windows Server 2003. The network contains a Windows Server 2003 computer named Certkiller 1 that functions as a VPN server.

You set the remote access permissions for members of the Certkiller \Domain Admins group and the Certkiller \Sales group in Active Directory to Control Access through Remote Access Policy. The remote access permissions in Active Directory are not standardized for users who are not members of the Certkiller \Domain Admins group and the Certkiller \Sales group.

You create three remote access policies as shown in the following table.

Policy name	**Order**	**Condition**	**Permission**
All Users	1	Day-And-Time-Restrictions matches Any Day; Any Time	Deny
Admin	2	Windows-Group matches Certkiller \Domain Admins	Allow
Sales	3	Windows-Group matches Certkiller \Sales	

You need to ensure that only members of the Certkiller \Domain Admins group and Certkiller \Sales group can establish a VPN connection to Certkiller 1.

What should you do?

A. Add the following policy condition to all Users Policy: Windows-Group matches " Certkiller \Domain Users."

B. Change the policy order to Admin-1, All Users-2, Sales-3.

C. Change the Remote Access Permission in Active Directory to Allow for all members of the Certkiller \Domain Admins and the Certkiller \Sales group.

D. Delete the All Users policy.

Answer: D

Explanation: A virtual private network (VPN) is the extension of a private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks. VPN connections can provide remote access and routed connections to private networks over the Internet.

In this server environment, only Allow Access and Deny Access remote access permissions are available for user accounts. In this case, the Allow Access setting is the default and is the equivalent of the Control Access Through Remote Access Policy setting in all other server environments. No setting at this functional

level allows you to override user-level remote access permissions in remote access policies. Note that by default the Remote Access Permission is set to Deny Access. Thus if you are to delete the restrictive All Users policy whose order is first, then you will enable the members of Certkiller \Domain Admins group and the Certkiller \Sales group will be able to establish VPN connections to Certkiller 1.
Incorrect answers:
A: In this scenario there is no need to add further policy conditions to the All Users Policy. In fact it needs to be deleted since it is taking priority due to its order ranking.
B: Shifting the policy order around is not going to enable the members of Certkiller \Domain Admins group and the Certkiller \Sales group to establish VPN connections to Certkiller 1
C: Even if you changed the Remote Access Permission in Active Directory to Allow, the All Users policy would still take preference since it is first in the policy order ranking. You need to delete the All Users policy.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 10, p. 26

QUESTION 623
You are the network administrator for Certkiller .com. The network contains a Windows Server 2003 computer named Certkiller 3, which runs Internet Authentication Service (IAS).
Three VPN servers are located in branch offices at IP addresses 131.107.10.5, 131.107.9.4, and 131.107.8.3. You expect no more than 30 concurrent connections per VPN server. All VPN servers receive the same settings when they dial in. The existing remote access policy, the Minutes clients can be connected (Session-Timeout) setting has a dial-in constraint of 10 minutes.
You do not have a certification authority (CA) on the network.
When users attempt to connect to one of the VPN servers, you want each VPN server to implement a different dial-in constraint for the Minutes clients can be connected (Session-Timeout) setting.
What should you do?

A. Configure a separate remote access policy for each VPN server. On Certkiller 3, configure a Client-IP-Address policy condition for each VPN policy.
B. Configure a separate remote access policy for each VPN server. On Certkiller 3, configure an L2TP Tunnel-Type remote access policy condition for each VPN policy. On each VPN server, configure L2TP ports with the server's IP address in the Phone number for this device setting.
C. Configure a single remote access policy. On each VPN server, configure PPTP ports with the server's IP address in the Phone number for this device setting.
D. Configure a single remote access policy. On each VPN server, configure L2TP ports with the server's IP address in the Phone number for this device setting.

Answer: A

Explanation: IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy, which provides authentication and accounting for network access. You should be configuring a separate remote access policy for each VPN server. Since Certkiller 3 runs Internet Authentication service, you should configure a Client-IP-Address policy condition for each VPN policy on it.

Incorrect answers:
B: Configuring a separate remote access policy for each VPN server is correct. But you should be configuring a Client-IP-Address policy condition for each VPN policy on Certkiller 3 and not L2TP Tunnel-type remote access policy conditions.
C, D: Using a single remote access policy will not ensure that each VPN server implements a different dial-in constraint. Whether it is PPTP ports or L2TP ports that are configured with the server's IP address, it will not work in this case.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 624
You are the administrator of an Active Directory domain. All servers run Windows Server 2003.
A server named Certkiller 1 is configured with Routing and Remote Access. Certkiller 1 is configured to give members of the Domain Admins group VPN access to the corporate network. The dial-in permission for all user accounts in Active Directory is set to Control Access through Remote Access Policy. A single remote access policy is configured on Certkiller 1. The remote access policy is configured as shown in the following table.

Name	**Condition**	**Permission**
Admin RRAS Policy	Windows-Groups matches Domain Admins	Allow

Certkiller 's written security policy states that all corporate executives should be allowed VPN access to the network. All executives are members of a group named ExecutiveVPN.
You need to provide all executives with VPN access to the network. Members of the Domain Admins group must continue to have VPN access. No other users should be allowed VPN access to the network.
What should you do?

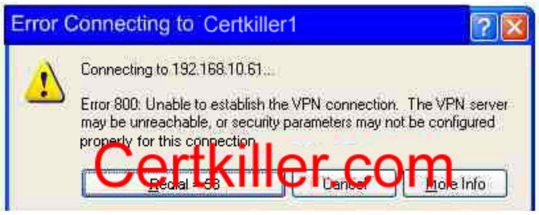
A. Create a new remote access policy that has the condition of Windows-Groups matches "Domain Users".
Set the permission on the policy to Deny and configure the policy order to 1.
B. Create a new remote access policy that has the condition of Windows-Groups matches "ExecutiveVPN".
Set the permission on the policy to Allow and configure the policy order to 2.
C. Create a new remote access policy that has the condition of Windows-Groups matches "Domain Users".
Se the permission on the policy to Allow and configure the policy order to 2.
D. Create a new remote access policy that has the condition of Windows-Groups matches "ExecutiveVPN".
Set the permission on the policy to Deny and configure the policy order to 2.
E. On the properties of all user accounts except for the accounts of users who are members of the Domain Admins group, set the dial-in permission to Deny.

Answer: B

Explanation: A remote access policy is a set of rules that are used to determine access rights or permissions for remote users and hosts. You basically define rules with conditions, which the system in turn evaluates to ascertain whether a particular user can connect or not. When two or multiple policies exist, the policies are

evaluated according to the order that you specify. Therefore, creating a new remote access policy that has the condition of Windows-Groups matches "ExecutiveVPN", and then setting the permission on the policy to Allow with a policy order of 2 would provide executives with VPN access to the network.
Incorrect Answers:
A: With the permission setting on Deny you will not be granting the proper permissions. Secondly the new remote access policy Windows-Groups conditions should math the Executive VPN and not Domain Users.
C: The permission set to Allow is correct. However, the new remote access policy Windows-Groups conditions should math the Executive VPN and not Domain Users.
D: All executives must be provided VPN access to the network and Denying them will thus not work.
E: Members of the Domain Admins group must continue to have VPN access. Thus setting the dial-in permission to Deny will not have the desired effect.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 10, pp. 587 - 593

QUESTION 625
You are an administrator of a single Active Directory forest that contains one domain. All servers run Windows Server 2003.
A server named Certkiller 1 is configured with Routing and Remote Access. Certkiller 1 is configured to allow only inbound VPN connections that use L2TP. You assign the Server (Request Security) IPSec policy on Certkiller 1. You configure the policy to use Kerberos and certificates for authentication.
From a Windows XP Professional computer named Client CK1 , which does not belong to the domain, you attempt to establish a VPN connection to Certkiller 1 and receive the error message shown in the exhibit.


Error Connecting to Certkiller1

Connecting to 192.168.10.61...

Error 800: Unable to establish the VPN connection. The VPN server may be unreachable, or security parameters may not be configured properly for this connection.

You verify that the VPN ports on Certkiller 1 are not being blocked by any intermediate devices.
You need to configure Client CK1 to allow it to establish a VPN connection to Certkiller 1.
What should you do?

A. Assign the Client (Respond Only) IPSec policy.
B. Assign the Server (Request Security) IPSec policy.
C. Install a valid IPSec certificate in the local machine store.
D. Configure the VPN connection so that only L2TP IPSec VPN is enabled.

Answer: C

Explanation: L2TP/IPSec requires a certificate infrastructure or a preshared key to issue computer certificates to the VPN server and all VPN clients. Machine certificates are digital certificates issued to machines instead of users. They allow each end of the connection to authenticate the computers involved. Machine endpoints are authenticated before the VPN client ever sends an authentication request. Machine

level authentication is a prerequisite step for a L2TP VPN. You can manually enroll machines by using the certificate authority tools to request a computer certificate for each machine that needs one. Alternatively, you force the CA to issue a certificate to the VPN server. This is done by restarting the VPN server or refreshing the local security policy.
Incorrect Answers:
A: Client (Respond Only) is used for computers that should not secure communications most of the time, but if requested to set up a secure communication, they can respond. By assigning the Client (Respond Only) IPSec policy you will not allow the establishment of a VPN connection to Certkiller 1.
B: Server (Request Security) is used for computers that should secure communications most of the time. In this policy, the computer accepts unsecured traffic but always attempts to secure additional communications by requesting security from the original sender. Thus by assigning this setting you will not accomplish your goal of allowing the establishment of a VPN connection to Certkiller 1.
D: To enable only L2TP IPSec VPN will not work as Certkiller 1 is configured to allow only inbound VPN connections that make use of L2TP and there are two ends to a connection.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 10, pp. 619 - 220

QUESTION 626
The network contains a server named RRAS1 that runs the Routing and Remote Access service. Users connect to RRAS1 by using VPNs through the Internet.
RRAS1 is configured to support VPN connections by using both PPTP and L2TP. Certkiller management informs you that support for PPTP will be phased out over the next two months.
You enable all of Certkiller 's portable computers to use L2TP to connect to RRAS1. However, some users also access RRAS1 by using their home computers. The home computers must be enabled for L2TP.
You need to view the current VPN connections to RRAS1 to find out which users are connecting to the server by using PPTP.
What should you do?

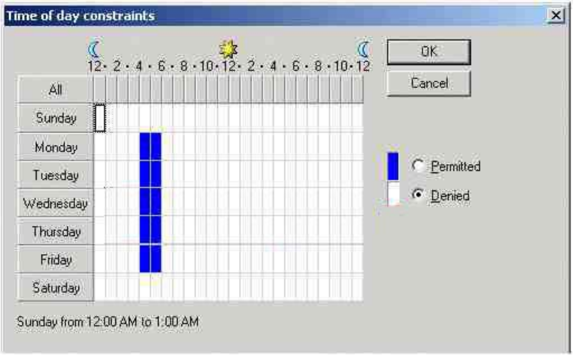
A. Configure auditing in the local security policy on RRAS1 to log all logon events.
B. Configure an audit policy on the Domain Controllers organizational unit (OU).
Audit all successful logons to the network.
C. Use the Routing and Remote Access console to review the remote access clients list.
D. Use the Routing and Remote Access console to review the properties for each active PPTP port.

Answer: D

Explanation: You can use a number of tools with the Routing and Remote Access management console to manage remote access clients. The management console provides administrators with a quick and easy way of viewing which clients are currently connected to a remote access server. To do so, click the Remote Access Clients container listed under your remote access server. The left pane displays the users currently connected. You can view status information for specific users by right-clicking their username and clicking the Status option. You can also disconnect a specific user by right-clicking the username and selecting the

Disconnect option.
Incorrect answers:
A: Logging all logon events is not just a schlep, but it will also not reveal to you current VPN connections to RRAS1 to check who uses the PPTP port.
B: This option will result in all the logon being audited and not just the current VPN connections to RRAS1 to check who uses the PPTP port.
C: This option can also work, but this would only be half a solution whereas if you could review the properties for each active PPTP port, you would be doing it properly.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

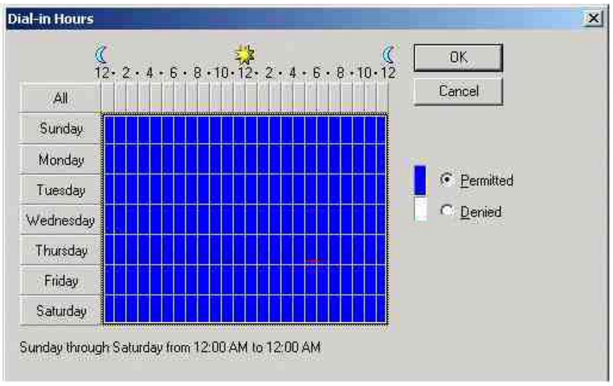
QUESTION 627
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003.
A Windows Server 2003 computer named RRAS1 functions as the Routing and Remote Access server. RRAS1. Certkiller .com is located in the company's main office.
One hundred managers dial in to RRAS1 from Windows XP Professional computers in company retail stores to submit sales reports. The manager's dial-in permissions are set to control access through Remote Access Policy. These dial-up connections occur every day, Monday through Friday, between 4:00 P.M. and 6:00 P.M. The reports take no more than one hour to complete.
You want to narrow the opportunity for unauthorized attempts to access RRAS1. On Thursday night, you ask another administrator to configure the appropriate time restriction settings.
On Friday, store managers report that they are unable to connect to RRAS1.
RRAS1 contains only one remote access policy. The policy is configured to Grant remote access permission. In the policy's conditions, in the Time of day constraints, you see the configuration shown in the Policy Condition exhibit.



○ Permitted
● Denied

Sunday from 12:00 AM to 1:00 AM

The policy profile-dial in constraint is configured to allow access as shown in the Policy Profile exhibit:



● Permitted
○ Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

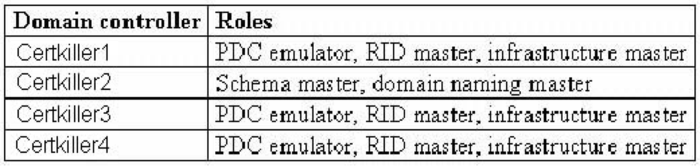
You need to ensure that store managers are able to dial in to RRAS1 to submit their sales reports.
What should you do?

A. Change the policy profile dial-in constraint for the Allow access only on these days and at these times setting to Monday through Friday from 4:00 P.M. to 10:00 P.M.
B. Change the policy condition Time of day constraints to All.
C. Change the policy condition Time of day constraints to Monday through Friday from 4.00 P.M. to 12:00 A.M.
D. Configure the Windows XP computers to Automatically synchronize with an Internet time server to ensure that their clocks differ by no more than five minutes from the Coordinated Universal Time on RRAS1.

Answer: D

Explanation: The Time of day constraints and profile-dial constraints are configured correctly, therefore making solutions A, B and C inappropriate. The authentication system will not allow access to a client computer if the time setting is more than five minutes from the Coordinated Universal Time on the RRAS server. This is why it is important that the time zone and the time are configured correctly on the client computers. The RRAS server will take into consideration the time differences between different time zones. With automatic synchronization with the RRAS1 server, the store managers will be able to get up to date sales figures to submit their reports.
Incorrect Answers:
A, B, C: In this scenario these options suggests inappropriate solutions as the Time of day constraints and profile-dial constraints are already configured. Suggesting changes to policy conditions would thus be obsolete.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 701

QUESTION 628
You are the network administrator for Certkiller .com. 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.



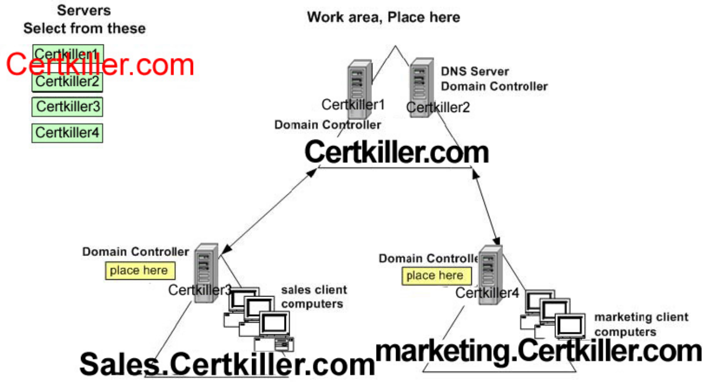
Domain controller	Roles
Certkiller1	PDC emulator, RID master, infrastructure master
Certkiller2	Schema master, domain naming master
Certkiller3	PDC emulator, RID master, infrastructure master
Certkiller4	PDC emulator, RID master, infrastructure master

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.

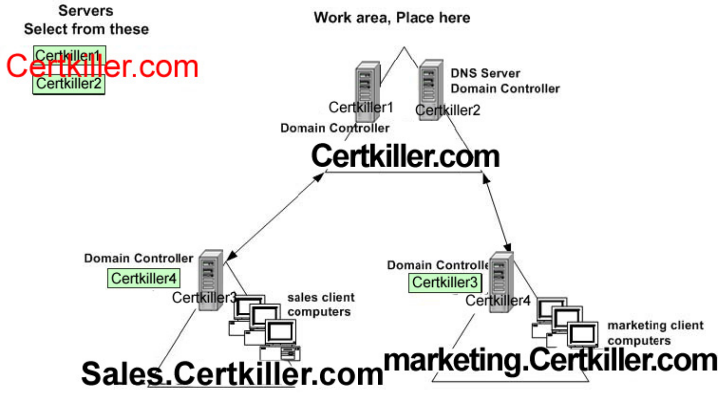
You need to identify the servers that are providing time synchronization services to the client computers in each child domain.

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.



Answer:



Explanation: Kerberos by default rejects authentication when time synchronization errors occur. By default, the first domain controller on each domain is the NTP server for that domain. The first domain controller in a domain is by default also the PDC emulator. Therefore, we can deduce that Certkiller 1 is the NTP server for the Certkiller .com domain.

You can configure the domain controllers in each child domain to synchronize 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.

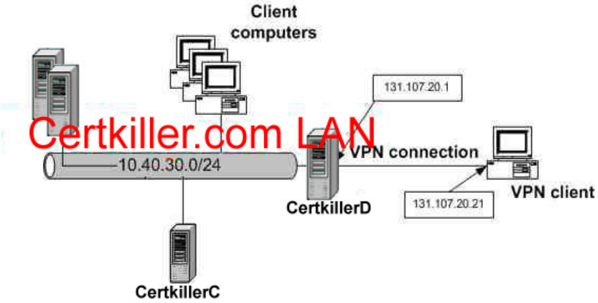
net time \\server4 /domain:marketing.contoso.com /setsntp:server1. Certkiller .com.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 297

QUESTION 629

You administer a Windows Server 2003 computer named Certkiller C which functions as a DHCP server. Certkiller C is configured to lease addresses in the 10.40.30.1 - 10.40.30.254 range. All addresses in this scope are reserved for computers on the internal network.
Another scope is configured to lease addresses in the 131.107.20.1 - 131.107.20.254 range. This scope is intended to provide addresses for Routing and Remote Access clients.
You configure a new Windows Server 2003 computer named Certkiller D to function as a Remote Access server for VPN connections. Users will connect to Certkiller D by using PPTP. Certkiller D is configured to assign IP addresses to Routing and Remote Access clients by using DHCP.
The relevant portion of the network is shown in the following diagram.



You connect to Certkiller D from a remote test computer by using a PPTP connection. The test computer successfully pings Certkiller D. However, when you run the ping command to connect to other computers on the internal network, you are unsuccessful.
You need to be able to access resources on the internal network from client computers that are connected to Certkiller D by a VPN connection.
How should you configure Routing and Remote Access on Certkiller D?

A. Enable the RIP protocol, and assign the demand-dial interface to it.
B. Enable LAN and demand-dial routing.
C. Configure the PPTP ports to allow demand-dial routing connections.
D. Create a static address pool in the 131.107.20.1/24 range.

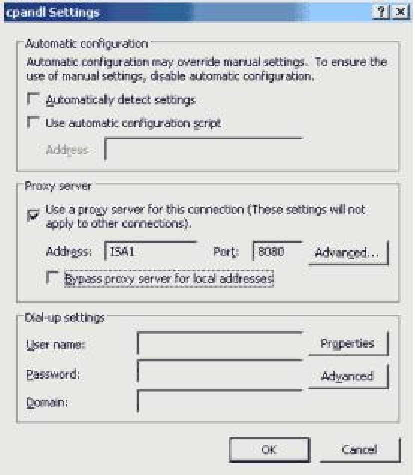
Answer: B

Explanation: To enable Routing And Remote Access for demand-dial routing, you have to select the LAN And Demand-Dial Routing option on Certkiller D. This is necessary to link the remote network with your LAN.
Incorrect Answers:
A: Enabling RIP Protocol and assigning the demand-dial interface to it will not work in this scenario.
C: Allowing demand-dial routing connections by configuring the PPTP ports will not work as you need to activate the LAN And Demand-Dial Routing option on Certkiller D.
D: The creation of a static address pool in that particular range will not allow you to accomplish your task. You need to link the remote network with the local area network.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing,

Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Chapter 9, Syngress Publishing Inc., Rockland, 2003, pp. 511, 712

QUESTION 630

You are the network administrator for Certkiller .
A new Windows Server 2003 computer named Certkiller 6 is located in a small branch office. Certkiller 6 runs third-party update software and needs to connect to the Internet to download software updates. Certkiller 6 distributes the updates to Windows XP Professional client computers in the branch office.
You configure Certkiller 6 so that when you double-click the Internet Explorer icon, a VPN dial-up connection to the main office automatically starts. You want Certkiller 6 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 Certkiller 6, you double-click the Internet Explorer icon to initiate an Internet connection. Certkiller 6 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.



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

☑ Use a proxy server for this connection (These settings will not apply to other connections).

Address: ISA1 Port: 8080

□ Bypass proxy server for local addresses

Dial-up settings

User name:

Password:

Domain:

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 Certkiller 6 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 Certkiller 6, select the Bypass proxy server for local addresses check box.
B. In the Internet Explorer settings for the VPN dial-up connection on Certkiller 6, enter 10.10.0.1 for the proxy server address.
C. In the Internet Explorer settings for the VPN dial-up connection on Certkiller 6, 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 and needs to be resolved by making use of DNS. The question states that ISA1 has dynamically updated host (A) resource records for both ISA1 interfaces. Thus when you query DNS for the IP address of ISA1 you could receive the IP address of the external interface, or the IP address of the internal interface. You should clear the Register this connection's addresses in DNS check box for the external interface of ISA1 because you only want the IP address of the internal interface.
Incorrect answers:
A: Selecting the Bypass proxy server for local addresses option would reduce traffic to the ISA server because only data that is intended for an external address would be sent to the ISA Server. This will not correct the problem of inconsistent connections.
B: This approach of making the proxy server address 10.10.0.1 relates only to Certkiller 6. The requirement is that Certkiller 6 and all other VPN connections to ISA1 should consistently connect to the Internet.
C: This approach too only involves Certkiller 6, and not all the clients. The other users will still be facing the same problem of inconsistent connections.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5
James Chellis, Paul Robichaux and Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 359

QUESTION 631
You are the network administrator for Certkiller .com. The network serves a main office and one branch office. Both offices are configured to route traffic to the Internet. A Windows Server 2003 computer named Certkiller 1 is located in the main office. A Windows 2003 computer named Certkiller 2 is located in the branch office.
You need to create an Internet connection between the main office and the branch office. You also need to ensure that the connection meets the following requirements:
• Provides the highest possible level of encryption for traffic between the two offices.
• Provides mutual authentication between the two servers.
• Requires no additional hardware or software.
Which connection or connections should you configure? (Choose all that apply)

A. An L2TP VPN connection.
B. An PPTP VPN connection.
C. A PPP over Ethernet (PPPoE) connection.
D. An IPSec tunnel

Answer: A, D

Explanation: A virtual private network (VPN) is a private network of computers that is at least partially connected using public channels or lines, such as the Internet. The two protocols used for accessing a VPN server are the Point-to-Point Tunneling Protocol (PPTP) and the Layer 2 Tunneling Protocol (L2TP). VPNs use encryption and secure protocols such as PPTP and L2TP to ensure that unauthorized parties do not intercept data transmissions. L2TP uses IPSec for data encryption thus you would also make use of an IPSec tunnel. This should ensure that you get the highest possible level of encryption for traffic between the two

offices, mutual authentication without necessitating additional hardware or software.
Incorrect answers:
B: PPTP is used over a PPP connection on an IP based network to create a secure tunnel.
C: This is an IP based network and making use of PPP over Point-to-Point Protocol over Ethernet (PPPoE) will not work. Thus this option is not the answer.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 632
You are the network administrator for Certkiller .com. 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?

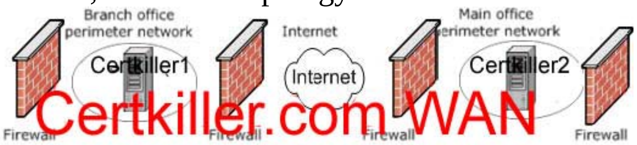
A. Configure the Internet Explorer LAN settings to Automatically detect settings.
B. In the TCP/IP settings for each VPN client connection, add the DNS IP addresses of the two DNS servers hosted by the ISP as the primary DNS address.
C. In the TCP/IP settings for each VPN client connection, add the DNS 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 to access the Internet. However, when they connect to the VPN server, the VPN server becomes the clients' default gateway. This indicates that all Internet traffic is moving through the VPN server. To prevent this from occurring, configure the TCP/IP settings for each VPN client connection by clearing the Make this connection the client's default gateway check box.
Incorrect Answers:
A: You should prevent all Internet traffic moving through the VPN server, thus you need to reconfigure the TCP/IP settings for the VPN client connections, not the LAN Internet Explorer settings.
B, C: Adding DNS IP addresses as primary DNS addresses, whether it is of the two DNS servers hosted by the ISP or the Certkiller DNS server, will not serve the same purpose as clearing the Make this

connection the client's default gateway. Thus these options will not work.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter and Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 73

QUESTION 633
Exhibit, Network Topology



You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
Certkiller .com has a main office and one branch office. The perimeter networks for each office are configured as shown in the exhibit.
You configure an L2TP/IPSec VPN tunnel between Certkiller 1 and Certkiller 2. You also configure and assign an IPSec policy named Certkiller IPSec that required secure communications.
You need to ensure that no unsecured traffic from the Internet reaches the internal network through this VPN. You also need to ensure that access to the VPN servers from their respective internal networks is not disrupted.
What should you do?

A. Configure input and output L2TP/IPSec packet filters on the internal interfaces on Certkiller 1 and Certkiller 2.
B. Configure input and output L2TP/IPSec packet filters on the external interfaces on Certkiller 1 and Certkiller 2.
C. In the properties of RASIPSec, edit the All IP Traffic IP Filter list to include the IP addresses for only Certkiller 1 and Certkiller 2.
D. In the properties of RASIPSec, edit the All ICMP Traffic IP Filter list to include the IP addresses for only Certkiller 1 and Certkiller 2.

Answer: B

Explanation: Packet filtering is a technology that filters what type of traffic is allowed into and out of the router. One of the most useful features in RRAS is its ability to selectively filter TCP/IP packets in both directions. You can construct filters that allow or deny traffic into or out of your network based on rules that specify source and destination addresses and ports. The basic idea behind packet filtering is simple: You specify filter rules and incoming packets are measured against those rules. You have two choices: Accept all packets except those prohibited by a rule or drop all packets except those permitted by a rule.
Filters are normally used to block out undesirable traffic. In general, the idea is to keep out packets that your machines shouldn't see.
If you want to ensure that no unsecured traffic from the Internet reaches your internal network through the VPN whilst ensuring access to the VPN servers from their respective internal networks, then you should configure input and output L2TP / IPSec packet filters on the external interfaces on both Certkiller 1 and Certkiller 2.
Incorrect answers:

A: The filters should be onfigured on the external interfaces pof both Certkiller 1 and Certkiller 2 and not on the internal interfaces.
C & D: Editing the All IP Traffic IP Filter to include the Certkiller 1 and Certkiller 2 IP addresses is not going to address the problem that you are trying to avoid. Neither will editing the All ICMP traffic IP Filter list.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, pp. 422, 447

QUESTION 634
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 computers and Windows XP Professional computers.
On a server named Certkiller 1, you configure Routing and Remote Access to be a VPN server.
Certkiller 1 is configured to use only the TCP/IP protocol.
Each day, a vendor establishes a VPN connection to Certkiller 1 and uploads data to Certkiller 1. Only the vendor has remote access permissions for Certkiller 1.
You discover that the vendor has accessed others computers on the network. You need to prevent the vendor from gaining access to the network to which Certkiller 1 is connected.
What should you do?

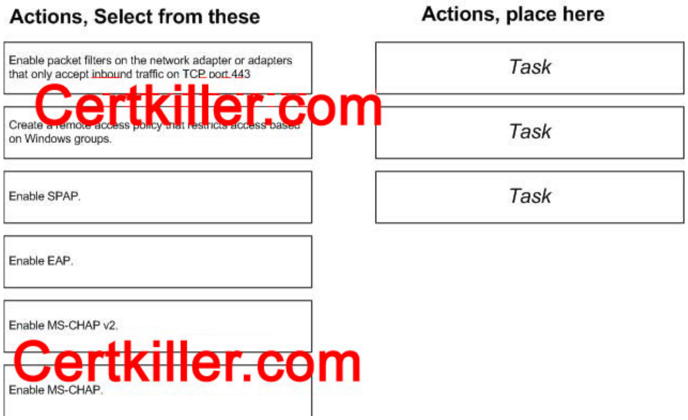
A. From a command prompt on Certkiller 1, run the route -p command.
B. Create a remote access policy for the vendor.
Add the NAS-Port-Type matches Virtual (VPN) condition for incoming connection requests to the remote access policy.
C. Open the Routing and Remote Access console on Certkiller 1.
Clear the Multilink connections check box in the server properties.
D. Open the Routing and Remote Access console on Certkiller 1.
Clear the Enable IP routing check box in the server properties.

Answer: D

Explanation: The Enable IP Routing checkbox regulates whether RRAS will route IP packets between a remote client and the other interfaces on a RRAS server. Therefore, when the option is enabled, a packet of a remote client can move to any host to which the RRAS server has a route. The option is enabled by default.
Clear the Enable IP routing check box in the server properties to restrict the vendor to accessing resources on only the RRAS server. By clearing this checkbox you disable the vendor accessing the other computers on the network without denying the vendor access to Certkiller 1.
Incorrect Answers:
A: Running the route -p command is to create a persistent routing table entry. This is exactly what you want to avoid.
B: This is unnecessary when all you need to is to access the Routing and Remote Access console and clear the Enable IP Routing check box.
C: Clearing the Multilink connections check box will not stop the vendor from being able to access the other computers that Certkiller 1 in linked to.

Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 135
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 10, p. 600

QUESTION 635
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains two Windows Server 2003 computers named Certkiller 5 and Certkiller 6. You configure Certkiller 6 as a VPN server.
You need to configure a secure remote PPTP connection to Certkiller 6. The connection will be used by users who connect to the Certkiller .com network when the work from home. These users are members of the domain and use Windows XP Professional computers. You will require these users to use smart cards for remote access.
You create a global group named Home Users and add the appropriate users to that group. You install and configure Certificate Services on Certkiller 5, and you enrol the smart cards.
You need to protect the remote connection from malicious users on the Internet. You need to ensure that Certkiller 6 receives VPN traffic from only members of the Home users group. You also need to minimize the effort required by members of the Home Users group to configure their connections.
What should you do on Certkiller 6?
To answer, drag the appropriate action or actions to the work area. Order is not important.
Drag and Drop.



Actions, Select from these

Enable packet filters on the network adapter or adapters that only accept inbound traffic on TCP port 443

Create a remote access policy that restricts access based on Windows groups.

Enable SPAP.

Enable EAP.

Enable MS-CHAP v2.

Enable MS-CHAP.

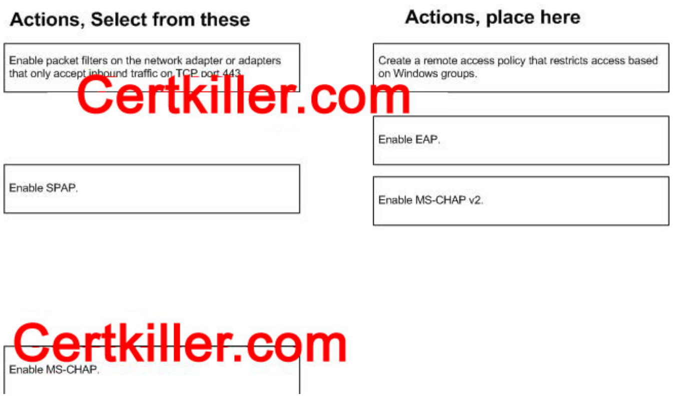
Actions, place here

Task

Task

Task

Answer:



Actions, Select from these

Enable packet filters on the network adapter or adapters that only accept inbound traffic on TCP port 443.

Enable SPAP.

Enable MS-CHAP.

Actions, place here

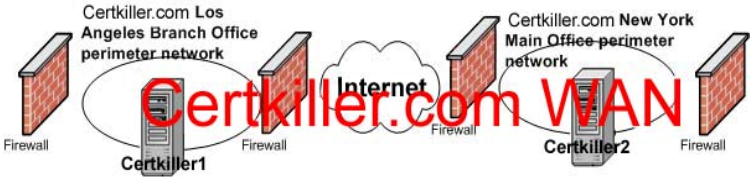
Create a remote access policy that restricts access based on Windows groups.

Enable EAP.

Enable MS-CHAP v2.

Explanation: In the question it was not necessary to put them in the right order.
Extensible Authentication Protocol (EAP) is a protocol that allows third parties to write modules that implement new authentication methods and retrofit them to fielded servers.
MSCHAP v2 authentication.The process begins with a challenge, consisting of a session ID and a challenge string, sent from the remote access server (also called the authenticator) to the remote client.The remote client responds with the username, a peer challenge, the received challenge string, the session identifier, and the user's password.These last three are in encrypted format.The remote access server checks the client responses and replies with a success or failure indication and an authentication response based on the sent challenge, the peer challenge, the encrypted response of the client, and the user's password.The client then verifies the authentication response of the server and completes the connection if the response is correct. If the client receives an invalid response from the remote access server, the connection is dropped.This twoway, mutual authentication process ensures authenticity of the client and server.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 395
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, MCSA/MCSE: (Exam: 70-291) Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 593

QUESTION 636
Exhibit, Network Topology


Certkiller.com Los Angeles Branch Office perimeter network
Firewall
Certkiller1
Firewall
Internet
Firewall
Certkiller.com New York Main Office perimeter network
Certkiller2
Firewall

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com.
The company has a main office in New York and one branch office in Los Angeles. The perimeter networks for each office are configured as shown in the exhibit.
Certkiller 1 and Certkiller 2 are each configured with a dedicated external connection to the Internet.
You need to configure a private network that allows for Internet-based communication between the mainoffice servers and client computers and between the branch office servers and client computers.
You also need to ensure that this communication is secured by using IPSec encryption.

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

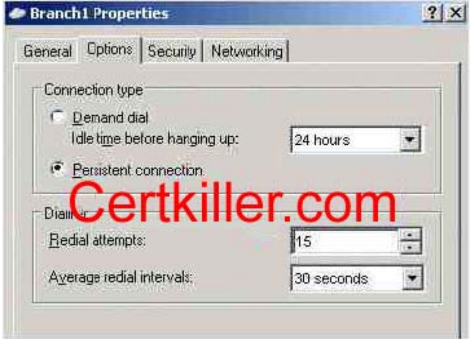
A. Configure a VPN connection between Certkiller 1 and Certkiller 2 that uses the L2TP tunnelling protocol.
B. Configure a VPN connection between Certkiller 1 and Certkiller 2 that uses the PPTP tunnelling protocol.
C. Install and configure a certification authority (CA) in the Active Directory domain.
D. Install a third-party S/MIME certificate on Certkiller 1 and Certkiller 2.
E. For each perimeter network server, configure a remote access policy to require the use of the EAPTLS authentication protocol.

Answer: A, C

Explanation: A virtual private network (VPN) is a private network that uses links across private or public networks (such as the Internet). When data is sent over the remote link, it is encapsulated, encrypted, and requires authentication services. And Layer 2 Tunneling Protocol (L2TP) is a generic tunneling protocol that allows encapsulation of one network protocol's data within another protocol. It is used in conjunction with IPSec to enable virtual private network (VPN) access to Windows 2003 networks. If you want the Internetbased communication between the main office serfvers and client computers and between the branch office servers and client computers to be secure and make use of IPSec encryption, then it would be logical to make use of a VPN that uses L2TP tunnelling between the main office and the branch office. In addition, to secure the communication, you should also make use of a certification authority in the Active Directory domain.
Incorrect answers:
B: PPTP tunnelling, though also a tunnelling protocol is not as suited to the situation as L2TP is to the situation at hand.
D: Making use of a third-party certificate service), but they are slightly less secure because you need to give the same key to every remote access user. Thus this option should not be considered.
E: EAP-Transport Level Security (TLS) allows you to use public-key certificates as an authenticator. TLS is very similar to the familiar Secure Sockets Layer (SSL) protocol used for web browsers. When EAPTLS is turned on, the client and server send TLS-encrypted messages back and forth. EAP-TLS is the strongest authentication method you can use; as a bonus, it supports smart cards. However, EAP-TLS requires your RRAS server to be part of a Windows 2000 or Server 2003 domain. This is not what is required under the given circumstances.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, pp. 344-346, 479

QUESTION 637
You are the network administrator for Certkiller .com. Certkiller has a main office and five branch offices. Business hours are 9:00 A.M. to 5:00 P.M. from Monday through Friday.
There is a demand-dial connection named Branch1 between the main office and the Chicago branch office. Branch1 is configured as shown in the dialog box.
On Saturday, an administrator in the main office attempts to perform a backup of a server in the Chicago office. He reports that he is unable to connect.

You need to ensure that the connection is available at all times. You also need to ensure that the connection will automatically attempt to connect if it fails for any reason.
What should you do?
To answer, configure the appropriate option or options in the dialog box.



Branch1 Properties

General | Options | Security | Networking

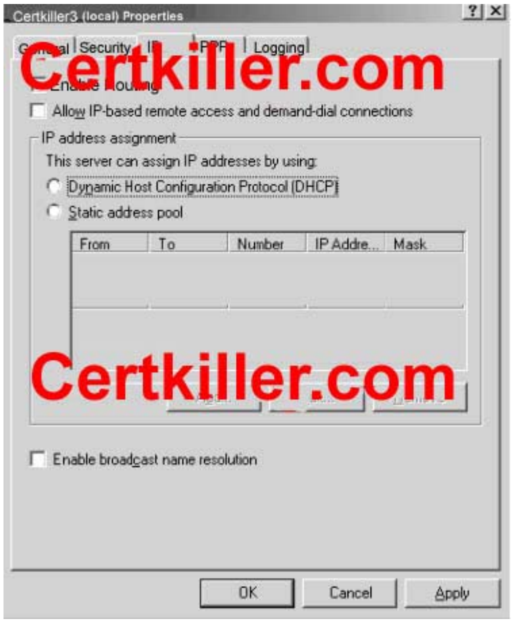
Connection type
○ Demand dial
Idle time before hanging up: 24 hours
● Persistent connection

Diali
Redial attempts: 15
Average redial intervals: 30 seconds

Answer: Activate the Persistent connection as the Connection type tab in the Options Tab in the properties window. You also need to set the redial attempts higher than 15 in the Dialing policy tab.

Explanation: When a demand-dial connection has been created, you can configure it further using the Properties window for the connection. From the Options tab, configure the connection type: either demand dial or persistent. You can also set the dialing policy by specifying the number of times that the calling router should redial if there is no answer and by specifying the interval between redial attempts. In this specific scenario you would activate the Persistent connection so as to have the connection available at all times as well as increase the redial attempt setting in case of receiving no answer from the router.
Having a Persistent connection does not preclude the event of connections being severed due to interruptions from a telnet service, etc.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 620

QUESTION 638
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional and are member of the domain.
On a server named Certkiller 3, you configure Routing and Remote Access to be a remote access server. All remote access client computers obtain an IP address from a DHCP server. You create remote access policies and verify that users can establish dial-up connections to Certkiller 3.
Users report that they cannot access other computers on the network while dialed in to Certkiller 3.
You need to ensure that remote access users can connect to all computers on the Certkiller .com network while dialed in to Certkiller 3. In the Routing and Remote Access console, you select the properties page for Certkiller 3.
What should you do next?
To answer, configure the appropriate option or options in the Certkiller 3 properties.
Multiple hotspot



Certkiller3 (local) Properties

□ Enable IP Routing

□ Allow IP-based remote access and demand-dial connections

IP address assignment

This server can assign IP addresses by using:

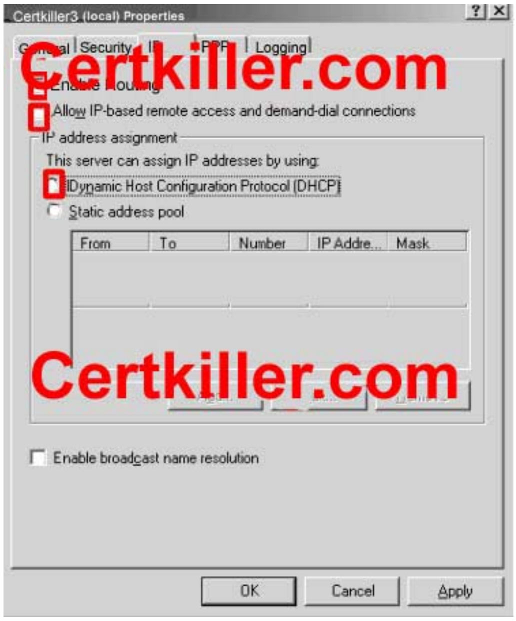
○ Dynamic Host Configuration Protocol (DHCP)

○ Static address pool

From	To	Number	IP Addre...	Mask

□ Enable broadcast name resolution

Answer:



Certkiller3 (local) Properties

□ Enable IP Routing

□ Allow IP-based remote access and demand-dial connections

IP address assignment

This server can assign IP addresses by using:

○ Dynamic Host Configuration Protocol (DHCP)

○ Static address pool

From	To	Number	IP Addre...	Mask

□ Enable broadcast name resolution

Explanation: The Enable IP Routing checkbox controls whether or not RRAS will route IP packets between the remote client and other interfaces on your RRAS server. When this box is checked, as it is by default, remote clients' packets can go to the RRAS server or to any other host to which the RRAS server has a route. To limit clients to only accessing resources on the RRAS server itself, uncheck this box.
The Allow IP-Based Remote Access And Demand-Dial Connections checkbox controls whether clients may use IP over PPP. It might seem odd to have this choice because the overwhelming majority of PPP connections use IP, but if you want to limit your server to NetBEUI, IPX, or AppleTalk remote clients, you can do so by making sure this box is unchecked.
The IP Address Assignment control group lets you specify how you want remote clients to get their IP addresses. The default setting here will vary, depending on what you told the RRAS Setup Wizard during

setup. If you want to use a DHCP server on your network as the source of IP addresses for remote clients, select the Dynamic Host Configuration Protocol (DHCP) radio button (you need to make that you've got the DHCP relay agent installed and running). If you'd rather use static address allocation, select the Static Address Pool button and then specify which IP address ranges you want issued to clients in the list below.
Reference:
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 342

QUESTION 639
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional and are members of the domain.
You configure a server named Certkiller 14 to be a VPN server. You place Certkiller 14 in the company's perimeter network. Four days later, remote access users report that they are having difficulty establishing remote access sessions to Certkiller 14.
You suspect that a computer in the Internet is conducting a denial-of-service attack on Certkiller 14.
You need to find out whether this type of attack is in progress.
What should you do?

A. Install Microsoft Baseline Security Analyzer (MBSA) on Certkiller 14. Run mbsa.exe and scan Certkiller 14 for Windows vulnerabilities. Analyze the resulting data.
B. Install Network Monitor Tools on Certkiller 14. Run Network Monitor and capture network traffic. Save the results to a file and analyze the data in the file.
C. From the command prompt on a server, run the pathping Certkiller 14 command. Save the results to a file and analyze the data in the file.
D. From the command prompt on a server, run the tracert Certkiller 14 command. Save the results to a file and analyze the data in the file.

Answer: B

Explanation: Sometimes the best way to see what's happening on your network is to watch the traffic as it passes. Network Monitor is a tool that will allow you to do just that. Network Monitor is a network analyzer (or "sniffer" after the Network General Sniffer toolset). Network analyzers capture raw traffic from the network and then decode it just as the protocol stack would. Because they don't depend on a protocol stack, you can use an analyzer to monitor traffic for protocol types you don't actually have installed. For example, you might use Network Monitor to capture and decode AppleTalk packets while troubleshooting a Mac connectivity problem, even without having AppleTalk on your workstation.
Incorrect answers:
A: Microsoft Baseline Security Analyzer (MBSA) is a utility you can download from the Microsoft website to ensure that you have the most current security updates. This is not going to aid you in this question.
C & D: The pathping tool provides the functionality of both ping and tracert and adds packet loss information as well. The most useful switch to know is the -n switch, which only displays the IP address of each hop rather than resolving each name. Running either pathping or tracert is thus not the solution in this case.
Reference:

James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows(r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, pp. 62, 86, 133

QUESTION 640

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 computers and Windows XP Professional computers. The main office is in New York, and a branch office is in Chicago.

In the Chicago office, you configure a server named Certkiller 2 to be a demand-dial VPN router. You create a demand-dial interface for dialing out. When you are creating this interface, you name it NYRouter. You use your domain user credentials, and you add a static route to the New York office.

You need to establish a router-to-router VPN connection from Certkiller 2 to a server named Certkiller 1, which is located in the New York office. Certkiller 1 is configured to be a demand-dial VPN router that has a demand-dial interface named Corp Certkiller . The Corp Certkiller interface is used for dialing in and uses the default Remote Access Policy for connection requests.

When you attempt to establish a router-to-router connection by using the NYRouter demand-dial interface, you receive the following error message: "The account does not have permission to dial in".

You need to ensure that Certkiller 2 can establish a router-to-router VPN connection to Certkiller 1.

What should you do?

A. Configure Certkiller 1's authentication provider to be RADIUS authentication.

B. Configure Certkiller 2's authentication provider to be RADIUS authentication.

C. Set the credentials for the Corp Certkiller demand-dial interface to use the Certkiller \RAS and IAS Servers domain local group for dialing in.

D. Set the credentials for the NYRouter demand-dial interface to use the Certkiller 1\Corp Certkiller user account for dialing out.

Answer: D

Explanation: When you wish to allow remote routers to dial in to a RRAS machine, you have to create a user account with the appropriate permissions. RRAS uses the information you enter in the Dial In Credentials page. The Demand-Dial Interface Wizard would create the user account if you complete the Dial In Credentials page. Credentials must match the credentials the remote router is expecting. Authentication would not occur if the credentials do not match. You have to grant dial-in permissions to the account that will be used to initiate the demand-dial connection. To solve the problem just outlined, the credentials for the demand-dial interface have to be configured to use the Certkiller 1\Corp Certkiller user account.

Incorrect Answers:

A: You must have a RADIUS server on the network in order to use RADIUS for authentication. Otherwise, an error will be generated. VPN clients will fail to be authenticated and will not be able to connect. Thus to have Certkiller 2 establish a router-to-router VPN connection to Certkiller 1 you need to NYRouter demand-dial interface credential set properly.

B: If you want Certkiller 2 to establish a successful router-to-router VPN connection to Certkiller 1 then this option is not viable. Dial-in permissions to the account that will be used to initiate the demand-dial connection has to be set.

C: This option outlines the demand-dial interface credentials, but unfortunately to Certkiller \RAS and IAS

Servers domain local group for dialing in instead of to Certkiller 1\Corp Certkiller user account for dialing out.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 607-613
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 9, pp. 510-512

QUESTION 641
You are the network administrator for Certkiller .com. The network consists of a single Active directory domain Certkiller .com. The domain contains Windows Server 20003 computers and Windows XP Professional Computers.
You configure a server named Certkiller A to be a file server. The written company security policy states that you must analyze network traffic that is sent to and from all file servers.
You need to capture file-transfer network traffic that is being sent to and from Certkiller
A. You install
network Monitor tools from a Windows Server 2003 product CD-ROM on a server named Certkiller B, which is on the same network segment as Certkiller A.
You run network Monitor on Certkiller B. However, Network Monitor captures only network traffic that is sent to and from Certkiller B. You need to capture all network traffic that is sent to and from Certkiller A.
What should you do?

A. Install the Network Monitor driver on Certkiller
A. Run Network Monitor Certkiller B to capture
network traffic.
B. Open Network Monitor on Certkiller B and create a capture filter to enable the capture of all protocols. Run Network Monitor to capture network traffic.
C. Install Network Monitor Tools on Certkiller
A. Run Network Monitor to capture network traffic.
D. Open Network Monitor on Certkiller B and increase the capture buffer from 1 MB to 20 MB in size. Run Network Monitor to capture network traffic.

Answer: C

Explanation: Only the version that ships with Microsoft SMS Server allows you to monitor all traffic on the same network segment. The question however states that Network Monitor was installed from the Windows Server 2003 product CD-ROM on the server named Certkiller B. Network Monitor is therefore only installed on the server named Certkiller B. To capture file-transfer network traffic being sent to and from Certkiller A, you have to install the Network Monitor application on Certkiller A and run Network Monitor to capture network traffic.
Incorrect Answers:
A: You should be installing Network Monitor Tools on Certkiller A and not the driver. In other works the Network Monitor application.

B: The question states that you need to monitor all traffic sent to and from Certkiller A as well as Certkiller B. This option suggests only the capture of network traffic on Certkiller B.
D: Certkiller B is not the only server that should be monitored. And furthermore increasing the capture buffer thus has no effect on whether Certkiller A traffic is also captured.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 3, pp. 137-146.

QUESTION 642
You are the network administrator for Certkiller .com. The network is connected to the Internet by using a multihomed Windows Server 2003 computer named Certkiller Router. Certkiller Router has Routing and Remote Access installed and is configured as a demand-dial router.
Certkiller Router has two network interfaces. One network interface is a network adapter that is connected to the LAN. The other network interface is a modem that is used for connecting to an Internet service provider (ISP). Certkiller Router is configured to dial out whenever an Internet connection is required.
When you inspect the telephone records, you notice that the dial-up connection to the Internet is being activated several times an hour, all day long, even when the office is empty. You suspect that one of the computers on the LAN is running an application that is configured to periodically connect to a host on the Internet.
To help you identify the application, you want to identify which computer is initiating the Internet connection, which host the computer is attempting to connect to, and what type of traffic it is attempting to send. You need to find a solution that will enable you to inspect the initial packets sent to the Internet after the connection is established. Due to the volume of data transferred to and from the Internet during normal Operations, you do not want to capture constantly.
What should you do?

A. Create and activate a System Monitor alert to run a script that will initiate a Network Monitor capture when packets are sent or received by the network adapter.
B. Create and activate a System Monitor alert to run a script that will initiate a Network Monitor capture when packets are sent or received by the modem.
C. Create and activate a Network Monitor trigger to run a script that will initiate a Network Monitor capture when packets are sent or received by the network adapter.
D. Create a Network Monitor trigger to run a script that will initiate a Network Monitor capture when packets are sent or received by the modem.

Answer: D

Explanation: Network Monitor triggers can send you a message when the packets you are on the lookout for emerge on the network. Network Monitor can track the network data stream. It will therefore assist in determining the source address of the computer that sent the message, the destination address of the computer that received the frame, and the data being sent to the destination computer.
Incorrect Answers:
A: Making use of System Monitor is the wrong tool in use for this job. You need to make use of Network Monitor.

B: You need a Network monitor trigger and not a System Monitor alert to check when packets are sent or received by the modem. System Monitor is used to monitor how services are performing.
C: The modem is the hardware that enables connection to the Internet, so if you monitor activity on the modem by making use of a Network Monitor trigger you will be able to track the computer responsible for initiating connection to the Internet, not the network adapter.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 369-372, 376

QUESTION 643
You are the administrator of a Windows Server 2003 computer named Certkiller 1. Certkiller 1 is an FTP server located in Certkiller 's internal network.
Administrators report an increased amount of FTP traffic to Certkiller 1.
You need to configure Certkiller 1 to achieve the following goals:
• Identify the media access control (MAC) address of any computer that is performing FTP transfers from Certkiller 1.
• Find out the exact FTP commands that were executed.
• Ensure that you do not disrupt the operation of Certkiller 1.
What should you do?

A. Configure a performance alert to write an event to the application event log whenever the number of established FTP connections exceeds 1.
B. Use a Network Monitor filter to capture IP traffic from any computer to Certkiller 1.
C. Run the finger command on Certkiller 1 to identify the source of the FTP requests.
D. Run the arp command on Certkiller 1 to identify the source of the FTP requests.

Answer: B

Explanation: Network Monitor is a very useful tool included with Windows Server 2003 that provides a method for detecting and isolating network issues. It allows you to capture data, identify its source, and analyze the content of the message. Because Network Monitor captures data by frames, every packet includes the source and destination address, the header information, and the actual data. Therefore, to achieve all three objectives highlighted in this question, use a Network Monitor capture filter to capture IP traffic from any computer to Certkiller 1, and apply the capture filter before capturing the data. Use the capture filter to capture only the necessary IP traffic to help you identify the reason for the increased amount of FTP traffic to Certkiller 1, and to drop the frames you not interested in.
Incorrect Answers:
A: Configuring a performance alert to log event when the established FTP connections exceed 1, will only help you in some of you objectives. You need to use a Network Monitor capture filter to accomplish all three of your objectives.
C: Running the finger command will not assist you in all the tasks that you have to perform in this question.
D: Running the arp command to find the MAC address of the client computer if you are unable to visit the client computer physically. But this is only a fraction of what is required from you in this question. You also need to find out the exact FTP commands that were executed and not just the source of these commands, without disrupting operations on Certkiller 1.

Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 198, 543
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 3, pp. 140, 144, 145.

QUESTION 644
You are the administrator of an Active Directory domain. The network contains a Windows Server 2003 domain controller named Certkiller 1.
Users report that they experience intermittent delays when they log on to Certkiller 1. Administrators report that replication attempts between Certkiller 1 and other domain controllers are occasionally delayed.
You need to verify the cause of the intermittent connection delays to Certkiller 1. You also need to find out whether the problem is related to a hardware deficiency on Certkiller 1. You need to track these delays over a period of one day.
What should you do first?

A. Run the netdiag / verbose command to perform a network diagnostic test on Certkiller 1.
B. Run the replmon command to view the Active Directory replication status on Certkiller 1.
C. Use Network Monitor to view the network traffic packet contents between Certkiller 1 and all other computers.
D. Create a System Monitor counter to track the queue lengths on the network adapter on Certkiller 1.

Answer: D

Explanation: System monitor can display performance data about the local computer, or it can display performance data on one or more remote computers in real time. The System Monitor tool can also log a history of performance results over time for local or remote computers. To monitor system performance, you must specify performance objects, counters, and instances of those objects so that the System Monitor knows which areas of system performance to track and display. Thus option D would be best suited to verify the causes of intermittent connection delays to Certkiller 1.
Incorrect answers:
A: The netdiag command is used to run a diagnostics test against your server to see if anything is not working correctly, this does not mean causes of problems. It just states what is working and what is not. The verbose parameter will display the configuration of default gateways, dynamic IP addressing from DHCP, DNS, IP addressing and WINS. It is not used to verify the causes of intermittent connection delays.
B: Replication Monitor, i.e. the replmon command, is used to monitor the status of Active Directory replication between domain controllers. If zone information is stored within Active Directory, this also enables you to monitor replication between DNS servers. But this is not what is required in this scenario.
C: Network Monitor is a tool included with Windows Server 2003 used to monitor and capture network traffic. This is not what is needed to be verified.
Reference:
Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment

Exam Cram 2 (Exam 70-290), Chapter 6
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 551

QUESTION 645
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
You configure several Group Policy objects (GPOs) to enforce the use of IPSec for certain types of communication between specified computers.
A server named Certkiller 5 runs the Telnet service. A GPO is supposed to ensure that all Telnet connections to Certkiller 5 are encrypted by using IPSec. However, when you monitor network traffic, you notice that Telnet connections are not being encrypted.
You need to view all of the IPSec settings that are applied to Certkiller 5 by GPOs.
Which tool should you use?

A. The IP Security Policy Management console
B. The IP Security Monitor console
C. The Resultant Set of Policy console
D. Microsoft Baseline Security Analyzer (MBSA)

Answer: C

Explanation: The RSoP console is used in Windows Server 2003 to determine which IPSec policies are assigned-but are not being applied- to IPSec clients. The Windows XP implementation of the RSoP console does not support the display of IPSec policies.
RSOP provides a machine-specific overview of the Policy state for the defined machine. It is a term for the resulting (effective) group policies that are applied to a computer and user. You will thus be able to see which IP settings are applied to Certkiller 5 by means of Group Policy Objects.
Incorrect answers:
A: The IPSec Security Management console displays the active IPSec policy name. This means that you will not be able to view all the IPSec policies that are applied.
B: One makes use of the IP Security Monitor tool to validate that communications between hosts are indeed secure. It provides information such as which IPSec policy is active and whether a secure communication channel is being established between computers. This is not the same as checking all IPSec settings that are applied.
D: The MBSA is not used to check IPSec policies that are applied.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 867
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 15, p. 26

QUESTION 646

You are the Network Administrator for Certkiller .com. The network contains 1,200 Windows XP Professional computers and the Windows Server 2003 computers shown in the following table.

Server name	Role
Certkiller A	Domain Controller, DNS Server
WINS1	WINS Server
Certkiller 1	File server
Certkiller 2	Application server
Certkiller 3	DHCP server

Client computers receive IP addresses from Certkiller 3. Client computers require NetBIOS over TCP/IP to access an application on Certkiller 2. All servers use static IP addresses. Certkiller 1 stores confidential company documents.

You run network monitoring software, and you notice NetBIOS queries to Certkiller 1. The queries are from source IP addresses that are not in use on your network. You suspect that an intruder is attempting to access Certkiller 1 over NetBIOS ports. You need to prevent access to Certkiller 1 through NetBIOS ports.

What should you do?

A. On Certkiller 3, in the DHCP server options, select the 001 Microsoft Disable Netbios Option option.

B. On WINS1, delete the WINS record for Certkiller 1.

C. On Certkiller 1, on the Advanced TCP/IP properties dialog box, select the Disable NetBIOS over TCP/IP option.

D. On Certkiller 1, on the Internet Protocol (TCP/IP) properties dialog box, remove the WINS1 IP address.

E. On all servers, in the Internet Connection Firewall Services tab, add a service entry for the NetBIOS ports

Answer: C

Explanation: NetBIOS is enabled by default for all local area connections in Windows Server 2003. However, if you have implemented DNS on your network and do not need to provide compatibility with versions of Windows earlier than Windows 2000, you have the option of disabling NetBIOS for any or all network connections. The main advantage of disabling NetBIOS is improved network security. NetBIOS as a service stores information about network resources that can be collected by any host through broadcastbased queries. Feasibly, this information could be exploited by a malicious intruder. Another advantage of disabling NetBIOS is that doing so can simplify administration by reducing the number of naming infrastructures that you must configure, maintain, and support. Thus to prevent an intruder from accessing Certkiller 1 through NetBIOS ports, disabling the NetBIOS over TCP/IP option would be the answer.

Incorrect answers:

A: NetBIOS is not a DHCP issue but rather a WINS issue.

B: Deleting the WINS record for Certkiller 1 on WINS1 is not going to help in this scenario. Windows Internet Name Service (WINS) is used to centralize the process of registering and resolving NetBIOS names to IP addresses. Centralizing the processes is not the same as preventing NetBIOS queries to Certkiller 1.

D: Removing WINS1 IP address from the Certkiller 1 TCP/IP properties dialogue box will not prevent NetBIOS queries to Certkiller 1.
E: Adding a service entry for the NetBIOS ports on all servers will defeat the purpose of preventing unauthorized NetBIOS intruding on Certkiller 1 that hosts the confidential files.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced training kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, 2003, Chapter 4, p. 8
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 2

QUESTION 647
You are the network administrator for Certkiller .com. The network contains 12 Windows Server 2003 computers and 300 Windows XP Professional computers.
Three servers named Certkiller 4, Certkiller 5, and Certkiller 6 run a critical business application. When performing performance baselining on these three servers, you notice that Certkiller 6 has a larger number of concurrently connected users at any given moment than Certkiller 4 or Certkiller 5. The additional workload is causing performance problems on Certkiller 6. You need to identify which client computers are connected to Certkiller 6.
You plan to run Network Monitor on Certkiller 6 to capture all packets sent to Certkiller 6. 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: Use the Capture Buffer Settings dialog box to increase the Network Monitor buffer size setting from the default of 1 MB. Performing this configuration would result in the buffer being less likely to become full. Data would therefore not be overwritten. The frame size setting should be decreased from its default setting of 65,472 bytes so that additional frames can be stored prior to the buffer becoming full.
Incorrect Answers:
A: Configuring the Network Monitor display filters would not assist in meeting the requirements.
B: This would also not assist in meeting the requirements.
D: The buffer size has to be increased.
E: The frame size has to be decreased.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing,

Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 841

QUESTION 648

You are a network administrator for Certkiller .

A Windows Server 2003 computer named Certkiller SrvA is exhibiting connectivity problems. You monitor Certkiller SrvA by using System Monitor and Network Monitor. While monitoring, you notice that Certkiller SrvA 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 Certkiller SrvA during the capture have not been captured.

You need to ensure that the impact of monitoring on Certkiller SrvA 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: The question states that the central processing unit runs on 95% on average. This means that there is probable not enough resources to the network Monitor to make use of. Running Network Monitor in dedicated capture mode frees resources on the computer for capturing data. This results in fewer frames being dropped. The capture statistics are not displayed or refreshed because the frames are copied to the capture buffer.

Incorrect Answers:

A: Running the diskperf command will not solve your problem. The problem is resources not being available for the Network Monitor to work optimally.

C: Filtering would mean that you will be selective in what you want to have filtered, with the result that selected frames will be dropped.

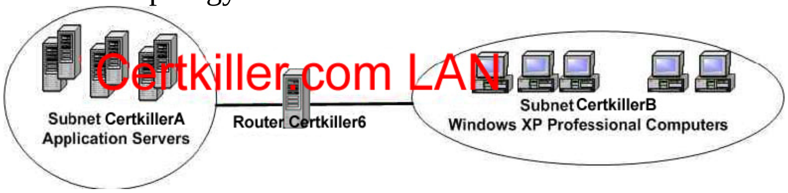
D: Increasing the buffer size will not necessarily work as the buffer size determines how much data you can capture at one time before ceasing to gather data. It has nothing to do with the 95% CPU usage.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 841

QUESTION 649

Network topology exhibit:



You are the network administrator for Certkiller .com. The Certkiller network consists of two subnets named subnet Certkiller A and subnet Certkiller B, which are connected by a Windows Server 2003

computer named Certkiller 6. Certkiller 6 has two network adapters and is configured as a LAN router. Certkiller 6 has Routing and Remote Access enabled.
Subnet Certkiller A contains six Windows Server 2003 computers that are configured as application servers. Subnet Certkiller B contains only Windows XP Professional computers. The relevant portion of the network is shown in the exhibit.
To improve security, you plan to configure IP packet filters on Certkiller 6. In order to create the correct IP packet filters on Certkiller 6, you need a list of all network protocols and ports that are used in communications between the application servers and the Windows XP Professional computers.
In order to gather the list of protocols and ports, you want to monitor the traffic that is forwarded by Certkiller 6 during a 24-hour period.
What should you do on Certkiller 6?

A. Run the netstat.exe command at the end of a 24-hour period.
B. Run the net session command at the end of a 24-hour period.
C. Use Network Monitor to perform a capture during a 24-hour period.
D. Use System Monitor to log all counters for the Network Interface object during a 24-hour period.

Answer: C

Explanation: You need to perform a capture during a 24-hour period by making use of Network Monitor if you want to gather the list of protocols and ports and monitor the traffic forwarded during a 24-hour period. You use Network Monitor to capture and display the frames that a computer running Windows 2000 Server receives from a local area network (LAN). Network administrators can use Network Monitor to detect and troubleshoot networking problems that the local computer may experience. Network Monitor is a tool included with Windows Server 2003 used to monitor and capture network traffic. It is useful for troubleshooting network problems.
Incorrect Answers:
A: Running the netstat.exe command will show information about existing network connections and network activity.
B: The net session command will not yield the correct information.
D: You do not want to log all the counters for the Network Interface object.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 9:68, 855

QUESTION 650
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
The network contains a Web server named Certkiller 1 that runs IIS 6.0 and hosts a secure Web site. The Web site is accessible from the intranet, as well as from the Internet. All users must authenticate when they connect to Certkiller 1. All servers on the Internet must use a secure protocol to connect to the Web site. Users on the intranet do not need to use a secure protocol.
You need to verify that all users are using a secure protocol to connect to Certkiller 1 from the Internet.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Monitor the events in the application log on Certkiller 1.
B. Monitor the events in the security log on Certkiller 1.
C. Monitor the Web server connections on Certkiller 1 by using a performance log.
D. Monitor network traffic to Certkiller 1 by using Network Monitor.
E. Monitor the IIS logs on Certkiller 1.

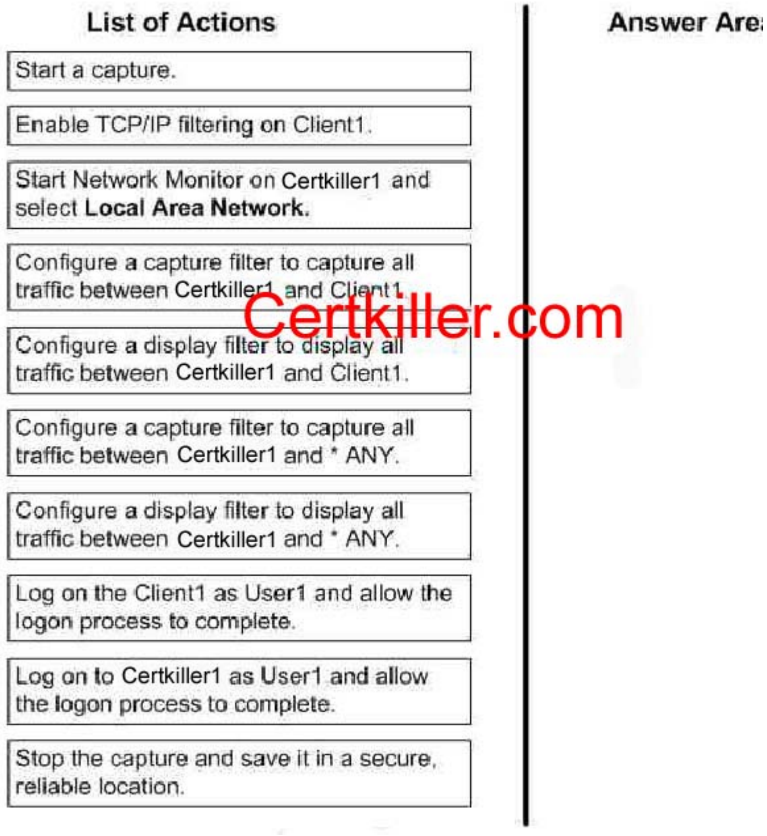
Answer: D, E

Explanation: To verify whether all users are making use of a secure protocol to connect to the server1 from the Internet, you must use the Network Monitor. Network Monitor is a software-based traffic analysis tool that allows a user to perform these tasks:

- Capture frames directly from the network
- Display and filter captured frames, immediately after capture or at a later time
- Edit captured frames and transmit them on the network (full version only)
- Capture frames from a remote computer (full version only)

Incorrect Answers:
A: Events in the application log on Certkiller 1 is accessible through the Event Viewer, only displays events pertaining to applications and programs running on the computer. You do not need this specific log.
B: Events in the security log, accessible through the Event Viewer, on Certkiller 1, displays contains events pertaining to security as defined in the Audit policy. E.g. this includes successful logons, resource access, and use of user rights. This is not what is asked for in the question.
C: Monitoring Web server connections on Certkiller 1 through a performance log is not what you want to accomplish, you need to verify whether all users are using a secure protocol to connect to Certkiller 1 from the Internet.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 4
J. C. Mackin, Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft Press, Redmond, 2003, 1: 26, 3: 3.

QUESTION 651
You are the administrator of an Active Directory domain. The domain contains a Windows Server 2003 computer named Certkiller 1. Certkiller 1 functions as a domain controller and a DNS server. The domain also contains a Windows XP Professional client computer named Client1.
You need to establish a detailed record of all the communications that occur when a typical member of the Domain Users group named User1 logs on to the Active Directory domain from Client1. You might need to use this information as a troubleshooting tool if communications between Client1 and Certkiller 1 are disrupted or degraded. You want to use Network Monitor to obtain this baseline information.
What should you do?
To answer, move the appropriate actions from the list of actions to the answer area, and arrange them in to correct order.



List of Actions

Start a capture.

Enable TCP/IP filtering on Client1.

Start Network Monitor on Certkiller1 and select **Local Area Network.**

Configure a capture filter to capture all traffic between Certkiller1 and Client1.

Configure a display filter to display all traffic between Certkiller1 and Client1.

Configure a capture filter to capture all traffic between Certkiller1 and * ANY.

Configure a display filter to display all traffic between Certkiller1 and * ANY.

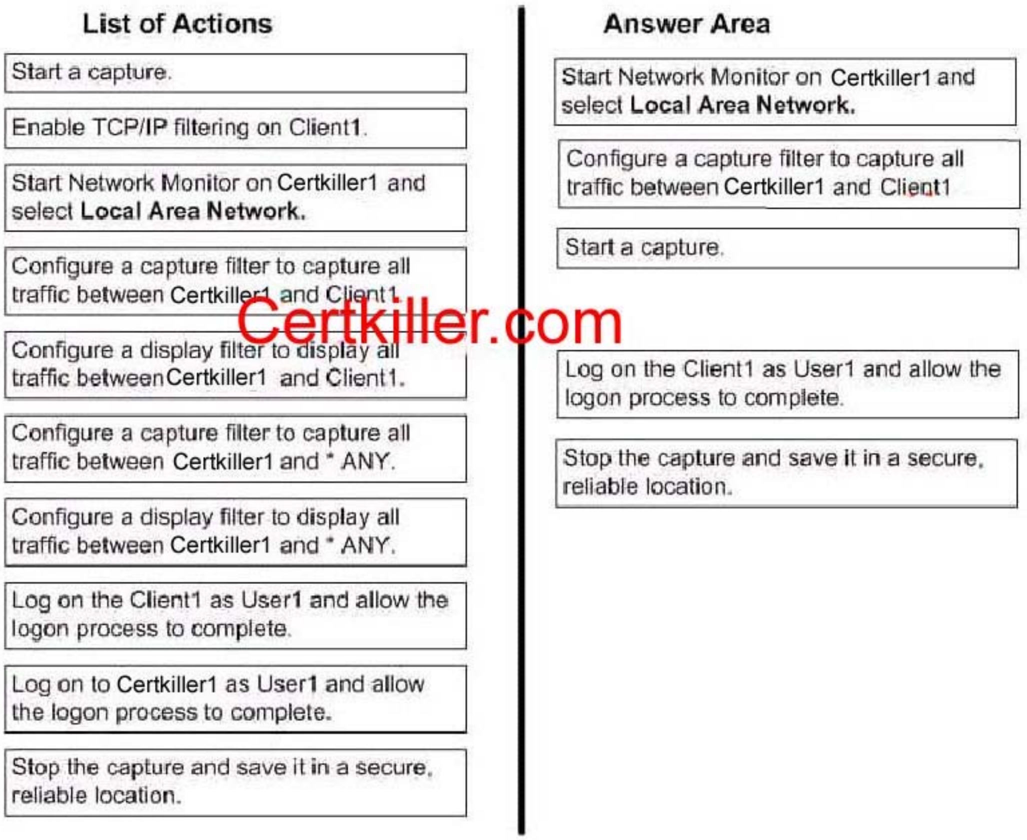
Log on the Client1 as User1 and allow the logon process to complete.

Log on to Certkiller1 as User1 and allow the logon process to complete.

Stop the capture and save it in a secure, reliable location.

Answer Are

Answer:



List of Actions

- Start a capture.
- Enable TCP/IP filtering on Client1.
- Start Network Monitor on Certkiller1 and select **Local Area Network.**
- Configure a capture filter to capture all traffic between Certkiller1 and Client1.
- Configure a display filter to display all traffic betweenCertkiller1 and Client1.
- Configure a capture filter to capture all traffic between Certkiller1 and * ANY.
- Configure a display filter to display all traffic between Certkiller1 and * ANY.
- Log on the Client1 as User1 and allow the logon process to complete.
- Log on to Certkiller1 as User1 and allow the logon process to complete.
- Stop the capture and save it in a secure, reliable location.

Answer Area

- Start Network Monitor on Certkiller1 and select **Local Area Network.**
- Configure a capture filter to capture all traffic between Certkiller1 and Client1
- Start a capture.
- Log on the Client1 as User1 and allow the logon process to complete.
- Stop the capture and save it in a secure, reliable location.

Explanation: Once Network Monitor is installed, users can capture all the frames sent to, or retained by the network adapter of the computer on which it is installed to a file. 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 can include starting a capture, ending a capture, or starting a program.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 542

QUESTION 652

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 computers and Windows XP Professional computers.

All confidential company files are stored on a file server named Server CK5 . The written company security policy states that all confidential data must be stored and transmitted in a secure manner. To comply with the security policy, you enable Encrypting File System (EFS) on the confidential files. You also add EFS certificates to the data decryption field (DDF) of the confidential files for the users who need to access them.

While performing network monitoring, you notice that the confidential files that are stored on

Server CK5 are being transmitted over the network without encryption.
You need to ensure the data is encrypted over the network.
What are two possible ways to accomplish this goal? (Each correct answer presents a complete solution. Choose two)

A. Enable offline files for the confidential files that are stored on Server CK5 , and select the Encrypt offline files to secure data check box on the client computers of the users who need to access the files.
B. Use IPSec encryption between Server CK5 and the client computers of the users who need to access the confidential files.
C. Use Server Message Block (SMB) signing between Server CK5 and the client computers of the users who need to access the confidential files.
D. Disable all LM and NTLM authentication methods on Server CK5 .
E. Use IIS to publish the confidential files.
Enable SSL on the IIS server.
Open the files as a Web folder.

Answer: B, E

Explanation: You can use IPSEC to encrypt network traffic or you can use SSL to encrypt network traffic.
Short for Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL. Many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.
Incorrect Answers:
A: Confidential files should not be allowed to be accessed when offline. It is a security risk that can be avoided. Thus this option will not suffice.
C: SMB is primarily used for file and print sharing, but is also used for sharing serial ports and abstract communications technologies such as named pipes and mail slots, making it inapplicable in this case.
D: LAN Manager and NTLM authentication are used by Microsoft systems for network authentication. Implementing Secure and Highly Secure security templates affects network security by altering the typical LAN Manager and NTLM authentication request protocols. Disabling LM and NTLM authentication methods on Server CK5 will thus not work in this scenario.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 37, 785

QUESTION 653
You are the network administrator for Certkiller .com. The network contains a Windows Server 2003 Web server named WebServer CK1 . WebServer CK1 is connected to the Internet by means of a dedicated link.
You are responsible for monitoring the bandwidth utilization of WebServer CK1 . You run a System Monitor log on WebServer CK1 , which monitors the Bytes Total/sec counter on the Network Interface object. The sample rate for the counter is set to 15 seconds. The log is archived once each day.

The size of the System Monitor log is becoming too large for the available disk space. You need to reconfigure the System Monitor log settings to reduce the amount of data that is captured.
What should you do?

A. Retain the current counter, but set the sample rate to 5 seconds.
B. Retain the current counter, but set the sample rate to 60 seconds.
C. Change the counter to Total Bytes, and set the sample rate to 15 seconds.
D. Change the counter to Current Bandwidth, and set the sample rate to 60 seconds.

Answer: B

Explanation: The Network Interface Bytes Total/Sec counter measures the total number of bytes that are sent/ received from the network interface. It incorporates all network protocols. You use less processor cycles when you reduce the sampling frequency because the slower a counter is sampled, the less the CPU has to be utilized.
Incorrect Answers:
A: The quicker the time setting, the more CPU intensive it becomes to run System Monitor. Thus setting the sample rate to 5 seconds will result in too much data being captured.
C: Viewing a different log will not yield the required information. You need the amount of data that is captured reduced. The time setting of 15 seconds is thus irrelevant to this scenario.
D: Setting the sample rate to 60 seconds is ideal. However, if you change the counter to Current Bandwidth you will not get the desired information.
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, 2003, Chapter 12, p. 479

QUESTION 654
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains 25 Windows Server 2003 computers and 6,000 Windows XP Professional computers.
The written company security policy states that network traffic to Web servers must be audited on a regular basis. A server named Certkiller 1 is configured as a Web server on Certkiller 's intranet. You install Network Monitor Tools from a Windows Server 2003 product CD-ROM on Certkiller 1.
You run Network Monitor on Certkiller 1 for three hours. When you stop the network capture, you see that Network Monitor captured over 40,000 frames. As you look at the captured frames, you notice that an extremely large number of TCP connection requests have all come from the 131.107.0.1 IP address.
In Network Monitor, you need to view only the frames for network traffic that are captured between Certkiller 1 and the 131.107.0.1 IP address.
What should you do?

A. Create an Address Capture filter for all network traffic between Certkiller 1 and the 131.107.0.1 IP address.
B. Create a Fin Frame Expression filter for network traffic captured between Certkiller 1 and the 131.107.0.1 IP address.

C. Create an Address Display filter for all network traffic captured between Certkiller 1 and the 131.107.0.1 IP address.
D. Create a Pattern Match capture trigger for the 131.107.0.1 IP address.

Answer: C

Explanation: Once Network Monitor is installed, users can capture all the frames sent to, or retained by the network adapter of the computer on which it is installed to a file. 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 can include starting a capture, ending a capture, or starting a program.
A capture filter functions like a database query that you can use to specify the types of network information you want to monitor. For instance, to view only a specific subset of computers or protocols, you can create an address database, and use the database to add addresses to your filter. The filter can then be saved to a file. You save both buffer resources and time by filtering frames. Later, if necessary, you can load the capture filter file and use the filter again.
Incorrect Answers:
A, B, D: An address capture filter, a Fin Frame Expression filter or a Pattern Match capture trigger will not yield the correct information that you need to view.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 833

QUESTION 655
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain consists of 25 Windows Server 2003 computers and 6,000 Windows XP Professional computers.
A server named Certkiller 3 is configured as a DNS server. You receive reports that host name resolution for computers on the network is slower than usual. To help find the cause of the problem, you need to capture all network traffic that is being sent to and from Certkiller 3.
You install Network Monitor Capture Utility (Netcap.exe) from a Windows XP Professional product CD-ROM on a client computer named client1. You need to capture, view, and analyze all network traffic that is sent to and from Certkiller 3.
What should you do?

A. Install the Network Monitor driver on all computers on the network. Run Network Monitor on Client1 to capture network traffic.
B. Run System Monitor on Certkiller 3. Create a counter log to capture network traffic to Certkiller 3 by using the Network Interface object and the Packets Received / sec counter.
C. Install the Network Monitor Tools from a Windows Server 2003 product CD-ROM on Certkiller 3. Run Network Monitor to capture network traffic.
D. Install the Tcpip.dll protocol parser on Certkiller 3. Run Netcap.exe on client1 to capture network traffic.

Answer: C

Explanation: Windows Server 2003 also has a Network Monitor tool that can monitor data travelling between the monitored computer and the rest of the network, and not network traffic in general. Thus this is the tool to use when you need to capture, view, and analyze all network traffic that is sent to and from Certkiller 3. Since the client computers run Windows XP Professional you need to install the network Monitor tools from a Windows Server 2003 product CD-ROM.
Incorrect Answers:
A: It is correct to run Network Monitor to capture network traffic, but this option will yield improper results for you since it suggests that the Network Monitor driver alone has to be installed on all the computers on the network and it is stated in the question that the client computers run Windows XP Professional and the Servers operate in a Windows Server 2003 environment.
B: System Monitor is a tool included with Windows Server 2003 that can be used to monitor the real-time performance of system components as well as services and applications. System Monitor can be used to collect and view real-time performance data, view data saved in a counter log, and present captured data using various views. But it is Network Monitor that monitor data travelling between the monitored computer and the rest of the network, and not network traffic in general.
D: Installing Tcpip.dll protocol parser on Certkiller 3 will not assist you in your task.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 4

QUESTION 656
You are the network administrator for Certkiller .com. The Mumbai office is currently connected to the corporate WAN by using a Windows Server 2003 computer named Certkiller 5.
Certkiller 5 is configured as a dial-up router. Certkiller 5 has two network adapters. One network adapter connects to the Ethernet LAN. The other network adapter is a broadband networking device.
Certkiller .com plans to increase the number of employees in the Mumbai office by at least 25 percent.
You need to confirm that the current network bandwidth of the broadband connection will be sufficient for the future expansion of the Mumbai office.
You want to use System Monitor on Certkiller 5 to find out the current utilization of the broadband network connection.
What should you do?

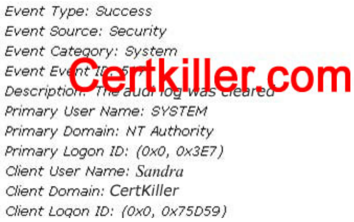
A. Monitor the Bytes Total/sec counter on the Network Interface Object.
B. Monitor the Bytes Total/sec counter on the Server Object.
C. Monitor the Server\\Packets/sec counter on the Server Object.
D. Monitor the Current Bandwidth counter on the Network Interface Object.

Answer: A

Explanation: The following is a counter that is useful for monitoring the network subsystem: Network Interface > Bytes Total/Sec. It measures the total number of bytes that are sent or received from the network interface and includes all network protocols. It incorporates all network protocols. This is the counter on the System Monitor to use if you want to find out the current utilization of the broadband connection.
Incorrect answers:

B & C: The Server Object is not going to yield the proper information for your purposes.
D: This is the correct object to monitor, but the wrong counter for the purposes of this question.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows
Server 2003, Sybex Inc. Alameda, 2003, p. 1240
James Chellis, Paul Robichaux & Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2003, p. 274

QUESTION 657
Exhibit:
You are the network administrator for Certkiller .com. All servers run Windows Server 2003.



```
Event Type: Success
Event Source: Security
Event Category: System
Event Event ID: 517
Description: The audit log was cleared
Primary User Name: SYSTEM
Primary Domain: NT Authority
Primary Logon ID: (0x0, 0x3E7)
Client User Name: Sandra
Client Domain: CertKiller
Client Logon ID: (0x0, 0x75D59)
```

You and an administrator named Sandra are members of the Administrators group on a server named Certkiller 2. Sandra is responsible for monitoring Certkiller 2. She periodically reviews the system and application logs. You are responsible for performing all administrative functions on Certkiller 2. The domain administrators periodically review the security log to investigate unauthorized access attempts.
Certkiller .com's written security policy states that all events in the security log must be retained until they are archived. You archive and clear the logs on Certkiller 2 once each month.
When you open the security log on Certkiller 2, you notice that the log has fewer events than usual. The oldest entry in the audit log contains the information displayed in the exhibit.
You must ensure that the Certkiller .com security policy is enforced.
What should you do on Certkiller 2?

A. In the local security policy, assign the Manage auditing and security log user right to your user account and remove all other entries.
B. In the local security policy, configure audit settings to enable Audit privilege use (success and failure).
C. Assign the System group the Deny - Full Control permissions for the Secevent.evt file.
D. Remove Sandra's user account from the Administrators group and add her user account to the Power users group.
E. In the properties of the security log, select the Do not overwrite events (clear log manually) option.

Answer: D

Explanation: The Power Users group only exists as a machine local group on 2000 and XP Workstations, and on nondomain controller servers. Members have a subset of the Administrator's rights. Power users can create user accounts and local groups and can manage the membership of Users, Power Users, and Guests, as well as administer other users and groups that they have created. Since Sandra is responsible for periodically reviewing the system and application logs, she does not have to be a member of the

Administrators group. The exhibit shows that Sandra has been the last entry to have been logged. If you want all events in the security log to be retained until archival, then you should add Sandra to the Power users group. Being a member of the Power users group will grant her enough permissions to carry out her tasks while complying with the company security policy.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows
Server 2003, Sybex Inc. Alameda, 2003, p. 721

QUESTION 658
You are the network administrator for Certkiller .com. The network contains a DNS server named Certkiller 1.
Certkiller 1 is configured to resolve queries for external internet resources. Certkiller 1 also hosts the Certkiller .com internal zone for Active Directory.
Users report that they are directed to the wrong Web site when browsing for well-known Internet Web sites.
You need to minimize the occurrence of unexpected results when users browse the Internet in the future. You also need to minimize disruption to users.
What should you do?

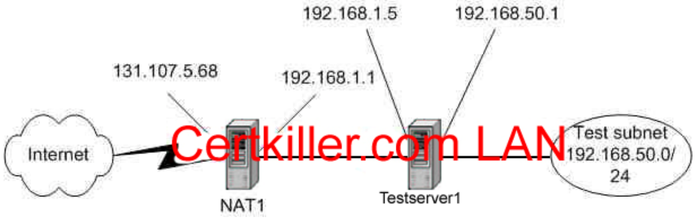
A. Enable the Disable recursion setting in the advanced properties of Certkiller 1.
B. Enable Fail on load if bad zone data setting in the advanced properties of Certkiller 1.
C. Enable the Secure cache against pollution setting in the advanced properties of Certkiller 1.
D. Enable the Enable automatic scavenging of stale resource records setting in the advanced properties of Certkiller 1 and set it to 7 days.

Answer: C

Explanation: When the Secure cache against pollution setting is disabled, all records received in response to DNS queries are cached. This is true even when the records do not match to a queried domain name. Enabling the Secure cache against pollution setting disables the ability to pollute the DNS cache with incorrect information, and spoof DNS queries. With Windows Server 2003 the default setting is that caches are secured against pollution. This will then prevent users that browse the Internet from being directed to the wrong websites.
Incorrect Answers:
A: Checking this option enables the use of recursive forwarders) lookups on the entire server regardless of conditional settings on the Forwarders tab. It disables the use of forwarders. This is not what is required in this scenario.
B: By default, Windows Server 2003 DNS servers load their zones regardless of any errors in zone files. The Fail on load if bad zone data option can be used to alter that behavior so that the DNS server service logs errors, but fails to load a zone file containing records data that is determined to have errors. However in this case it is a matter of queries not being resolved.
D: Because stale resource records can accumulate within a zone over a period of time. E.g., if a computer registers its own resource record and is shut down improperly, the record might not be removed from the zone file. Scavenging stale resource records can eliminate any problems, such as outdated information. Thus Enabling automatic scavenging of stale resource records and setting it to 7 days may still allow

users to be directed to the wrong web sites. Information can still become outdated within 7 days. You need to secure the cache from pollution.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 496-497
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 3, pp. 285, 291

QUESTION 659
You are the network administrator for Certkiller .com. All servers run Windows Server 2003.
You implement a new test subnet for testing purposes. You connect the test subnet to the corporate network by using a multihomed server named Testserver1 that has the Routing and Remote Access service enabled. All Internet access for Certkiller is provided by a Network Address Translation (NAT) server named NAT1. The relevant portion of the network is shown in the exhibit.



You notice that computers on the test subnet cannot connect to any Internet resources by host name or IP address. From a computer on the test subnet, you successfully ping 192.168.1.1.
You need to configure the network so that computers on the test subnet can access the Internet.
What should you do?

A. Change the default gateway to 192.168.1.1 for all computers on the test subnet.
B. Change the default gateway on Testserver1 to 192.168.1.1.
C. Configure NAT on Testserver1.
D. Run the route add command on all computers on the test subnet.

Answer: B

Explanation: For the test subnet computers to be able to access the Internet they need to have Testserver1's default gateway to be 192.168.1.1 since it already has the Routing and Remote Access service enabled and NAT services is provided by NAT1 as illustrated in the exhibit and NAT1 is connected to the Internet.
Incorrect Answers:
A: The default gateway on the Testserver1 has to be changed to 192.168.1.1 and not the other way around.
C: Configuring Network Address Translation on Testserver1 is obsolete since Certkiller is provided by a Network Address Translation (NAT) server named NAT1.
D: When you run the route-add command, you are actually configuring the computers with a static IP address. You can run into trouble with static IP addresses in a number of situations. This is impractical since NAT1 provides Network Address Translation.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing,

Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 138

QUESTION 660

You are the network administrator for Certkiller .com. All servers run Windows Server 2003.
You configure a server named Certkiller 1 with Routing and Remote Access. Certkiller 1 functions as a Network Address Translation (NAT) server. You configure two network connections on Certkiller 1, as shown in the following table.

Connection name	**IP address**	**Connected to**
Local Area Connection	192.168.1.254	Internal network
Local Area Connection 2	131.107.2.67	Internet

Users report that they cannot connect to the Internet. They can successfully access Certkiller 1 from remote subnets on the network.
You need to configure Certkiller 1 so that users can connect to the Internet.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

A. Configure Local Area Connection at the private interface.
B. Configure Local Area Connection as the public interface.
C. Configure Local Area Connection 2 as the private interface.
D. Configure Local Area Connection 2 as the public interface.
E. Enable NAT on the public interface.
F. Enable Basic Firewall on Local Area Connection.
G. Enable Basic Firewall on Local Area Connection 2.

Answer: A, D, E

Explanation: NAT is one of the protocols supported by the Routing and Remote Access service in Windows Server 2003. If you use NAT, you must include the Routing and Remote Access service in your solution. The features of NAT provide you with a simple solution for Internet connectivity. Network Address Translation (NAT) is a method of allowing computers internal to your network that has been given non-public addresses to communicate with computers on the Internet.
NAT is an appropriate solution for Internet connectivity when:
• Requirements for Internet access and access to the private network do not require restrictions on a user-by-user basis.
• The private network consists of any number of users in a non-routed environment.
• The organization requires private addressing for the computers on the private network.
Incorrect Answers:
B: A Local Area Connection is usually not the public interface but rather the private interface.
C: In this scenario Local Area Connection 2 is not the private interface because it is connected to the Internet.
F, G: Enabling a firewall on either Local Area Connection or Local Area Connection 2 is not what is needed. You must enable NAT on the Public Interface.

Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, 2003, pp. 1:11, 9:45-47

QUESTION 661
You are the network administrator for Certkiller .
You work in the Certkiller 's branch office in Cape Town. The network in your office consists of 40 Windows XP Professional desktop computers and one Windows Server 2003 computer named Certkiller 3. Certkiller 3 connects to the Internet through a 512-Kbps leased line. The main office of the company is in Johannesburg.
Users of the desktop computers in the Cape Town office are developers who are developing a new software product. You want these users to place daily builds of the product in a shared folder on Certkiller 3. You want developers in the Johannesburg office to be able to download the daily builds from Certkiller 3 by using FTP.
You install IIS on Certkiller 3 and configure the FTP site so that it is available to the developers in the Johannesburg office. However, when you monitor inbound Internet connection attempts to Certkiller 3, you notice many attempted HTTP connections.
You want to secure Certkiller 3 so that it is not susceptible to malicious Internet users. Certkiller 3 must also connect to the Internet to use Windows Update and to download virus definition updates. You do not want to purchase additional hardware or software.
What should you do on Certkiller 3?

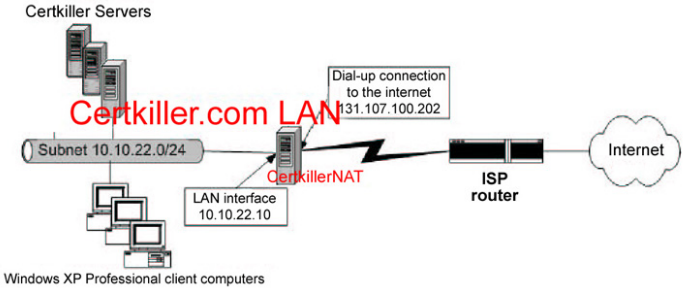
A. Enable Internet Connection Sharing (ICS).
B. Configure port filtering on the network adapter to allow only TCP port 80 and TCP port 21.
C. Enable Internet Connection Firewall (ICF) and create service setting in the Internet Connection Firewall settings that allows:
Internal and external TCP port 21 to Certkiller 3.
Internal and external TCP port 80 to Certkiller 3.
D. Enable Internet Connection Firewall (ICF) and select the FTP Server check box in the Services tab. Enter Certkiller 3 as the server hosting the FTP services.

Answer: D

Explanation: To avoid purchasing additional hardware or software, the Internet Connection Sharing (ICS) feature included in Windows Server 2003 should be utilized to provide simplified NAT services to clients in the private network. ICS is a form of NAT and is simpler to implement than NAT. FTP is used to copy files between two computers on the Internet. This would be for the daily builds of the product that is placed in the shared folder. To enable developers in the Johannesburg office to download the daily builds from Certkiller 3 using FTP, you have to select the FTP Server check box in the Services tab and specify Certkiller 3 as the server hosting the FTP services.
Incorrect Answers:
A: ICS is a limited implementation of NAT. Basically ICS allows one public address to be translated for the internal private subnet systems. Also, ICS provides a form of dynamic address allocation to clients on the network in a way similar to DHCP. This dynamic address allocation does not provide any configuration options or features to control it when compared to standard DHCP. ICS also provides

name resolution for the ICS clients. This option is thus not the answer since Certkiller 3 hosts the FTP site and is installed with IIS.
B: Port filtering on the adapter to allow only port 21 and port 80-traffic is risky because TCP Ports 20 and 21 are well-known port numbers and hackers often try to exploit these ports. Port 80 is for HTTP and thus cannot be disabled since you would Certkiller 3 is configured with IIS and has the shared folder that is supposed to be available to the remote FTP server.
C: Enabling ICF and configuring the settings to allow internal as well as external port 21- and port 80-traffic to Certkiller 3 would not be advisable since Certkiller 3 also hosts shared files for the FTP server.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Chapter 9, Syngress Publishing Inc., Rockland, 2003, pp. 42, 519 - 528, 770

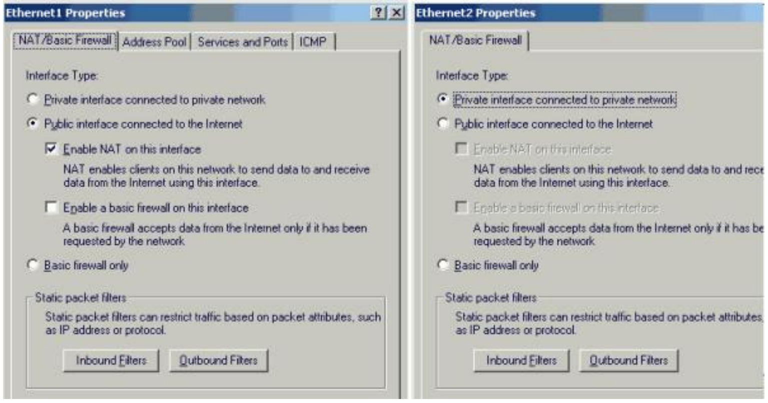
QUESTION 662
You are the network administrator for Certkiller .com. The network configuration is shown in the Network exhibit.


Certkiller Servers
Certkiller.com LAN
Dial-up connection to the internet 131.107.100.202
Subnet 10.10.22.0/24
CertkillerNAT
LAN interface 10.10.22.10
ISP router
Internet
Windows XP Professional client computers

A DHCP server on the local subnet is configured to assign IP addresses to client computers in the 10.10.22.20 - 10.10.22.254 range.
All client computers connect to the Internet by using the server named Certkiller NAT.
Certkiller NAT is a Windows 2003 Server that has Routing and Remote Access installed.
Certkiller NAT has the NAT/Basic Firewall routing protocol enabled. The network interfaces on Certkiller NAT are configured as shown in the following table.

Interface name	IP address	Connect to
Ethernet1	10.10.22.10	LAN
Ethernet2	131.107.100.202	Internet

The configuration of the NAT/Basic Firewall routing on Certkiller NAT is shown in the NAT Configuration exhibit:



Ethernet1 Properties

NAT/Basic Firewall | Address Pool | Services and Ports | ICMP

Interface Type:
○ Private interface connected to private network
● Public interface connected to the Internet
☑ Enable NAT on this interface
NAT enables clients on this network to send data to and receive data from the Internet using this interface.
☐ Enable a basic firewall on this interface
A basic firewall accepts data from the Internet only if it has been requested by the network
○ Basic firewall only

Static packet filters
Static packet filters can restrict traffic based on packet attributes, such as IP address or protocol.
Inbound Filters | Outbound Filters

Ethernet2 Properties

NAT/Basic Firewall

Interface Type:
● Private interface connected to private network
○ Public interface connected to the Internet
☐ Enable NAT on this interface
NAT enables clients on this network to send data to and rece
data from the Internet using this interface.
☐ Enable a basic firewall on this interface
A basic firewall accepts data from the Internet only if it has be
requested by the network
○ Basic firewall only

Static packet filters
Static packet filters can restrict traffic based on packet attributes,
as IP address or protocol.
Inbound Filters | Outbound Filters

Client computers are unable to connect to the Internet

You run the ping command from a command prompt on Windows XP Professional computer on the local network, and you receive the following result.

```
C:\>ping 10.10.22.10
Pinging 10.10.22.10 with 32 bytes of data:
Request timed out:
Request timed out:
Request timed out:
Request timed out:
Ping statistics for 10.10.22.10: Packets: Sent = 4, Received = 0, Lost =
4 (100% loss),
```

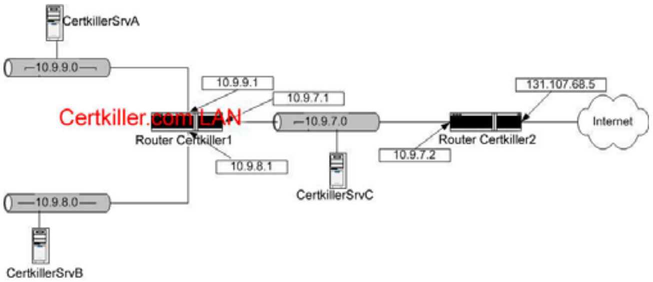
You need to ensure that client computers are able to connect to the Internet.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure the DHCP server to assign a default gateway of 131.107.100.202 to client computers.
B. Configure the DHCP server to assign a default gateway of 131.107.100.201 to client computers.
C. Configure the NAT/Basic Firewall interface type for Ethernet1 to be a private interface.
D. Configure the NAT/Basic Firewall interface type for Ethernet2 to be a public interface.
E. Configure the outbound port filters on Ethernet1 to allow all network protocols.
F. Configure the outbound port filters on Ethernet2 to allow all network protocols.

Answer: C, D

Explanation: You can determine from the exhibits that Ethernet1 is the interface connected to the LAN, and Ethernet2 is the interface connected to the Internet. Ethernet1 should be configured as the private interface, and Ethernet2 should be configured as the public interface.
Incorrect Answers:
A: The default gateway for the client computers should be set to 10.10.22.10.
B: The default gateway for the client computers should be set to 10.10.22.10.
E: This is not a port filter problem. The NAT interfaces are incorrectly configured.
F: This is not a port filter problem. The NAT interfaces are incorrectly configured.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 663
You are the network administrator for Certkiller .com. The relevant portion of the network is shown in the exhibit.



You need to configure Certkiller SrvA to communicate with Certkiller SrvB, Certkiller SrvC, and the Internet.

You open the TCP/IP properties of Certkiller SrvA, and you notice that the following default gateways are already configured in the order shown:

- 131.107.68.5
- 10.9.7.2
- 10.9.8.1
- 10.9.7.1
- 10.9.9.1

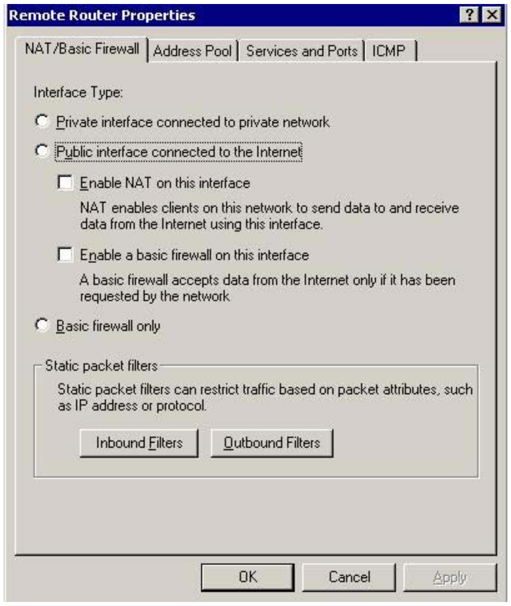
Which IP address or addresses should you remove from the default gateway addresses on Certkiller SrvA? (Choose all that apply)

A. 131.107.68.5
B. 10.9.7.2
C. 10.9.8.1
D. 10.9.7.1

Answer: A, B, C, D

Explanation: Certkiller Srv1 only needs one default gateway configured. This should be the address of the internal interface of the router. In this case, it is 10.9.9.1. All other default gateways should be removed.
Note: You would only configure multiple default gateways if there are multiple routers on the same subnet as your computer.
Reference:
James Chellis, Paul Robichaux and Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 54

QUESTION 664
You are the network administrator for Certkiller .com. 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 Certkiller Srv as a Network Address Translator (NAT) server.
Certkiller Srv is used to connect all computers on the company network to the Internet.
You remove both of the old 10-Mbps network adapters in Certkiller Srv, 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 Certkiller Srv, 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 Certkiller Srv.
On Certkiller Srv, 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.



Remote Router Properties

Interface Type:

○ Private interface connected to private network

○ Public interface connected to the Internet

□ Enable NAT on this interface

NAT enables clients on this network to send data to and receive data from the Internet using this interface.

□ Enable a basic firewall on this interface

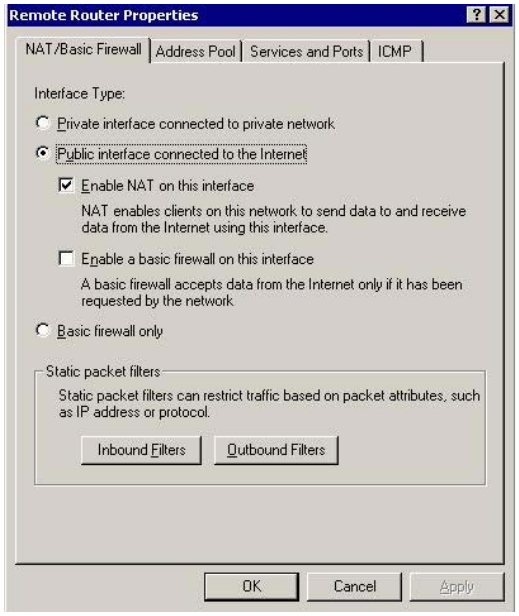
A basic firewall accepts data from the Internet only if it has been requested by the network

○ Basic firewall only

Static packet filters

Static packet filters can restrict traffic based on packet attributes, such as IP address or protocol.

Answer:



Remote Router Properties

Interface Type:

○ Private interface connected to private network

● Public interface connected to the Internet

☑ Enable NAT on this interface

NAT enables clients on this network to send data to and receive data from the Internet using this interface.

□ Enable a basic firewall on this interface

A basic firewall accepts data from the Internet only if it has been requested by the network

○ Basic firewall only

Static packet filters

Static packet filters can restrict traffic based on packet attributes, such as IP address or protocol.

Explanation: You have to select the Public interface connected to the internet checkbox because the network adapter connected to the Internet has a public IP address. The Enable a basic firewall on this interface check box should be checked to convert public IP addresses to internal private IP addresses.

Reference:

Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

James Chellis, Paul Robichaux and Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc. Alameda, 2003, pp. 356-357

QUESTION 665

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

Directory domain named Certkiller .com
A supplier named Adventure Works allows Certkiller to directly view the Adventure Works inventory. Adventure Works hosts a Web site that buyers can access through a VPN connection. Users in the purchasing department at Certkiller access the Adventure Works Web site every day. During each visit to http://inventory.adventure-works.com, users click on up to six hyperlinks to access the desired data. In conversation with Adventure Works network administrators, you find out that the http://inventory.adventure-works.com Web site should cause cookies to be created on the purchasing department users' computers. The cookies cause the Web page to display the "Your last search results" hyperlink. This hyperlink would be very useful for users in your purchasing department, because they usually search for the same data during each visit to the Web site. However, none of your users see this hyperlink.
You view the Internet Explorer Internet options on one of the purchasing department user's Windows XP Professional computers. The Privacy tab indicates a setting of High. Your company places a high priority on protecting user privacy and confidential data.
You want to allow cookies that will cause http://inventory.adventure-works.com to display the last search results for each purchasing department user.
How should you configure the Internet options on purchasing department computers?

A. In the Privacy tab, use the Sites button to allow http://inventory.adventure.works.com.
B. In the Privacy tab, change the privacy setting to Medium.
C. Set the advanced privacy settings to Override automatic cookie handling.
Block first-party cookies and accept third-party cookies.
D. Set the advanced privacy settings to Override automatic cookie handling.
Accept first-party cookies and block third-party cookies

Answer: A

Explanation: The Privacy tab indicates a setting of high, which is why cookies are being blocked. You need to Edit the settings in the Privacy tab to allow cookies that will cause http://inventory.adventure-works.com to display the last search results for each purchasing department user.
Incorrect Answers:
B: Changing the privacy setting to Medium has to be done by making use of the Edit button. Furthermore, making it Medium is not going to allow cookies. There will still be blocking of cookies.
C, D: Both these options still suggests some sort of blocking. Blocking is not what is required in this situation.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 850-853

QUESTION 666
You are the network administrator for Certkiller .com. Certkiller has six regional offices. The main office is in Seattle. The company network consists of a single Active Directory domain named Certkiller .com. The primary DNS server for the domain is in the Seattle office. Each regional office has the following servers.
• A secondary DNS server

- A DHCP server
- A Microsoft Internet Security and Acceleration (ISA) Server computer that connects to the LAN to the Internet

Company sales representatives visit each regional office several times each month. All sales representatives use Windows XP Professional portable computers.

Help desk technicians report that sales representatives are frequently unable to connect to the Internet when they visit a regional office. All sales representatives have instructions about how to change the ISA server in their Internet Explorer Options settings so that they can use the Internet in each regional office. However, the sales representatives often lose the instructions or express frustration with the need to frequently reconfigure their Internet Explorer settings.

You want to eliminate the need for the sales representatives to reconfigure their Internet Explorer settings each time they visit a different regional office. You configure a wpad.dat script file in each office. You create and configure a 252 Proxy Autodiscovery option in each DHCP server scope.

What should you do next?

A. Configure each Windows XP Professional portable computer's Internet Explorer LAN settings to Automatically detect settings.

B. On each Windows XP Professional portable computer, in the Internet Explorer LAN settings, select the Use automatic configuration script check box.

C. Create an alias (CNAME) resource record named Proxy for each ISA Server computer.

D. Configure the reverse lookup zone on the DNS server with pointer (PTR) resource records for each ISA Server computer.

Answer: B

Explanation: For a Web Proxy client or a Firewall client to connect to an ISA Server computer, you must configure the browser or Firewall client to forward Internet requests to a specific ISA Server computer. If the ISA Server computer becomes unavailable or you want to use a different ISA Server computer, you must change this configuration. When you enable automatic discovery, Firewall clients and Web Proxy clients can automatically detect an ISA Server computer on the network. Using automatic discovery can help you to minimize the time spent troubleshooting connection problems on client computers.

Web Proxy clients enable automatic discovery by using Web Proxy AutoDiscovery Protocol (WPAD) information. Firewall clients use Winsock Proxy AutoDetect Protocol (WSPAD). Both clients connect to an ISA Server computer and request configuration information after locating the ISA Server computer by using a WPAD entry on the Dynamic Host Configuration Protocol (DHCP) server or the Domain Name System (DNS) server. Automatic discovery is especially useful when you move your computer from one network to another. Thus this option will make the need for sales representatives to reconfigure their Internet Explorer settings each time they visit a different regional office, obsolete.

Incorrect Answers:

A: Automatically detect settings to be set on each portable computer is not eliminating the need to reconfigure Internet Explorer settings you need to select the Use automatic configuration script because it is a matter of changing the script.

C: Creating an alias (CNAME) will just hide network details form the client it connects to. This is not solving the problem that the portable computer users are experiencing.

D: The Reverse Lookup Zones folder contains all of the reverse lookup DNS domain zones that are hosted on the DNS server you are looking at. By configuring reverse lookup zone on the DNS server with a

pointer resource record for each ISA Server computer will thus not work.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE: Exam 70-291: Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 480, 520-522

QUESTION 667
You are the network administrator for Certkiller .com. The network consists of five Windows Server 2003 computers and 50 Windows XP Professional computers on a single subnet.
On Sunday, another administrator installs a new firewall between the LAN and the company's T1 Internet connection. The network is configured as shown in the exhibit.
Local host names are resolved on the network by using a WINS server. All client computers are configured to use ISP1 for DNS name resolution.
On Monday morning, users report that they are no longer able to access secure and nonsecure Internet Web sites.
From a Windows XP Professional computer, you are able to successfully perform the following tasks:
Ping the IP addresses of Web servers on the Internet.
Use Internet Explorer to open both secure and nonsecure Web sites by using an IP address in place of the URL.
You run the nslookup command and attempt to resolve an Internet fully qualified domain name (FQDN). You receive the following error message:
*** [131.107.100.200] can't find www. Certkiller com: No response from server >
You need to use minimum amount of administrative effort to provide users with the ability to browse web sites on the Internet.
What should you do?

A. Configure the firewall to allow traffic on TCP ports 80 and 443.
B. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
C. Install and configure the DNS service on one of the local servers.
D. Install and configure Microsoft Internet Security and Acceleration (ISA) server on one of the local servers.

Answer: B

Explanation: Port 53 is used for Domain Name System (DNS) Name Queries. This would be the minimum effort that can be applied to provide web browse abilities on the Internet for users.
Incorrect answers:
A: Port 80 is only to allow HTTP traffic.
C & D: These options suggest too much administrative effort as there is no need to install and configure either DNS service or Microsoft Internet Security and Acceleration (ISA) server on one of the local servers. All that has to be done is to configure the firewall to allow traffic on the appropriate ports.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 34

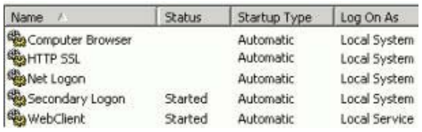
QUESTION 668
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
One domain controller on the network is configured as a certification authority (CA). The network contains a Web server that runs IIS 6.0 and hosts a secure intranet site. The server also hosts other sites that do not require HTTPS.
You configure a server certificate on the IIS server by using a certificate from your internal C
A. All
users are required to connect to the intranet site by using HTTPS.
Some users report that they cannot connect to the secure intranet site by using HTTPS. You confirm that all users can connect to the nonsecure sites hosted on the Web server by using HTTP.
You want to view the failed HTTPS requests.
What should you do?

A. Review the log fields created by IIS on the Web server.
B. Review the security log in Event Viewer on the Web server.
C. Review the security log in Event Viewer on the CA.
D. Review the contents of the Failed Requests folder on the CA.

Answer: A

Explanation: Internet Information Services (IIS) is software services that support Web site creation, configuration, and management, along with other Internet functions. Internet Information Services include Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). Reviewing the log fields created by the IIS on the Web sever will yield the necessary information to see the failed HTTPS requests.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, p. 11:35

QUESTION 669
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. The domain contains a Windows Server 2003 member server named Certkiller A, which contains confidential information. Certkiller A also runs IIS and functions as a Web server for the company intranet.
You want to secure the Web traffic to and from Certkiller
A. You configure IIS to require only secure
communications. Users must be authenticated on Certkiller A by using a domain user name and password.
Certkiller A has been functioning properly for five months. Now, when users attempt to connect to Certkiller A by using Internet Explorer, an error message appears.
Certkiller A responds to the ping command by host name and IP address. You view the services on Certkiller A, 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 Certkiller A.
Which two actions should you perform on Certkiller A? (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: You have to start the HTTP SSL service for IIS to use encryption, and you have to start the Net Logon service to provide authentication.
Incorrect Answers:
A: To be able to connect to the intranet Web users have to be authenticated since IIS was configured. Starting the Computer Browser service will thus not be sufficient.
D: Also called run as: this service allows a user to run a specified program with permissions that are different from those belonging to the account with which the user is currently logged on. But then you will not be granting accessibility to the primary user in this case. According to the exhibit this service was already started and still users could not access the intranet Web. Your brief is to enable all users to access the intranet Web.
E: Restarting the Web Client service will not work. It did not work earlier while it was started.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 583

QUESTION 670
You are the administrator of a Windows Server 2003 computer named Certkiller 1.
Users report that they cannot locate or access shared folders on Certkiller 1. Administrators report that they cannot log on or connect to Certkiller 1, and that they cannot receive administrative alerts.
You discover that the following services on Certkiller 1 are disabled:

- Distributed Link Tracking Server
- Indexing Service
- Routing and Remote Access
- Telnet
- Workstation

You need to resolve all of the problems that have been reported.
Which service should you enable and start on Certkiller 1?

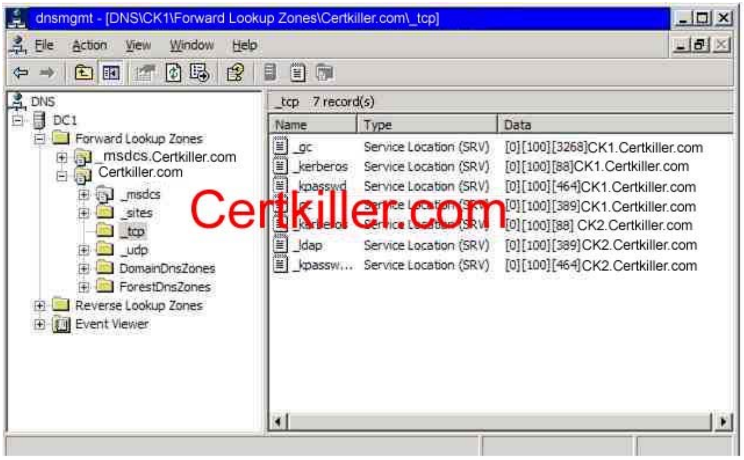
A. Distributed Link Tracking Server
B. Indexing Service

C. Routing and Remote Access
D. Telnet
E. Workstation

Answer: E

Explanation: The Workstation service has to be enabled on Certkiller 1 for clients to access shared folders.
Incorrect Answers:
A, B, C, D: Distributed Link Tracking Service, Indexing Service, Routing and Remote Access Service enables remote clients to dial into a Windows Server 2003 server and access network resources as though they were physically attached to the network & Telnet will not resolve the problem of receiving administrative alerts.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 858

QUESTION 671
You are a network administrator for Certkiller .com. The network contains an Active Directory domain named Certkiller .com. The domain contains three domain controllers named CK1 , CK2 , and CK3 . All three domain controllers are configured as DNS servers.
You monitor all three domain controllers. You notice that CK3 is not processing user logon requests.
You view DNS on CK1 , as shown in the exhibit.



Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268]CK1.Certkiller.com
_kerberos	Service Location (SRV)	[0][100][88]CK1.Certkiller.com
_kpasswd	Service Location (SRV)	[0][100][464]CK1.Certkiller.com
[illegible]	Service Location (SRV)	[0][100][389]CK1.Certkiller.com
_kerberos	Service Location (SRV)	[0][100][88] CK2.Certkiller.com
_ldap	Service Location (SRV)	[0][100][389]CK2.Certkiller.com
_kpassw...	Service Location (SRV)	[0][100][464]CK2.Certkiller.com

You must ensure that CK3 can process user logon requests.
What should you do on CK3 ?

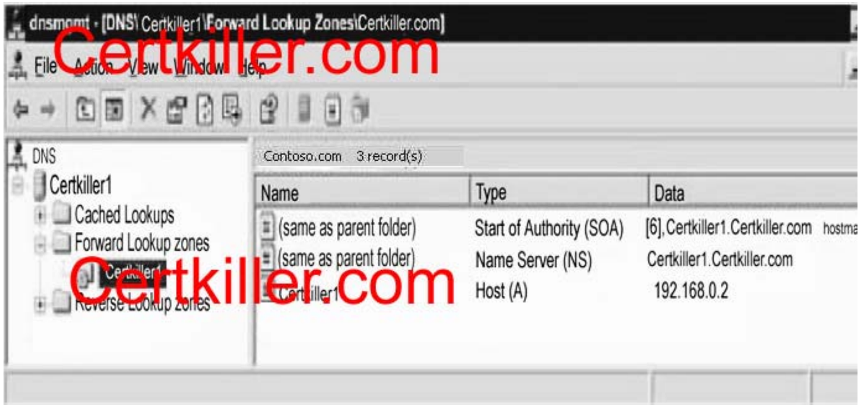
A. Run the ipconfig /registerdns command.
B. Run the nslookup command, and then run the set type = srv command.
C. Restart the Net Logon service.
D. Restart the DNS Server service.

Answer: B

Explanation: The nslookup utility can be used to list all records in a zone. You can use the netlogon.dns file

found in %systemroot%\system32\config, because it contains all the necessary SRV records needed for AD functionality. This should solve your problem.
Incorrect answers:
A: The ipconfig /registerdns command will only flush the resolution cache and update the clients records in DNS. This is not going to ensure that CK3 can process user logon requests.
C & D: Restarting the Netlogon service is not the solution, neither is the restarting of the DNS server.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 442, 546-547, 858
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 3
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 220

QUESTION 672
Exhibit



Contoso.com 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[6],Certkiller1.Certkiller.com hostma
(same as parent folder)	Name Server (NS)	Certkiller1.Certkiller.com
Certkiller1	Host (A)	192.168.0.2

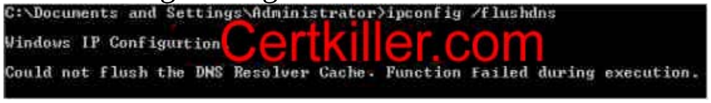
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional or Windows 2000 Professional. The network contains two domain controllers and three member servers. The network contains a single DNS server named Certkiller 1.
The DNS server fails. You install a new server that runs Windows Server 2003. You reassign the failed DNS server's IP address to the new server. You install DNS on the server. You configure a new primary zone named Certkiller .com, and you configure the zone to support dynamic updates.
Users report that they cannot log on to the domain. You review the DNS domain information. The information is shown in the exhibit.
You need to ensure that all users can log on to the domain.
What should you do?

A. Restart the Net Logon service on the domain controllers.
B. Force a DNS registration on each of the member servers in the domain.
C. Install DNS on a domain controller. Create a zone named Certkiller .com. Configure the zone to be an Active Directory-integrated zone and to support only secure updates.
D. For each of the domain controllers, create a host (A) resource record in the Certkiller .com domain.

Answer: A

Explanation: The Net Logon service is a service that accepts logon requests from any client and provides authentication from the Security Accounts Manager (SAM) database of accounts. By restarting this service on the domain controllers you will enable all users to log on to the domain.
Incorrect answers:
B: Forcing DNS registration will not allow all users to log on.
C: There is no need to create zones and configuring it to be Active Directory-integrated zone. All that is necessary is to restart the Net Logon service on the domain controllers to enable all users to logon.
D: This record maps a DNS name to an IP address. Creating a host (A) resource record will thus not be enough in this case.
Reference:
J. C. Mackin and Ian McLean, MCSA/MCSE Self-Paced Training Kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 network Infrastructure, Microsoft Press, Redmond, 2003, Part 1, Chapter 4, pp. 205 - 210, 428

QUESTION 673
You are the administrator of a Windows Server 2003 computer named Certkiller 1. The LAN connection TCP/IP properties on Certkiller 1 are configured to use a static IP address.
An administrator reports that Certkiller 1 is receiving incorrect results to a query for Certkiller 2. Certkiller .com. You log on to Certkiller 1 and run the ipconfig /flushdns command. You receive the following message.

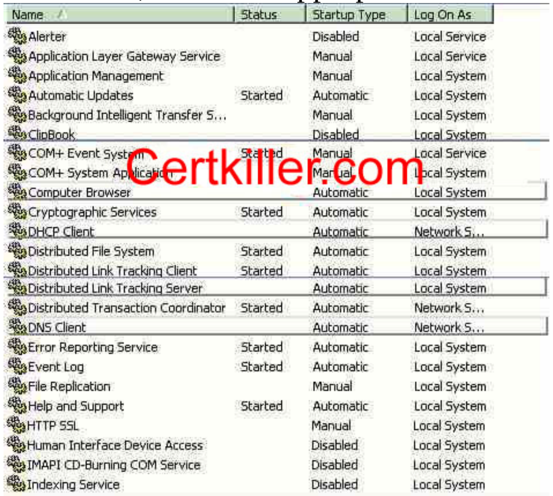


```
C:\Documents and Settings\Administrator>ipconfig /flushdns

Windows IP Configurtion

Could not flush the DNS Resolver Cache. Function failed during execution.
```

You need to start the appropriate service or services to ensure that Certkiller 1 can correctly resolve name resolution queries. You want to achieve this goal by using the minimum amount of administrative effort.
Which service or services should you start?
To answer, select the appropriate service or services in the work area.



Name	Status	Startup Type	Log On As
Alerter		Disabled	Local Service
Application Layer Gateway Service		Manual	Local Service
Application Management		Manual	Local System
Automatic Updates	Started	Automatic	Local System
Background Intelligent Transfer S...		Manual	Local System
ClipBook		Disabled	Local System
COM+ Event System	Started	Manual	Local Service
COM+ System Application		Manual	Local System
Computer Browser		Automatic	Local System
Cryptographic Services	Started	Automatic	Local System
DHCP Client		Automatic	Network S...
Distributed File System	Started	Automatic	Local System
Distributed Link Tracking Client	Started	Automatic	Local System
Distributed Link Tracking Server		Automatic	Local System
Distributed Transaction Coordinator	Started	Automatic	Network S...
DNS Client		Automatic	Network S...
Error Reporting Service	Started	Automatic	Local System
Event Log	Started	Automatic	Local System
File Replication		Manual	Local System
Help and Support	Started	Automatic	Local System
HTTP SSL		Manual	Local System
Human Interface Device Access		Disabled	Local System
IMAPI CD-Burning COM Service		Disabled	Local System
Indexing Service		Disabled	Local System

Answer: Select the "DNS Client" service.

Explanation: To ensure that Certkiller 1 can correctly resolve name resolution queries you need to enable the

"DNS Client" service as is responsible for directing name resolution. The DNS Client service first attempts name resolution through DNS; if this fails, the DNS Client service then submits the name to NetBIOS. In other words it acts as a resolver.

Reference:

J. C. Mackin, Ian McLean, MCSA/MCSE Self-Paced training kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, 2003, Chapter 4, pp. 3-4

QUESTION 674

You are the network administrator for Certkiller .com. The network contains two Windows Server 2003 computers named Certkiller 1 and Certkiller 2. The two servers are configured as shown in the following table.

Server name	**Static IP address**	**Network Services**
Certkiller 1	192.168.2.1	DHCP
Certkiller 2	192.168.2.2	DNS, WINS

Users report that they cannot log on to the network by using their client computers. Administrators report that IP addresses are not being renewed on these client computers.

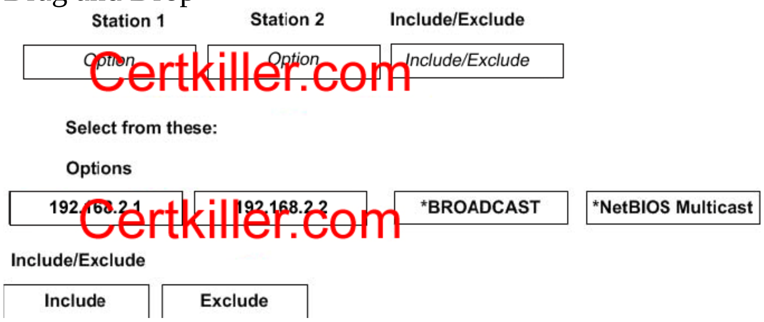
You observe that all network services are running on each server. You start Network Monitor on Certkiller 1.

You need to find out why the client computers are not receiving new IP addresses. You need to configure an address filter on Certkiller 1 to capture the minimum amount of data required.

What should you do?

To answer, drag the appropriate source or sources to the correct location or locations.

Drag and Drop



Station 1 | Station 2 | Include/Exclude

Option | Option | Include/Exclude

Select from these:

Options

192.168.2.1 | 192.168.2.2 | *BROADCAST | *NetBIOS Multicast

Include/Exclude

Include | Exclude

Answer: 192.168.2.1, Broadcast, Include

QUESTION 675

You are the network administrator for Certkiller .com. 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 Certkiller Srv as a print server. The name of the print queue is \\ Certkiller Srv\laserprinter. You assign the Everyone group the Allow - Print permissions.

Three days later, you discover that print jobs submitted to \\ Certkiller Srv\laserprinter are not being printed. You log on to the client computer named Client1. Client1 is configured to use \\ Certkiller Srv\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 \\ Certkiller Srv \laserprinter. You see the following status of

the print queue: "laserprinter on Certkiller Srv is unable to connect". You are able to connect to Certkiller Srv by running the ping command.
You need to ensure that print jobs submitted to \\ Certkiller Srv \laserprinter will be printed.
What should you do?

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

Answer: D

Explanation: A stalled print spooler service is typically the problem when print jobs are not being printed, and errors are not being received. When different people experience the same problem, the problem is likely to be connected to the server, and not the client. From a client computer, you can connect to the server and restart the Print Spooler service.
Incorrect Answers:
A: Creating another share will not solve the problem because the printer is already shared.
B: This command would not fix the printing problem as it will not address the problem at hand.
C: Because different people are experiencing the same problem, the problem is likely to be with the server and not the client.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 82

QUESTION 676
You are the administrator of an Active Directory domain. Certkiller 's WAN consists of eight regional offices. Each regional office has a file and print server. All of these servers are located in the same organizational unit (OU). The Print Spooler service periodically fails on these servers.
You need to be able to remotely restart the Print Spooler service on one of the servers in case of a failure.
What should you do?

A. Create a Group Policy object (GPO) that sets the Print Spooler service to Automatic.
Link the GPO to the OU that contains the servers.
B. Use Remote Desktop to configure the Service Recovery options on each server to restart the Print Spooler service on the first failure.
C. Create a batch file in the Netlogon share that contains the net start "print spooler" command.
Create a Group Policy object (GPO) on the OU that links the batch file to the startup scripts.
D. Create an alert that triggers the execution of the net start "print spooler" command when the Max Jobs Spooling Print Queue counter exceeds 0.

Answer: B

Explanation: Remote Desktop For Administration enables administrators to perform administrative tasks on remote servers and clients from a centralized console such as setting the Service Recovery options on each remote server to restart the Print Spooler service. With Remote Desktop For Administration, you can remotely administer any Windows Server 2003 server over any TCP/IP connection. Other administrative tasks that can be performed include running a backup job, changing Control Panel configuration settings, defragging a server's disks, installing an application, and promoting/demoting a domain controller, among other tasks.
Incorrect Answers:
A: Linking a GPO that sets the Print Spooler service to Automatic to the servers' OU will not allow you to remotely restart the Print Spooler on server failure.
C: Linking a Netlogon batch file with the net start "print spooler" command to the startup scripts will not restart a print spooler remotely. You need to make use of Remote Desktop to configure Service Recovery options.
D: When there is a print spooler failure then what is needed is to do a service recovery remotely in this case. This can only be done through the Remote Desktop if you are to be able to restart the service remotely.
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, 2003, Chapter 2, p. 66

QUESTION 677
You are the administrator of a Windows Server 2003 computer named Certkiller 1. Certkiller 1 has a third-party application installed on it. The third-party application runs as a service that is named Service1. Service1 fails periodically.
You need to configure the recovery options for Service1 to meet the following requirements:
• If Service1 runs successfully for a day or more, you need to ensure that only the service is immediately restarted upon failure.
• If, after this failure, Service1 does not run successfully for another day, you must ensure the entire server is immediately restarted.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

A. Configure the Reset fail count after value for Service1 to 1 day.
B. Configure the Restart service after value for Service1 to 1,440 minutes.
C. Configure the response to the first failure to be restart Service1.
D. Configure the response to the first failure to be restart Certkiller 1.
E. Configure the response to the second failure to be restart Service1.
F. Configure the response to the second failure to be restart Certkiller 1.

Answer: A, C, F

Explanation: This question basically involves managing services through Control Panel. You can indicate the number of days after which the number of times a failure has occurred should be reset to 0 in the Reset fail Count dialog box. The Restart Service After dialog box is where you indicate the number of minutes to wait prior to trying to restarting a service (Service1) subsequent to a failure. The Restart Computer Options dialog box is where you indicate the number of minutes to wait prior to restarting the computer (Certkiller 1).

Incorrect Answers:
B: 1440 minutes is a 24 hour period which is one day. Thus the time period is correct, but you need to configure the Reset fail count after value and not the Restart service after.
D: Certkiller 1 should not be used to configure the response to the first failure for restart. You should be making use of Service1
E: Certkiller 1 should not be used to configure the response to the second failure for restart.
Reference:
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd & Laura Hunter, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Chapter 12, Syngress Publishing Inc., Rockland, 2003, pp. 777 - 783

QUESTION 678
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. The network contains a server named Certkiller 4 that has Terminal Services enabled.
An administrator named Jack is responsible for backing up Certkiller 4. She is a member of the Backup Operators local group on Certkiller 4. You want to allow Jack to perform her assigned tasks remotely by connecting to Certkiller 4 through a Terminal Services connection. When Jack attempts to connect to Certkiller 4, she cannot log on. You can successfully connect and log on to Certkiller 4.
You need to ensure that Jack can successfully connect and log on to Certkiller 4. You must assign Tess only minimum rights that she needs to do her work.
What should you do on Certkiller 4?

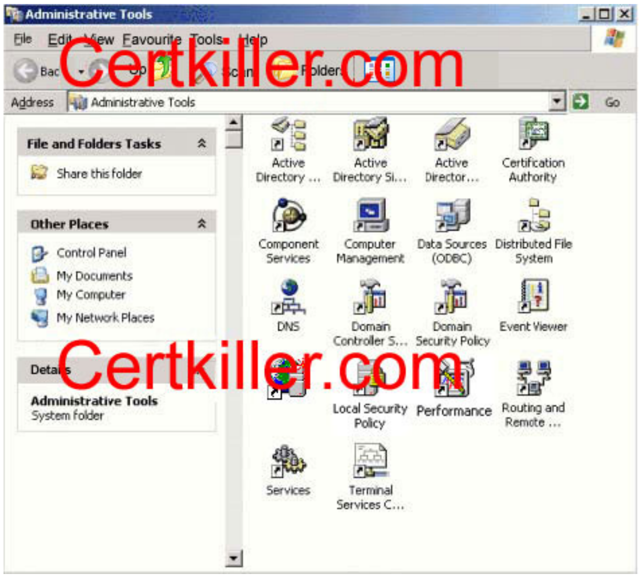
A. Add Jack to the local Power Users group.
B. Add Jack to the local Remote Desktop Users group.
C. In the local security policy, assign Jack the Allow log on locally user right.
D. In Terminal Services Configuration, set the connection encryption level to Client Compatible.

Answer: C

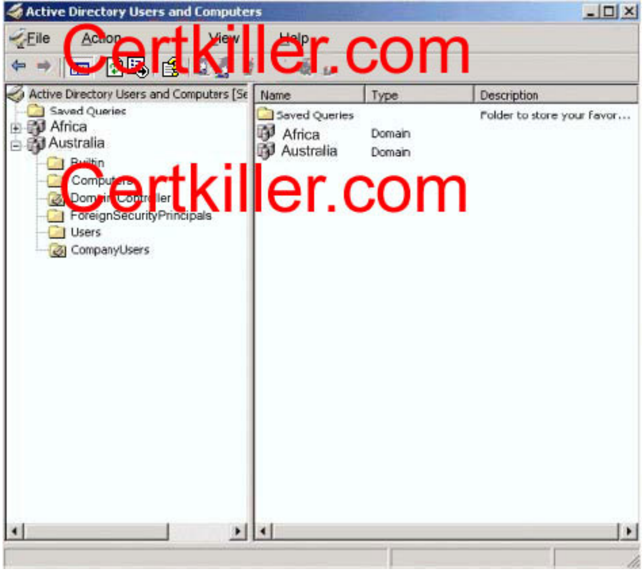
Explanation: User right assignment is done in the Security settings in the local Policies. The default security settings do not allow regular users to log on interactively at a server. You can change this setting through Start _ Administrative Tools _ Security Policy. Expand Local Policies, then User Rights Assignment. Doubleclick Allow Log On Locally and click the Add User Or Group button. In the Add User Or Group dialog box, type in Sandra and click the OK button. In the Security Policy Setting dialog box, click the OK button. Close any open dialog boxes.
Allow log on locally user right can be assigned to Account Operators, Administrators, Backup Operators, Print Operators and Server Operators. Users with this right can log on to the server console interactively.thus this option would represent the minimum rights that Jack would need to ensure that she can connect and log on to Certkiller 4 to carry out her tasks.
Incorrect answers:
A: Power Users group is a group whose members can manage accounts, resources, and applications that are installed on a workstation, stand-alone server, or member server. This group does not exist on domain controllers. Administrative tasks that can be performed by members of this group include creating local users and groups; modifying and deleting accounts that they have created; removing users from the

Power Users, Users, and Guests groups; installing most applications; and creating and deleting file shares. This is not what is required by Jack in the current circumstances.
B: This right would allow the user to be able to log on to the Terminal server and use either Remote Desktop for Administration. This is not required in the given circumstances.
D: In Terminal Services Configuration there is a General tab. This tab identifies the connection type (RDPTcp) and RDP version number.There is a Comment text box in which you can store information for administrative purposes. More importantly, this tab enables you to specify the level of encryption that will be required for connection to Terminal Services.The default encryption setting is Client Compatible.This setting attempts to use the maximum level of encryption allowed on the client. This is not what Jack needs.
Reference:
Lisa Donald, Suzan Sage London & James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 142
Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Laura E. Hunter & Will Schmied, MCSA/MCSE: Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 440, 549, 560

QUESTION 679
You are the network administrator for Certkiller . The network consists of a single Active Directory forest that contains two domains named Africa and Australia. The functional level of both domains is Windows 2000 native.
Certkiller .com has multiple offices in Africa and Australia. User accounts are organized in the domains based on the users' geographical location.
Certkiller .com uses Microsoft Exchange 2000 Server for e-mail. A group named Sales is used to send email messages to the users in the sales department in the Cape Town office.
You need to configure the Sales group so that it can include users in the Australia domain. You also need to configure the Sales group so that it can be used to control access to the HR folder on the file server. In addition, you need to add the Sales group a user named Jack King, who is a new employee in the sales department in the Cape Town office.
What should you do?
Take the appropriate actions in the simulation window.
Simulation Windows

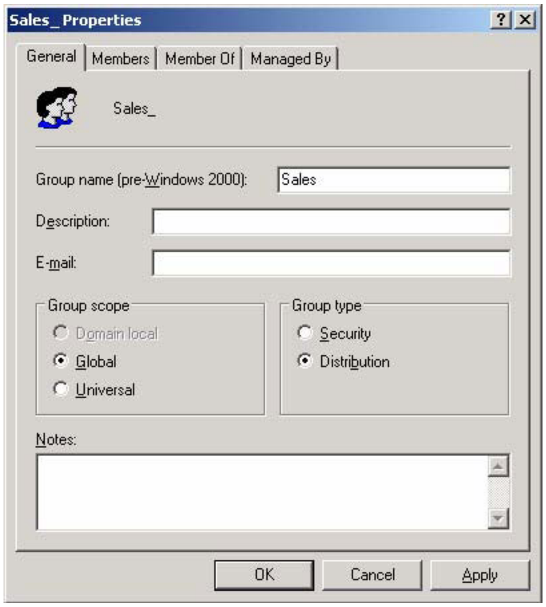


Answer:
Step #1.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [Se
Saved Queries
Africa
Australia
Builtin
Computers
Domain Controller
ForeignSecurityPrincipals
Users
CompanyUsers

Name	Type	Description
Saved Queries		Folder to store your favor...
Africa	Domain	
Australia	Domain	

Open the Users container in the Africa domain and go into the properties of the Sales group. The sales group is likely to be a global distribution group because it is used to send email.



Sales_Properties

Sales_

Group name (pre-Windows 2000): Sales

Description:

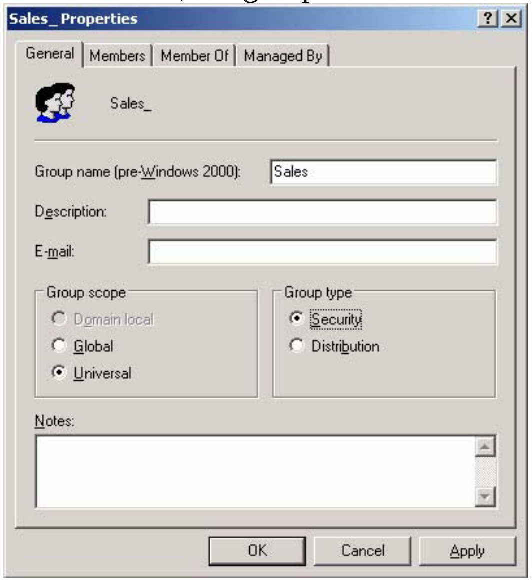
E-mail:

Group scope
○ Domain local
● Global
○ Universal

Group type
○ Security
● Distribution

Notes:

To add users from the other domain, the group needs to be changed to a universal group. To access the file server, the group needs to be a security group.



Sales_Properties

Sales_

Group name (pre-Windows 2000): Sales

Description:

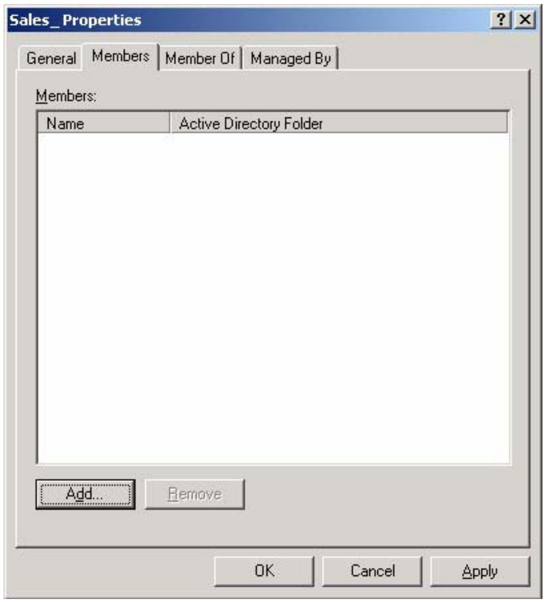
E-mail:

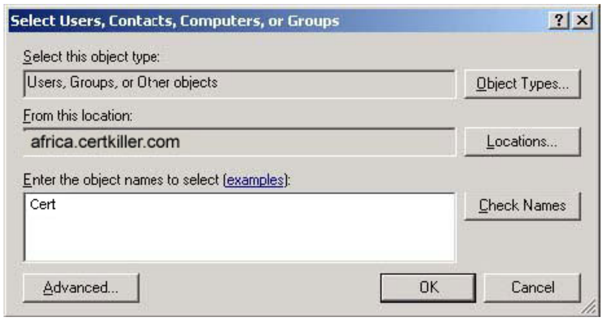
Group scope
○ Domain local
○ Global
● Universal

Group type
● Security
○ Distribution

Notes:

To add Jack to the group, click the members tab, click add and type Tess.





Select this object type: Users, Groups, or Other objects

From this location: africa.certkiller.com

Enter the object names to select (examples): Cert

QUESTION 680

You are the administrator of a Windows Server 2003 computer named Certkiller 5. Certkiller 5 functions as a file server for Certkiller .com's Sales and Human Resources (HR) departments.

On Certkiller 5 you create a share named Sales on the C:\Sales folder, and you create a share named Certkiller on the C:\Company\ Certkiller folder.

Users who are members of the SalesGroup need to be able to create and modify files in the C:\Sales folder. These users also need to be able to modify the permissions on all of the files in the C:\Sales folder. However, these users report that when they attempt to perform these tasks, they receive the following error message: "Access denied."

Users who are members of the HRGroup group should only be able to read files that are in the C:\Company\ Certkiller folder. However, some of the users in the HRGroup are occasionally able to modify those files.

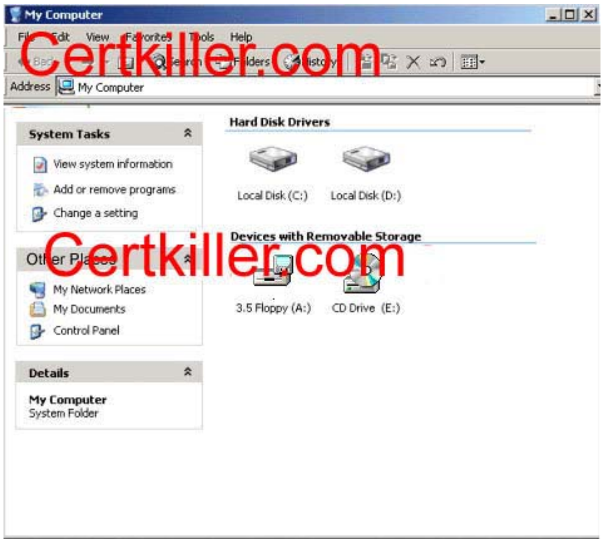
You need to resolve these problems by performing the following administrative tasks on Certkiller 5:

- Correct the permissions on the Sales shared folder for the SalesGroup group.
- Ensure that the Certkiller share is the only point of access for the C:\Company\ Certkiller folder.

What should you do?

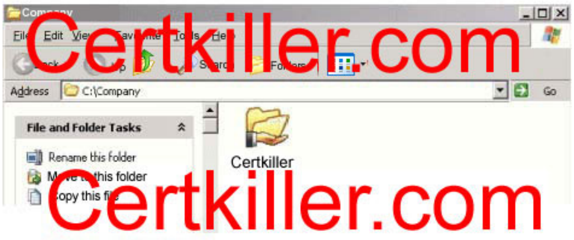
Take the appropriate actions in the simulation window.

Simulation Window

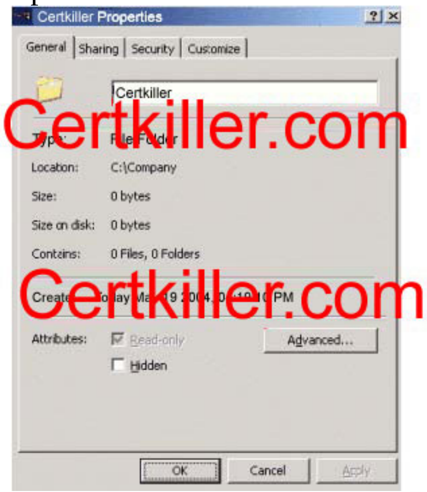


Answer:

Step #1:



Step #2:


Certkiller Properties

General | Sharing | Security | Customize

Certkiller

Type: File Folder

Location: C:\Company

Size: 0 bytes

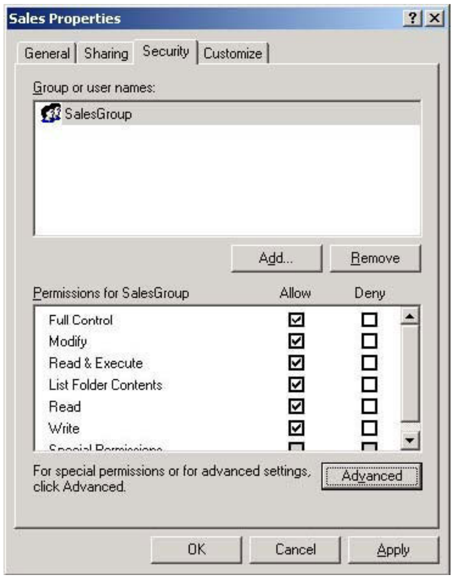
Size on disk: 0 bytes

Contains: 0 Files, 0 Folders

Created: Today, March 09 2004, PM

Attributes: ☑ Read-only □ Hidden

Step #3



Sales Properties

Group or user names:

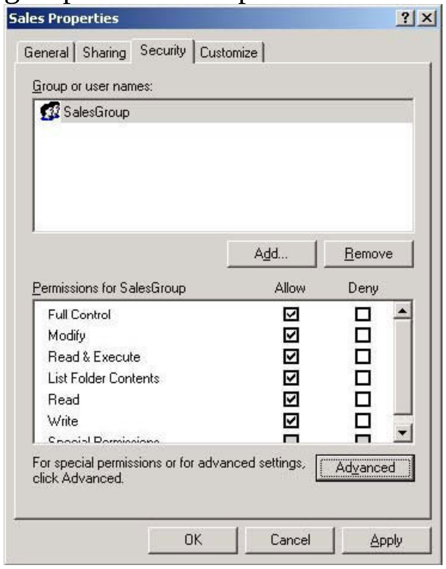
SalesGroup

Permissions for SalesGroup	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Salesgroup needs to be able to modify the files in the Sales folder and to change permissions on the files. The question doesn't say Salesgroup should be able to change ownership of the files. Therefore, we can give Salesgroup full control then take away the change ownership permission to the Sales folder.

Right click on the Sales folder and select properties. Click the security tab and grant the Salesgroup group full control permission.



Sales Properties

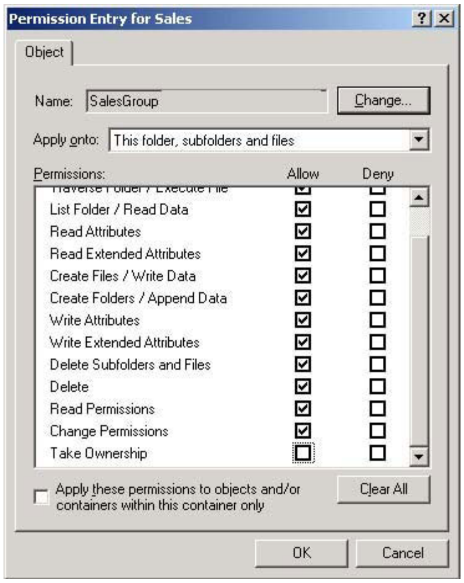
Group or user names:

SalesGroup

Permissions for SalesGroup	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Click Advanced, click Edit then take away the Take Ownership permission.



Name: SalesGroup

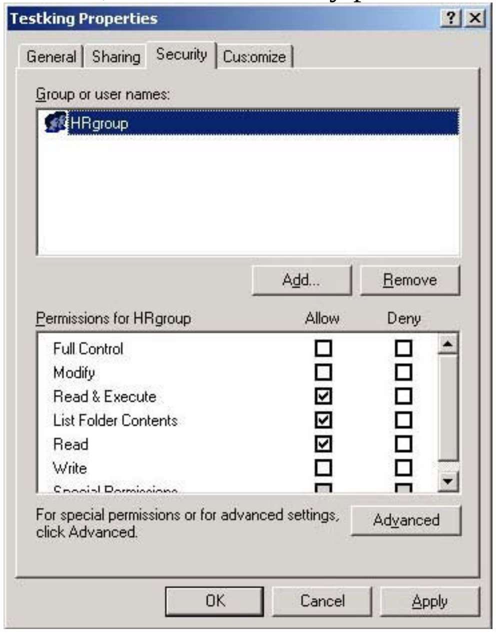
Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	□
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	☑	□
Create Folders / Append Data	☑	□
Write Attributes	☑	□
Write Extended Attributes	☑	□
Delete Subfolders and Files	☑	□
Delete	☑	□
Read Permissions	☑	□
Change Permissions	☑	□
Take Ownership	□	□

□ Apply these permissions to objects and/or containers within this container only

HRgroup needs read only permission to the Certkiller folder.

Right click on the Certkiller folder and select properties. Click the security tab and remove the Full Control, Write and modify permissions.



Group or user names:

HRgroup

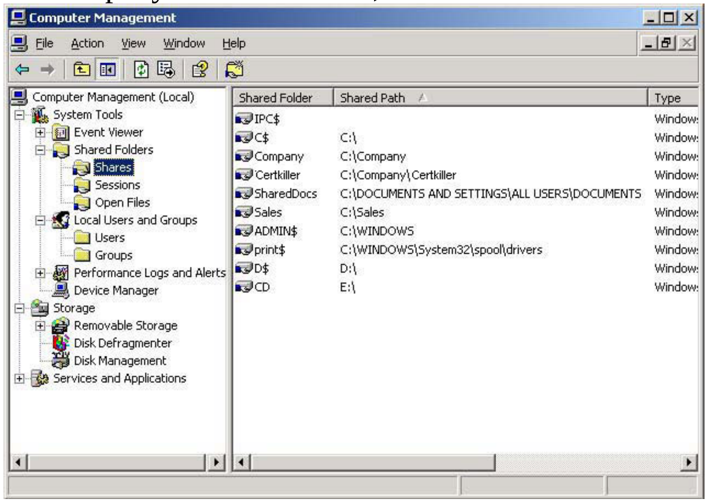
Permissions for HRgroup	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

We need to "ensure that the Certkiller share is the only point of access for the C:\Company\ Certkiller folder".

We can check for multiple shares on the Certkiller folder or the Company folder using the Shared Folders node in Computer management. The only share should be the " Certkiller " share. If the

C:\Company folder is shared, we need to delete the share.



Shared Folder	Shared Path	Type
IPC$		Window
C$	C:\	Window
Company	C:\Company	Window
Certkiller	C:\Company\Certkiller	Window
SharedDocs	C:\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS	Window
Sales	C:\Sales	Window
ADMIN$	C:\WINDOWS	Window
print$	C:\WINDOWS\System32\spool\drivers	Window
D$	D:\	Window
CD	E:\	Window

QUESTION 681

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

Certkiller .com's written security policy states that passwords reset by help desk technicians should be set to Password12!, and users must change the password immediately after logging on.

An employee named Jack King has been on vacation and has not had access to the network. She returns to the office and attempts to log on to the network. She receives the following error message: "Unable to log you on because your account has been locked out, please contact your administrator." Tess cannot remember her password.

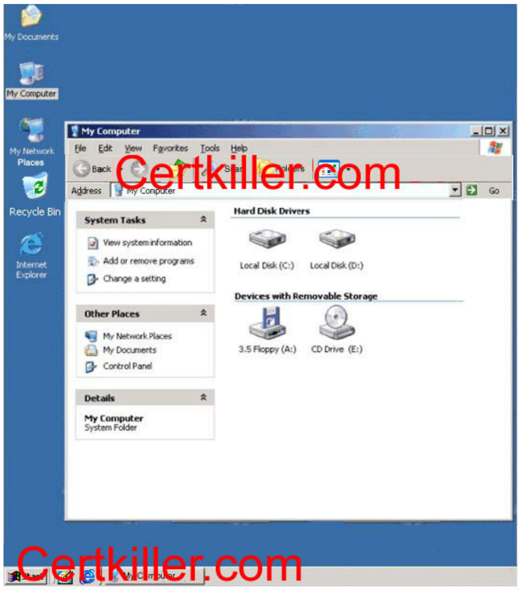
Sandra King works as a contractor for Certkiller .com. Sandra's user account has expired. She will continue to work for Certkiller .com, but she will work in the Foo Ltd., division.

You need to ensure that both Sandra and Jack can access domain resources. You need to ensure that Sandra's user account will continue functioning indefinitely, and that her user principal name (UPN) is changed to reflect the Foo Ltd., division.

What should you do?

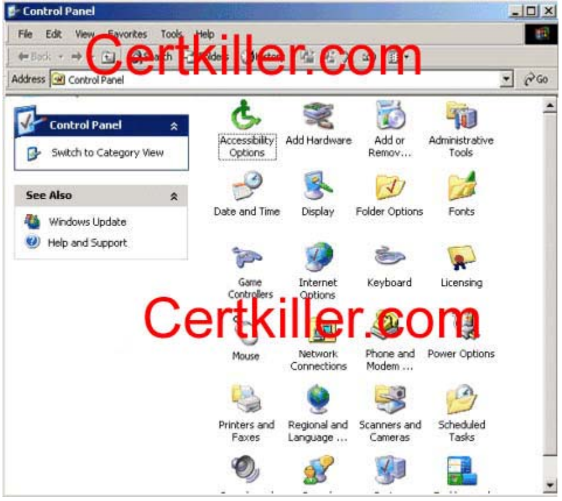
Take the appropriate actions in the simulation window.

Simulation Window

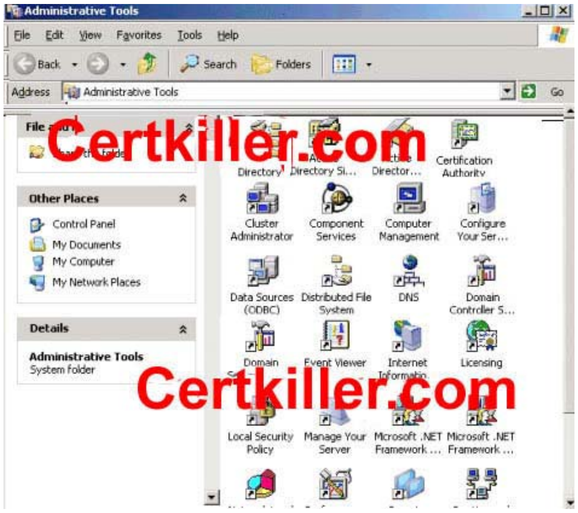


Answer:

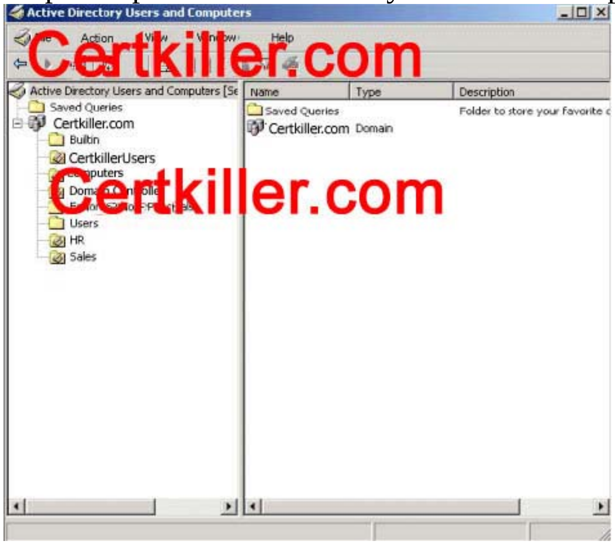
Step #1



Step #2



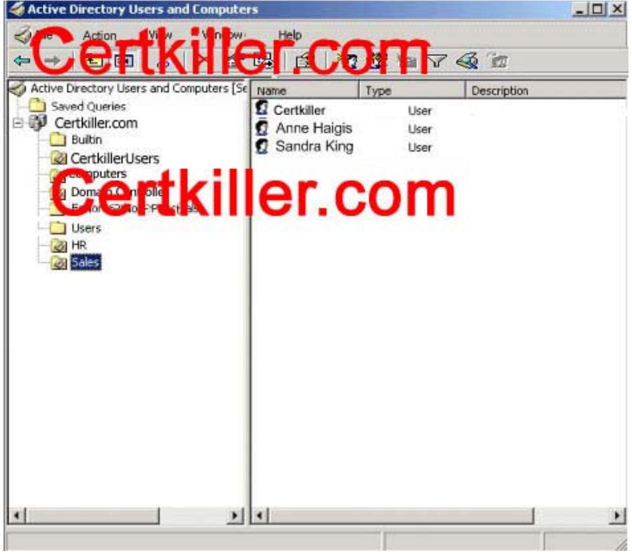
Step #3 Open Active Directory Users and Computers.



Name	Type	Description
Saved Queries		Folder to store your favorite c
Certkiller.com	Domain	

Step #4 Select the Sales OU

You can also try to open the Users OU first, it is not penalized, but Jack is not present there.

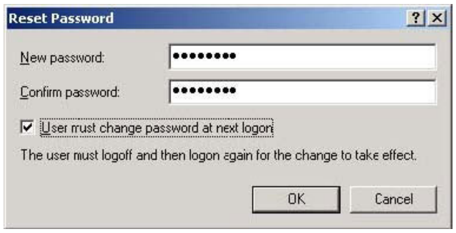


Name	Type	Description
Certkiller	User	
Anne Haigis	User	
Sandra King	User	

Step #5

We need to reset the password for the Jack King account.

Right click on the Jack King user account object and select Reset Password. Type in the password of Password12! And check the checkbox:



New password: ••••••••

Confirm password: ••••••••

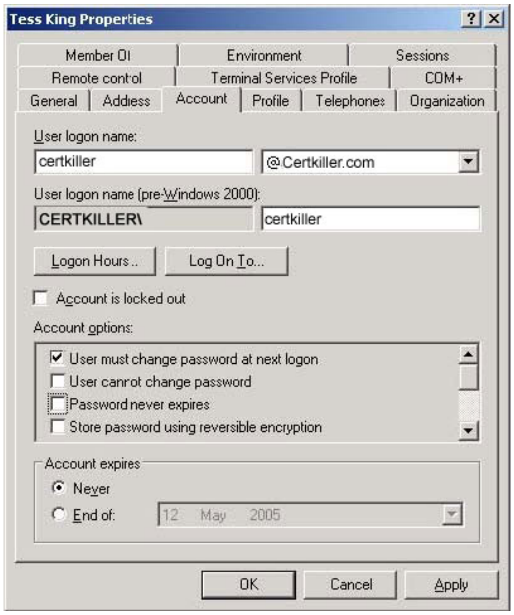
☑ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Step #6

We also need to unlock the Jack King account.

Right click on the Jack King user account object and select properties. Click the Account tab. Clear the "Account is locked out check box".



User logon name: certkiller @Certkiller.com

User logon name (pre-Windows 2000): CERTKILLER\ certkiller

□ Account is locked out

Account options:

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Store password using reversible encryption

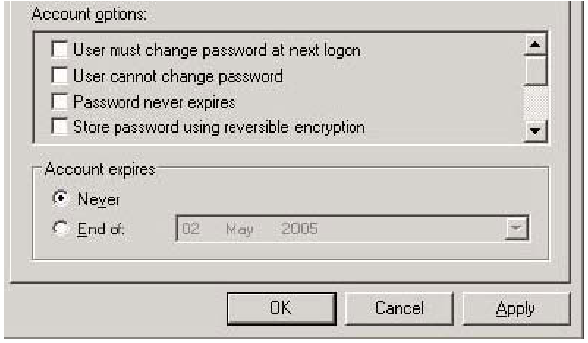
Account expires

● Never

○ End of: 12 May 2005

Sandra's account has expired. We need to ensure that Sandra's user account will continue to function indefinitely, and that her user principal name (UPN) is changed to reflect the Foo Ltd. Right click on Sandra's account and select properties. Click the account tab.

In the "Account Expires" section, select "Never".



Account options:

□ User must change password at next logon

□ User cannot change password

□ Password never expires

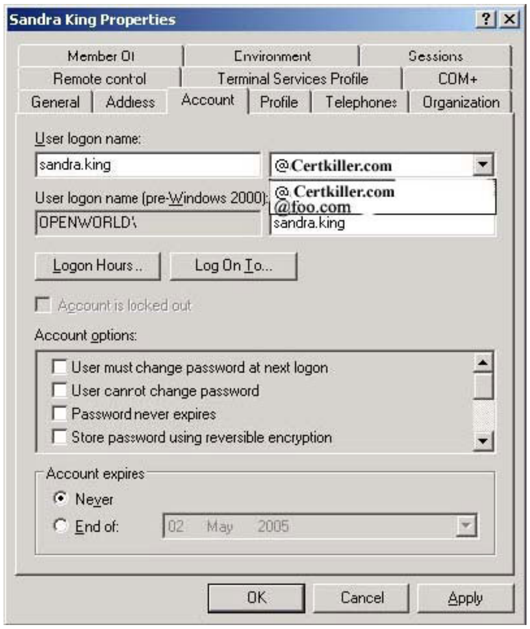
□ Store password using reversible encryption

Account expires

● Never

○ End of: 02 May 2005

To change Sandra's user principal name (UPN), click the drop down list and select foo.com from the domain list.



Sandra King Properties

User logon name: sandra.king @Certkiller.com

@.Certkiller.com
@foo.com

User logon name (pre-Windows 2000): OPENWORLD\ sandra.king

□ Account is locked out

Account options:

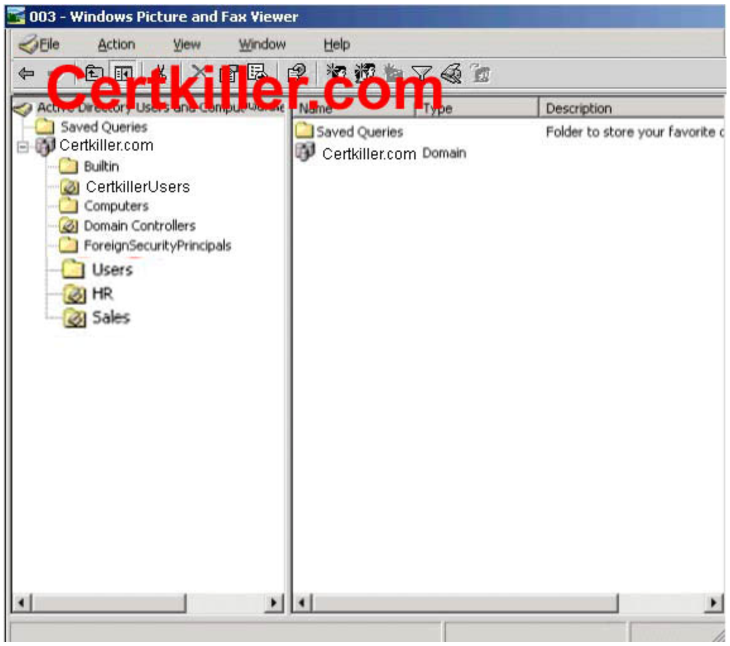
□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: 02 May 2005

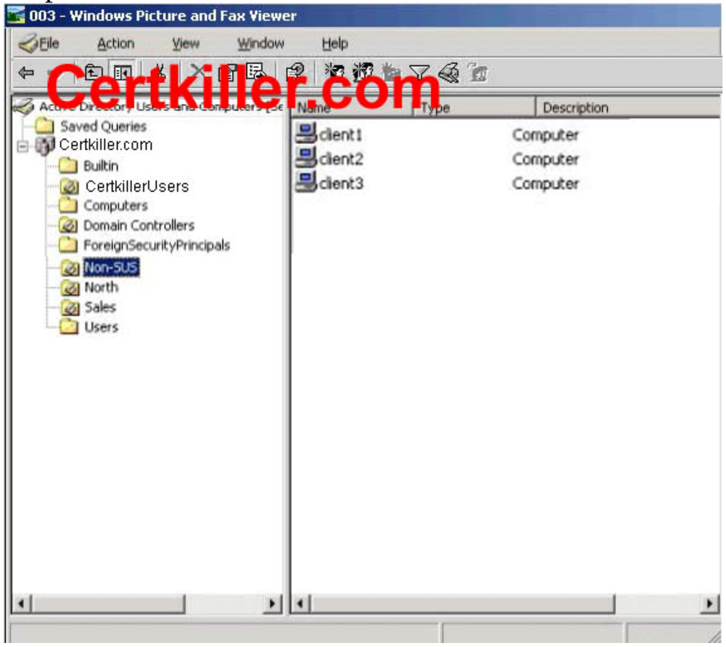
QUESTION 682

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003
Software Update Services (SUS) is installed on a single server named Certkiller 3. Certkiller 3 receives receive critical updates and security updates from Microsoft Windows Update servers.
A systems engineer installs and configures a server named Certkiller 13 as a second SUS server for the domain. You need to ensure that the new SUS Server will automatically synchronize with Certkiller 3.
You also need to approve the current list of updates that are available for the new SUS server and ensure that any revised updates are automatically approved.
What should you do?
Take the appropriate actions in the simulation window.
Simulation Window



Name	Type	Description
Saved Queries		Folder to store your favorite c
Certkiller.com	Domain	

Answer:
Step #1



Name	Type	Description
client1	Computer	
client2	Computer	
client3	Computer	

QUESTION 683

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003 and all client computers run WindowsXP Professional.

You are responsible for the day-to-day administration of user accounts for customer service employees in Certkiller .com's Moscow office. You perform administrative tasks by using a server Certkiller 4. Each user is allowed to customize their desktop. A shared folder named Users on Certkiller 4 has been created to store user folders for customized desktop settings.

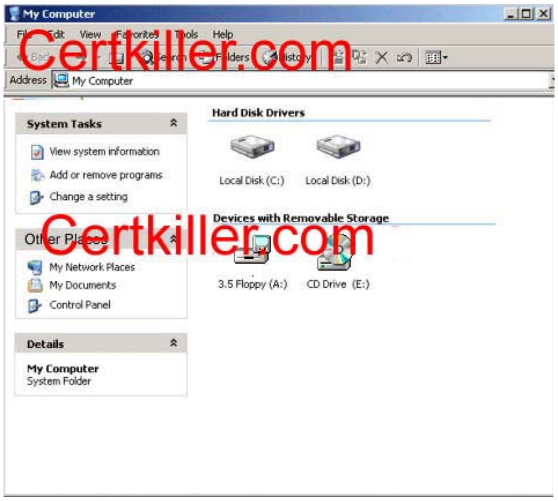
You need to perform the following tasks:

- Use Active Directory Users and Computers to set user accounts in the Sales OU to retain customized desktop settings, regardless of the client computer used. You want to achieve this goal by using the minimum amount of administrative effort.
- Make the user profile named Jack King the default profile for any new user who logs on to Certkiller 4.

What should you do?

Take the appropriate actions in the simulation window.

Simulation Window

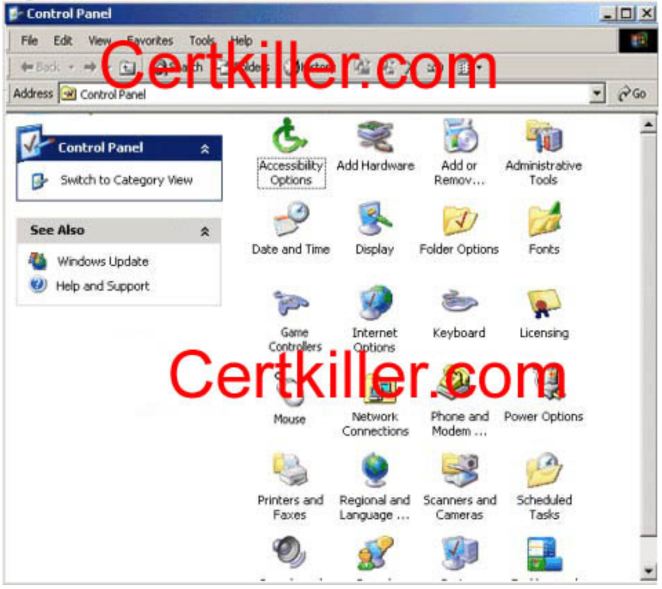


Answer:

The first requirement of this question states: Use Active Directory Users and Computers to set user accounts in the Sales OU to retain customized desktop settings, regardless of the client computer used. We can do this by configuring the user accounts in the Sales OU to use roaming user profiles.

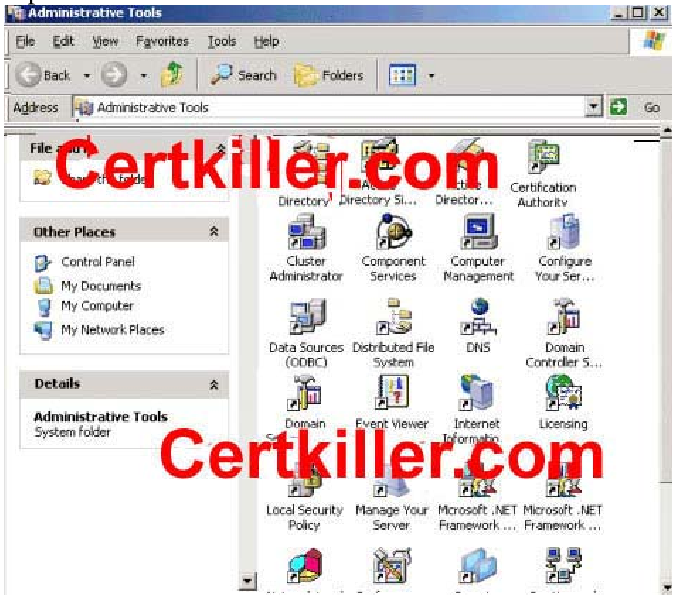
Step #1

Open Control Panel.



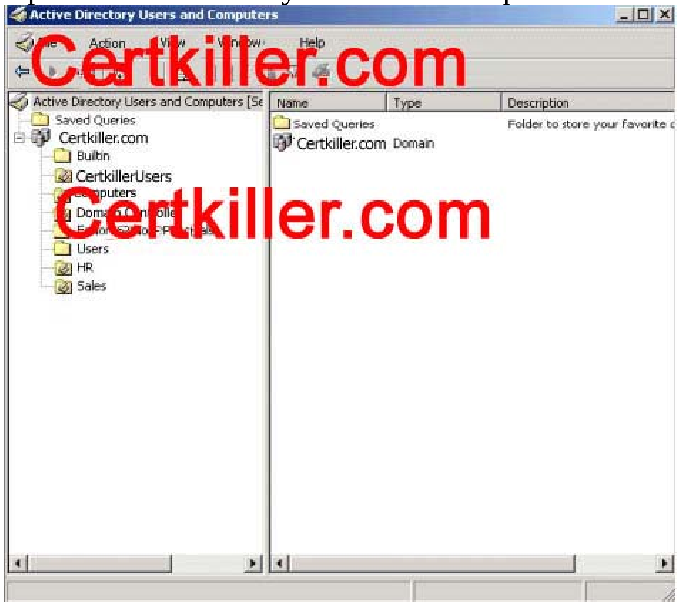
Step #2

Open Administrative tools.



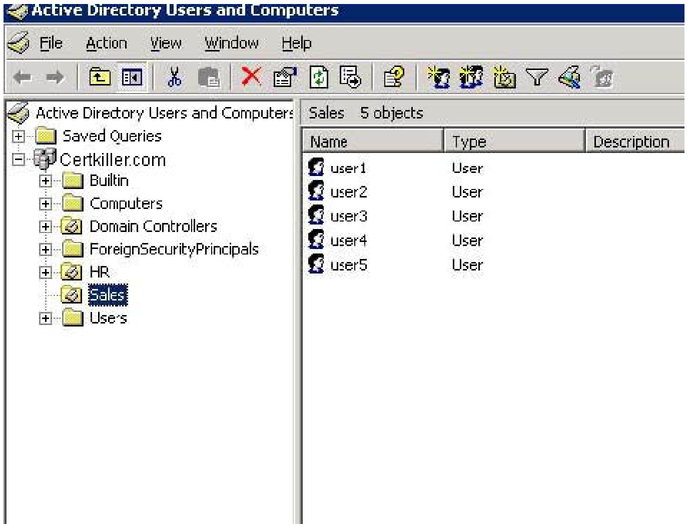
Step #3.

Open Active Directory Users and Computers.



Step #4

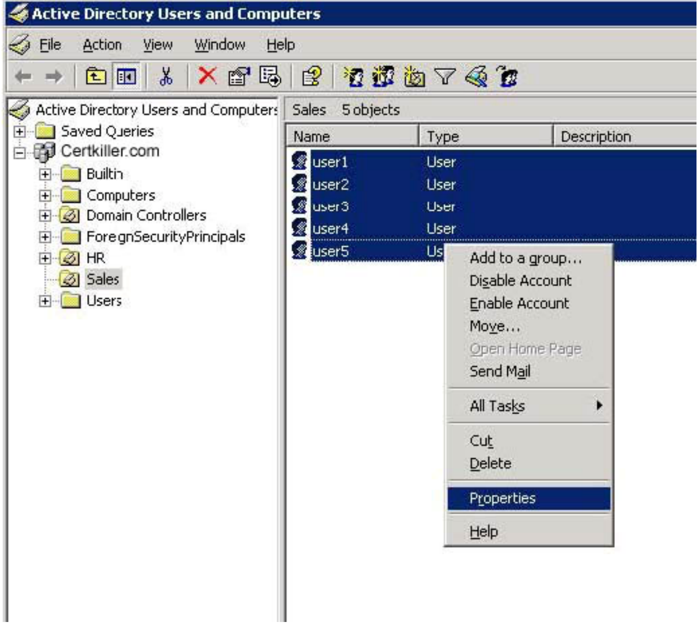
Select the Sales OU.



Name	Type	Description
user1	User	
user2	User	
user3	User	
user4	User	
user5	User	

Step #5

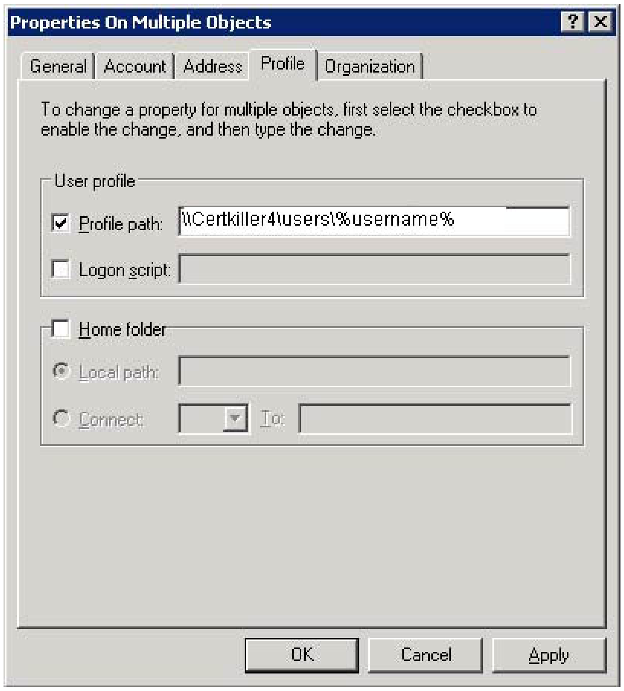
Select all the users accounts in the Sales OU. Right click and select properties.



Name	Type	Description
user1	User	
user2	User	
user3	User	
user4	User	
user5	Us	

Step #6.

On the profile tab, enter the path for the roaming profiles. Then click Ok.



Properties On Multiple Objects

To change a property for multiple objects, first select the checkbox to enable the change, and then type the change.

User profile

☑ Profile path: \\Certkiller4\users\%username%

□ Logon script:

□ Home folder

● Local path:

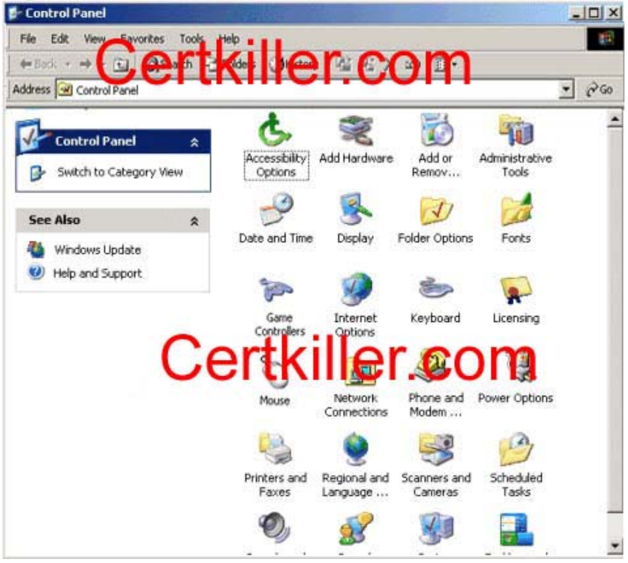
○ Connect: To:

The second requirement of the question states: Make the user profile named Jack King the default profile for any new user who logs on to Certkiller 4.

We can do this by copying the Jack King profile to the Default User profile.

Step #1.

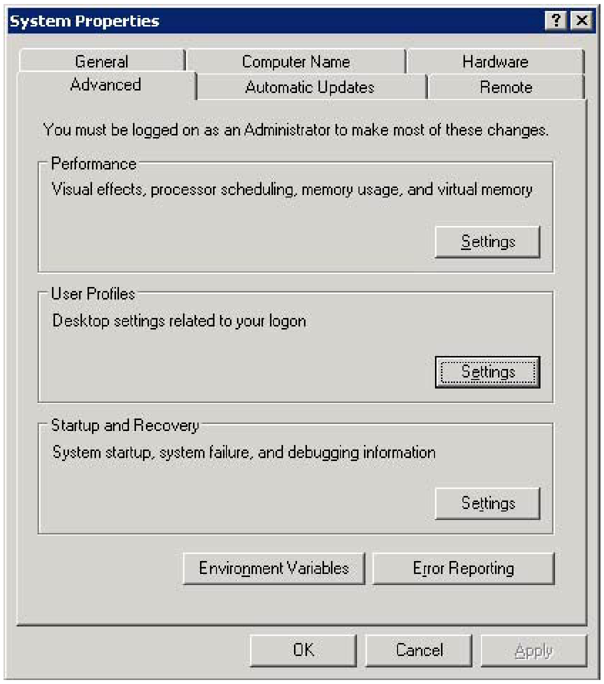
Open Control Panel.



Step #2.

Open the System applet and select the Advanced tab.

Click the Settings button for the User Profiles section.



System Properties

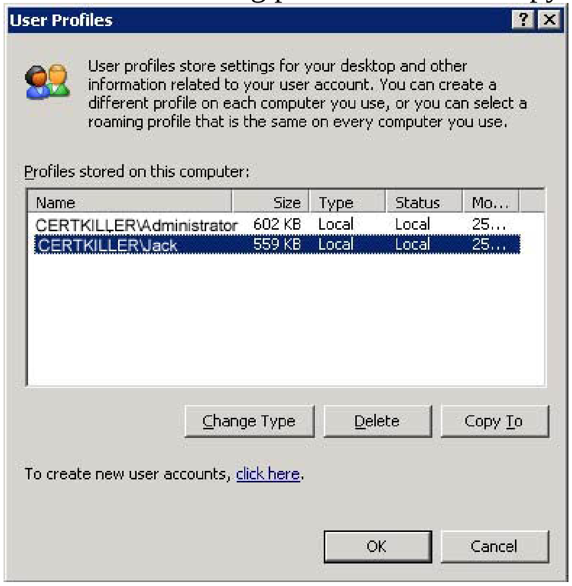
You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your logon

Startup and Recovery
System startup, system failure, and debugging information

Step #3.
Select the Jack King profile and click Copy To.



User Profiles

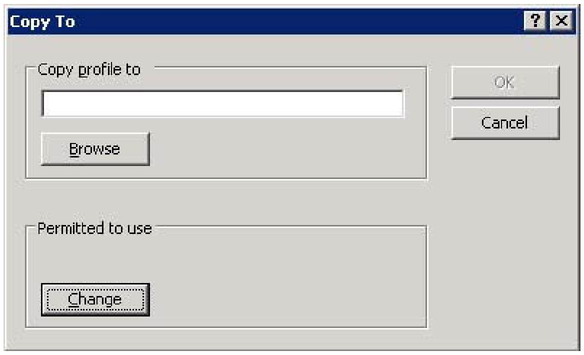
User profiles store settings for your desktop and other information related to your user account. You can create a different profile on each computer you use, or you can select a roaming profile that is the same on every computer you use.

Profiles stored on this computer:

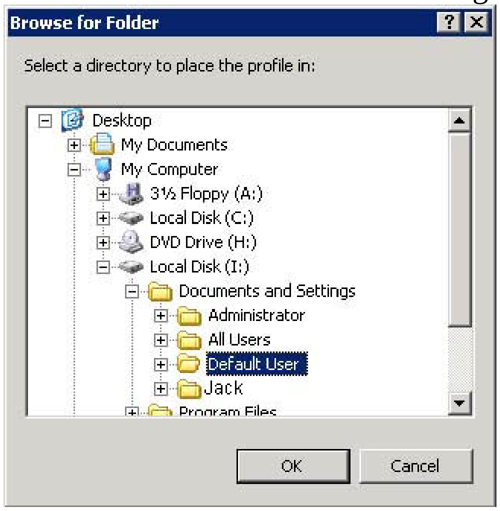
Name	Size	Type	Status	Mo...
CERTKILLER\Administrator	602 KB	Local	Local	25...
CERTKILLER\Jack	559 KB	Local	Local	25...

To create new user accounts, click here.

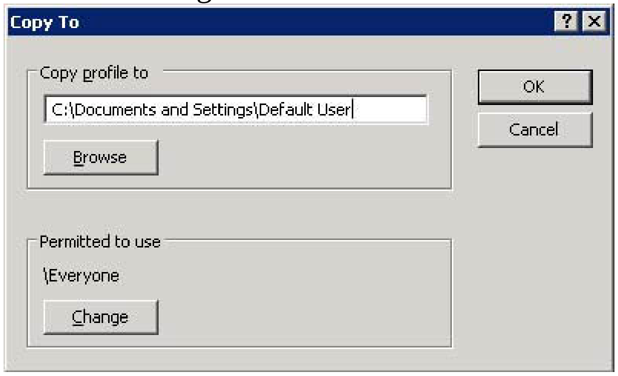
Step #4.
Click Browse.



Step #5.
Browse to the Documents and Settings\Default User folder and click ok.



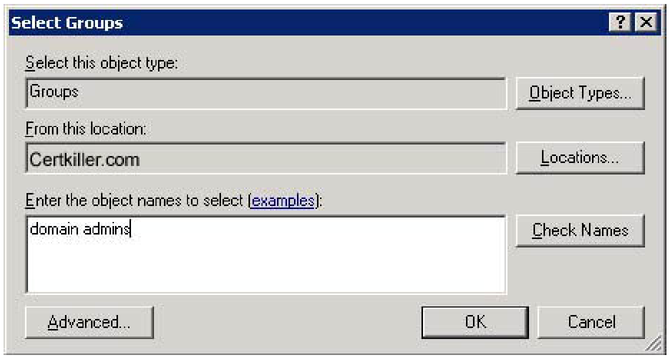
Step #6.
Click the Change button.



Copy profile to: C:\Documents and Settings\Default User

Permitted to use: \Everyone

Step #7.
Type in Everyone and click ok.

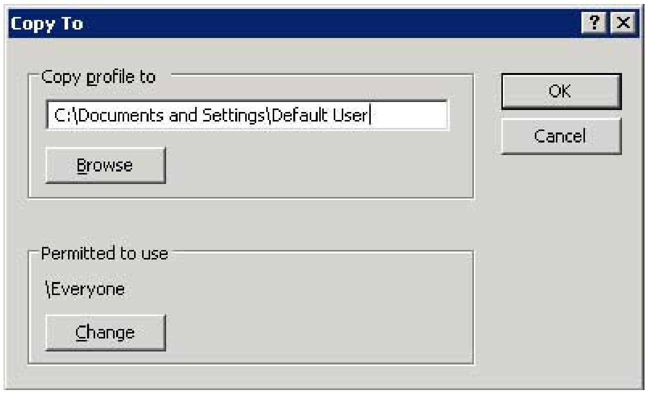


Select this object type:
Groups

From this location:
Certkiller.com

Enter the object names to select (examples):
domain admins

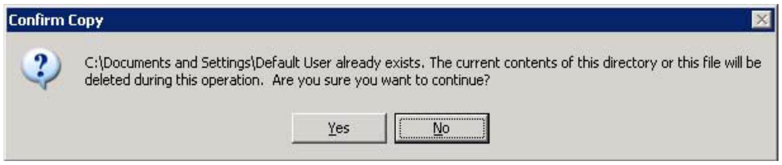
Step #8.
Click Ok.



Copy profile to
C:\Documents and Settings\Default User

Permitted to use
\Everyone

Step #9
Click the Yes button.

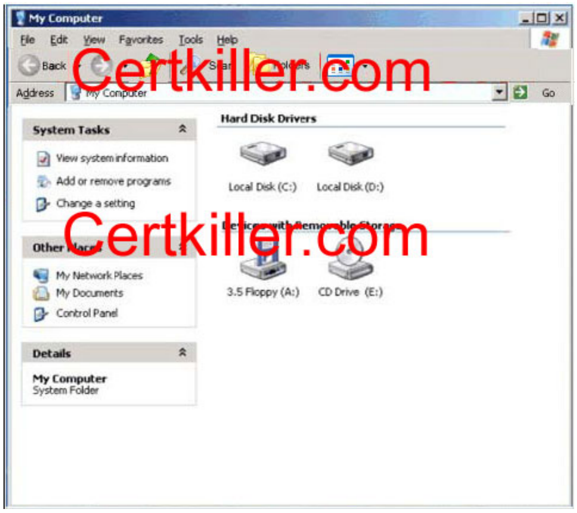


C:\Documents and Settings\Default User already exists. The current contents of this directory or this file will be deleted during this operation. Are you sure you want to continue?

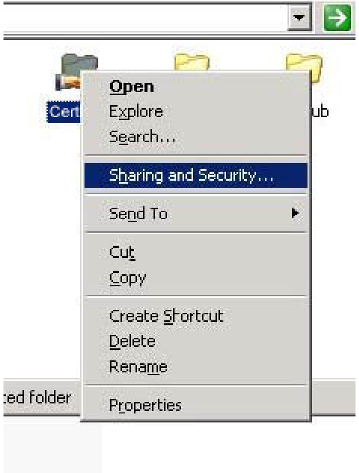
QUESTION 684
You are the network administrator for Certkiller . You administer a file server named Certkiller 6. Certkiller 6 runs Windows Server 2003.
Several users require access to resources on Certkiller 6. There are number of existing share and NTFS permissions for the C:\ Certkiller and C:\Sales folders on Certkiller 6.
You need to modify the existing permissions to ensure the appropriate access for the users and groups listed in the following table.

Group or User	**Access**
SalesGroup	The ability to read files in the C:\ Certkiller shared folder
SalesUser	The ability to modify files in the C:\Sales shared folder
Administrators	The ability to full control over the files in the C:\ Certkiller shared folder

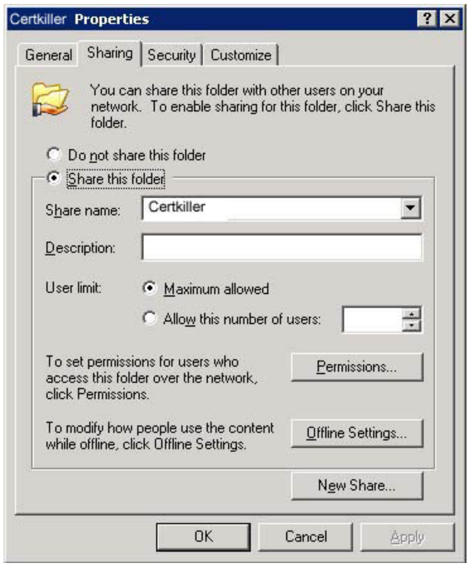
You want to use a single share permission entry for each shared folder. You must not change the access for any other user or groups.
What should you do?
Take the appropriate actions in the simulation window.
Simulation Window



Answer:
Step #1:
Open Local Disk (C:)
Step #2:
Right-click on the Certkiller folder, and select Sharing and Security



Step #3
On the Sharing tab, click Permissions.



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Certkiller

Description:

User limit: ● Maximum allowed

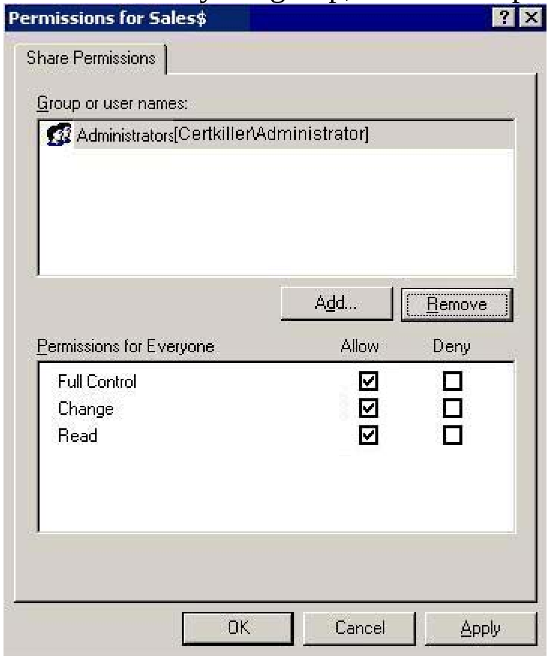
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

Step #4

Allow the Everyone group, full control permission and click Ok.



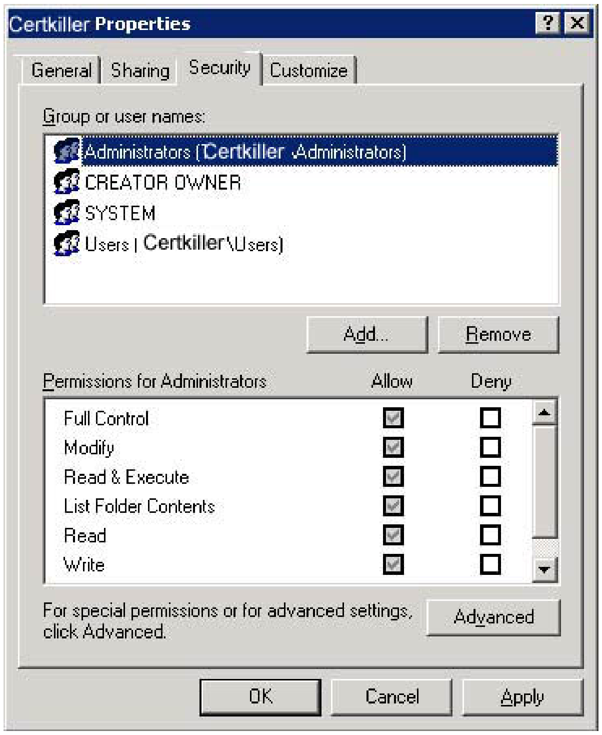
Group or user names:

Administrators[Certkiller\Administrator]

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Step #5.

Go to the Security tab and click the Advanced button.



Group or user names:

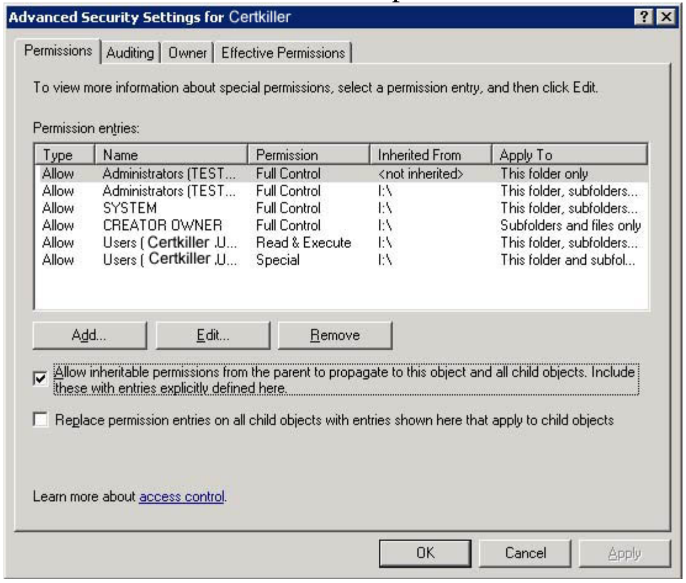
- Administrators (Certkiller \Administrators)
- CREATOR OWNER
- SYSTEM
- Users (Certkiller\Users)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Step #6

Untick the "Allow inheritable permissions..." checkbox.



To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (TEST...	Full Control	<not inherited>	This folder only
Allow	Administrators (TEST...	Full Control	I:\	This folder, subfolders...
Allow	SYSTEM	Full Control	I:\	This folder, subfolders...
Allow	CREATOR OWNER	Full Control	I:\	Subfolders and files only
Allow	Users (Certkiller .U...	Read & Execute	I:\	This folder, subfolders...
Allow	Users (Certkiller .U...	Special	I:\	This folder and subfol...

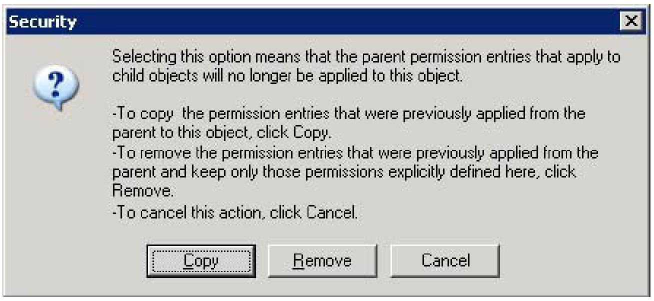
☑ Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

□ Replace permission entries on all child objects with entries shown here that apply to child objects

Learn more about access control.

Step #7

Click Copy then click ok to return to the permission dialog box.



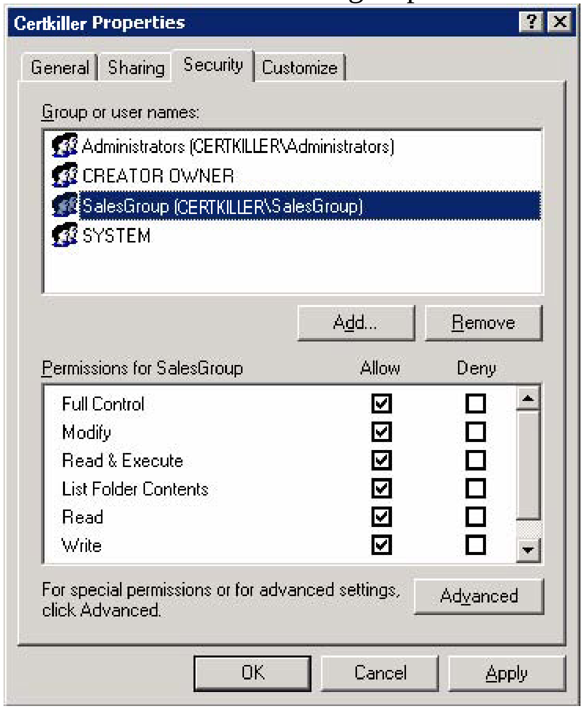
Security

Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.

-To copy the permission entries that were previously applied from the parent to this object, click Copy.
-To remove the permission entries that were previously applied from the parent and keep only those permissions explicitly defined here, click Remove.
-To cancel this action, click Cancel.

Step #8

Ensure the Administrators group has Full Control Permission and SalesGroup have Read permission.



Certkiller Properties

Group or user names:

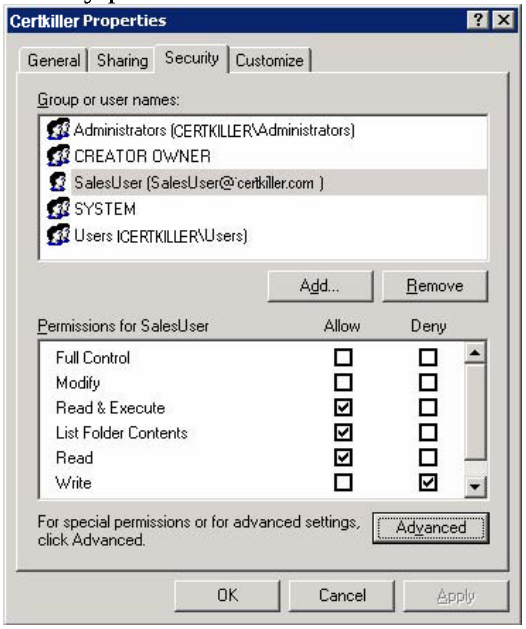
- Administrators (CERTKILLER\Administrators)
- CREATOR OWNER
- SalesGroup (CERTKILLER\SalesGroup)
- SYSTEM

Permissions for SalesGroup	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Follow the previous steps to configure access to the Sales folder. The SalesUser account should have

Modify permission on the folder.



Certkiller Properties

Group or user names:

- Administrators (CERTKILLER\Administrators)
- CREATOR OWNER
- SalesUser (SalesUser@certkiller.com)
- SYSTEM
- Users (CERTKILLER\Users)

Permissions for SalesUser	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	☑

For special permissions or for advanced settings, click Advanced.

QUESTION 685

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All network servers run Windows Server 2003 and all client computers run Windows XP Professional. Four of the client computers on the network are named Certkiller 1, Certkiller 2, Certkiller 3, and Certkiller 4.

You are responsible for the day-to-day administration of the computer objects in the domain.

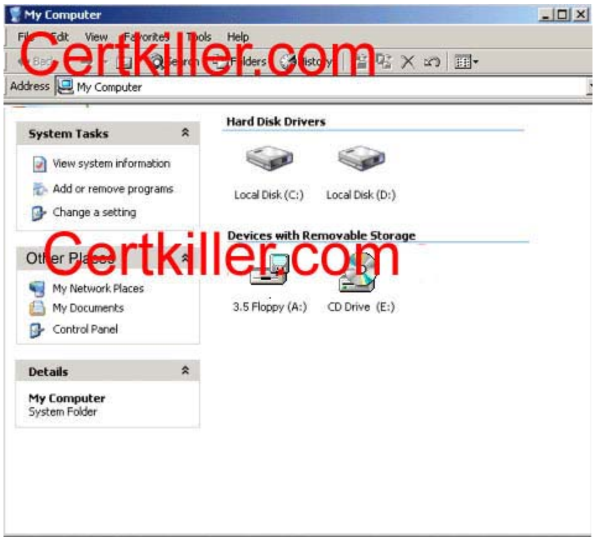
You need to use Active Directory Users and Computers to perform the following tasks:

- Delete an obsolete computer account named Certkiller A for a computer that has been rebuilt and renamed.
- Reset the computer for Certkiller 2.
- Move the Certkiller 3 and Certkiller 4 objects from the Computers container to the Sales OU.
- Add Certkiller 1 to the Windows XP Client global security group.

What should you do?

Take the appropriate actions in the simulation window.

Simulation Window

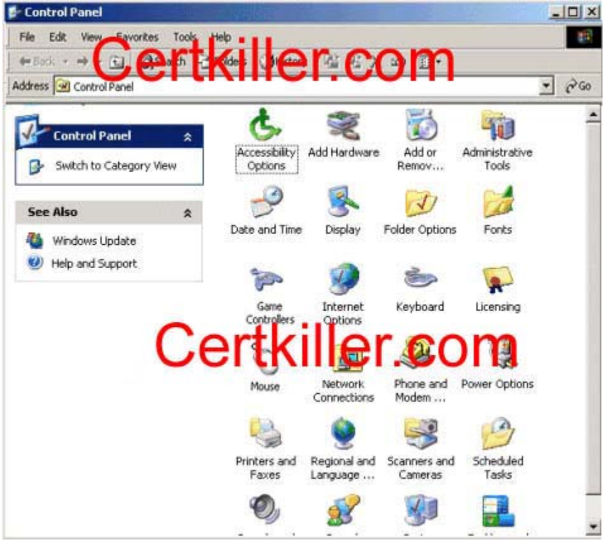


Answer:

The first requirement of this question states: Delete an obsolete computer account named Certkiller A for a computer that has been rebuilt and renamed.

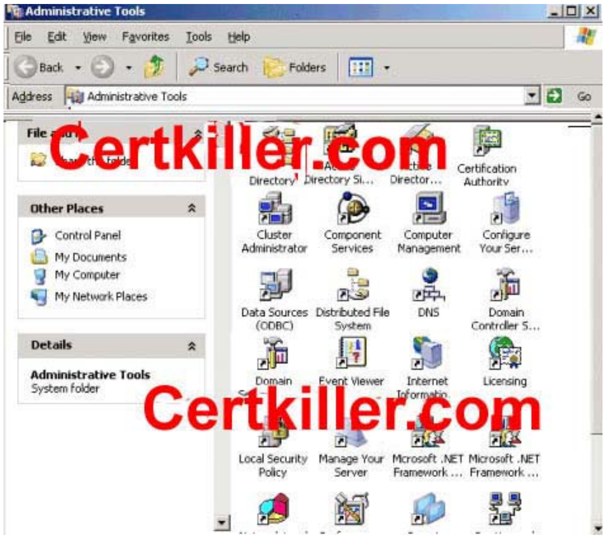
Step #1

Open Control Panel.



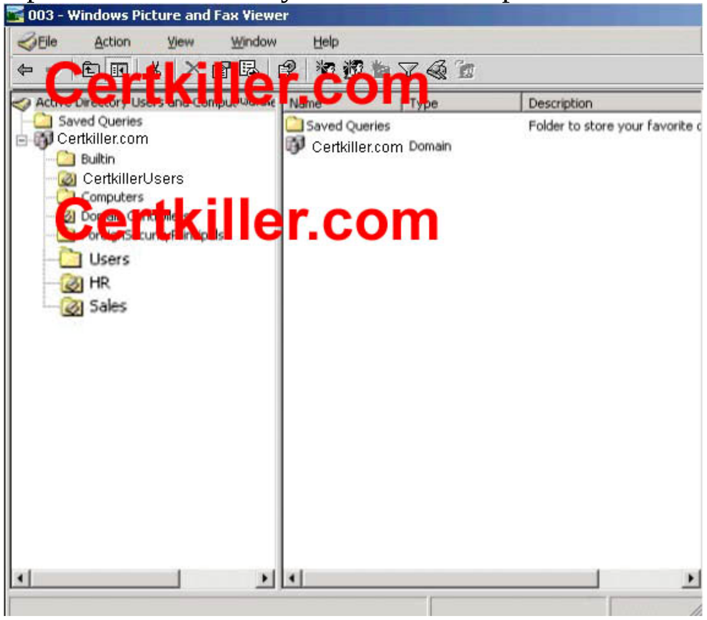
Step #2

Open Administrative Tools.

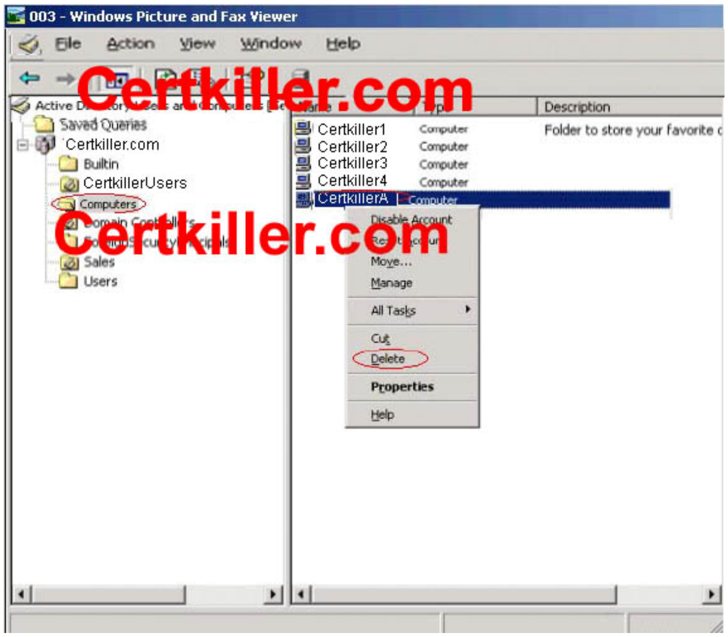


Step #3

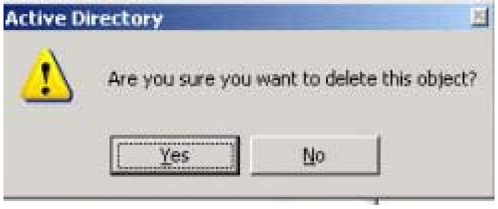
Open Active Directory Users and Computers.



Step #4. Select the Computers Container, right-click on Certkiller A and Select delete.



Step #5 Confirm

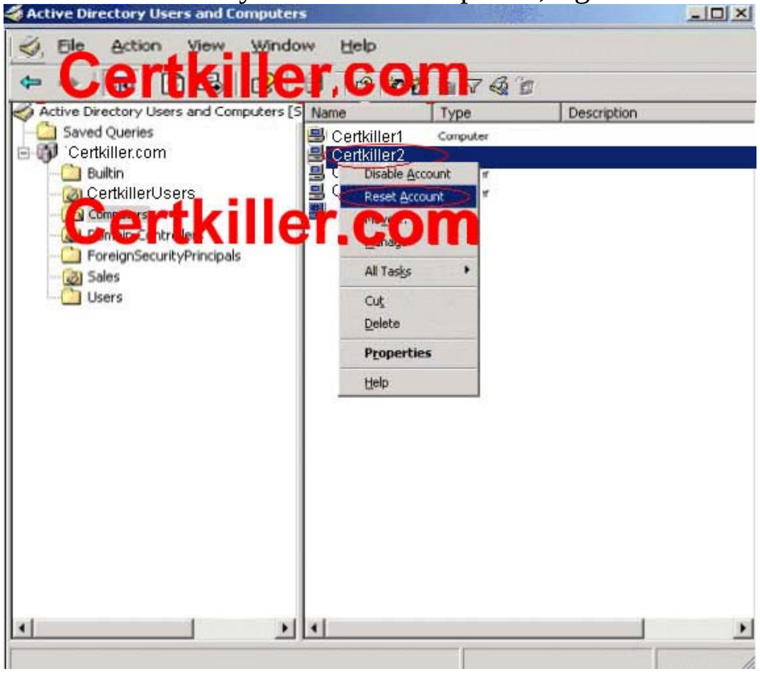


Are you sure you want to delete this object?

The second requirement of this question states: Reset the computer for Certkiller 2.

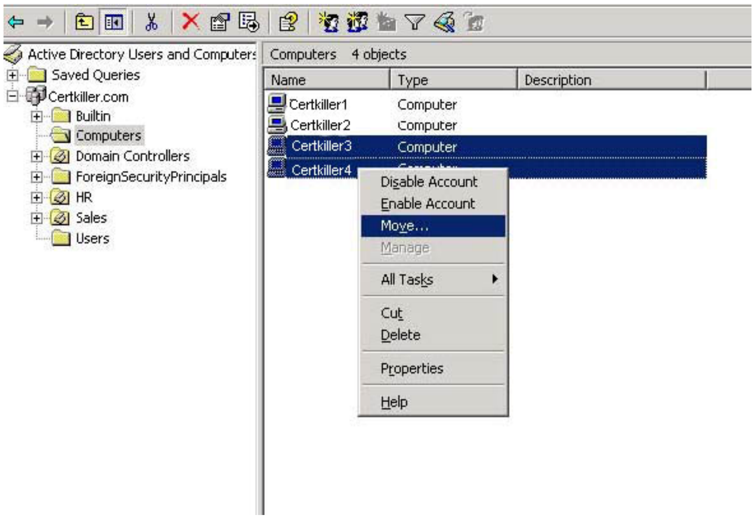
Step #1

In Active Directory Users and Computers, right-click on Certkiller 2 and select Reset Account



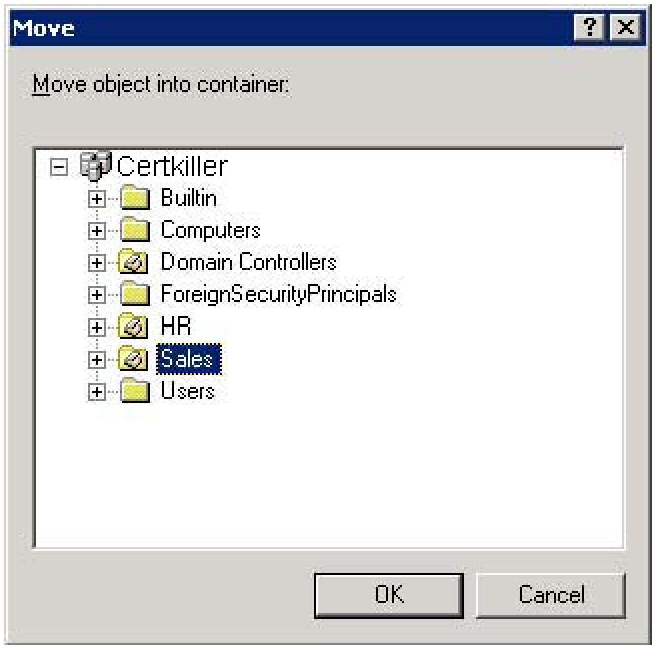
The third requirement of this question states: Move the Certkiller 3 and Certkiller 4 objects from the Computers container to the Sales OU.

Step #1.
In Active Directory Users and Computers, select Certkiller 3 and Certkiller 4, right-click and select Move.

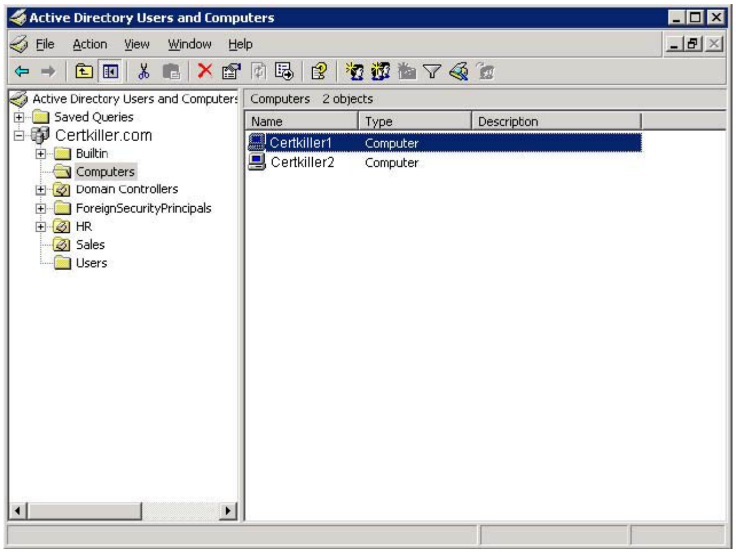


Name	Type	Description
Certkiller1	Computer	
Certkiller2	Computer	
Certkiller3	Computer	
Certkiller4	Computer	

Step #2.
Select the Sales OU and click OK.



The fourth requirement of this question states: Add Certkiller 1 to the Windows XP Client global security group.
Step #1.
In Active Directory Users and Computers, double click Certkiller 1.

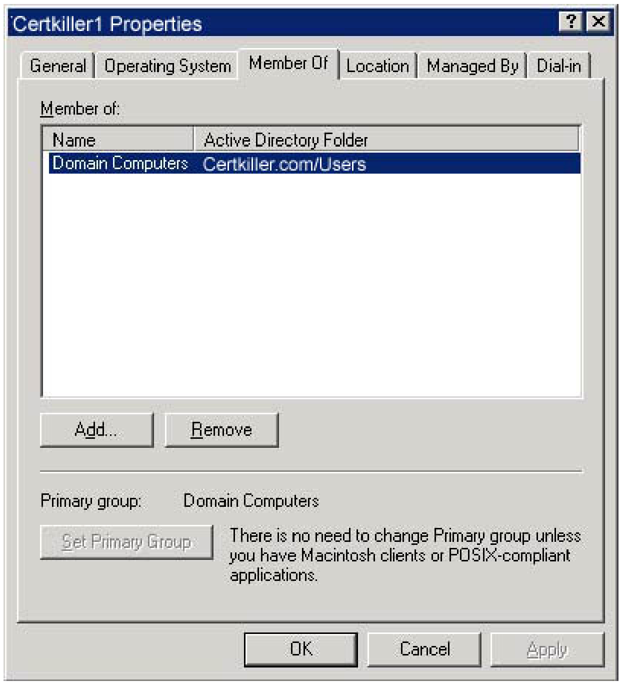

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computers
Saved Queries
Certkiller.com
Builtin
Computers
Doman Controllers
ForeignSecurityPrincipals
HR
Sales
Users

Computers 2 objects

Name	Type	Description
Certkiller1	Computer	
Certkiller2	Computer	

Step #2.

Select the Member Of tab and click the Add button.



Member of:

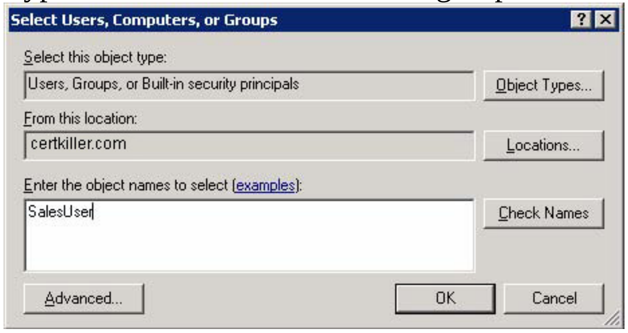
Name	Active Directory Folder
Domain Computers	Certkiller.com/Users

Primary group: Domain Computers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Step #3.

Type Windows XP Client for the group name and click OK.

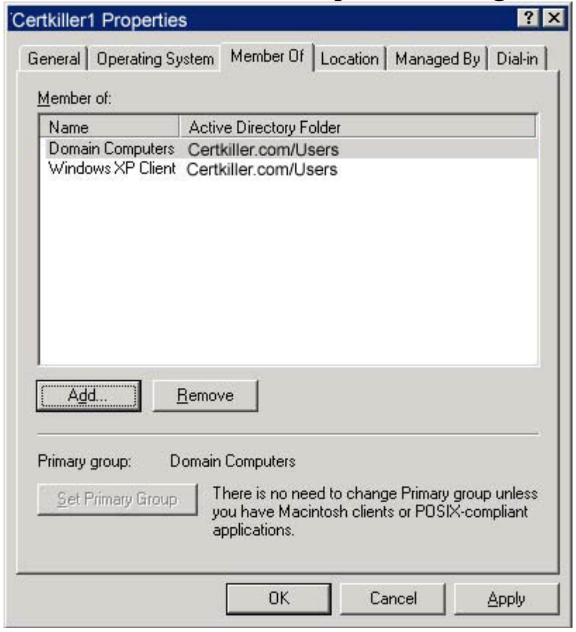


Select this object type:
Users, Groups, or Built-in security principals

From this location:
certkiller.com

Enter the object names to select (examples):
SalesUser

Step #4.
Click OK to close the Properties dialog box.



Certkiller1 Properties

Member of:

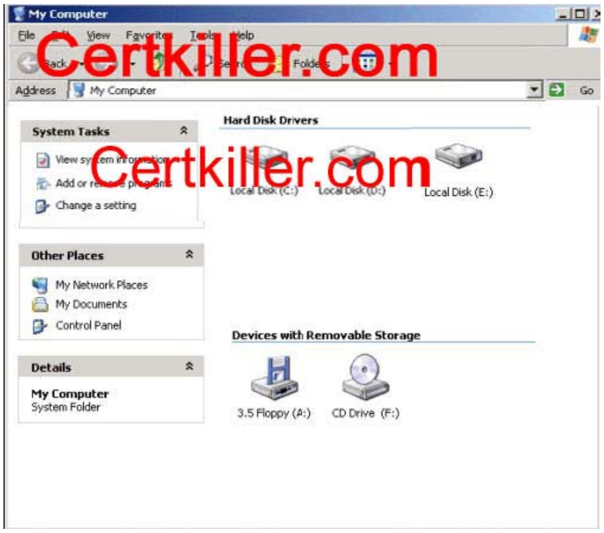
Name	Active Directory Folder
Domain Computers	Certkiller.com/Users
Windows XP Client	Certkiller.com/Users

Primary group: Domain Computers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

QUESTION 686

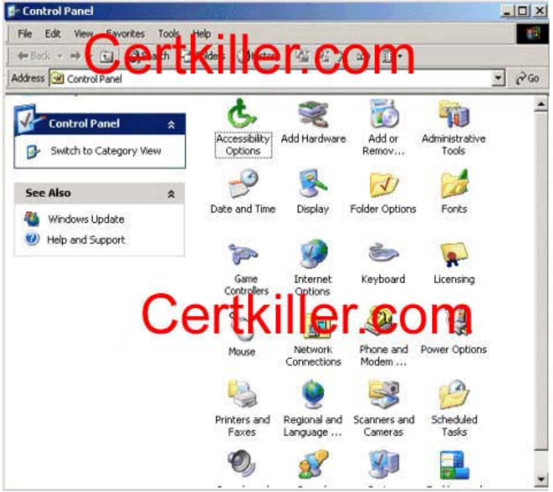
You are the network administrator for Certkiller .com. All network servers run Windows Server 2003.
A file server in the data center is used to store customer data and large database reports that are generated daily. The disk that holds this data is near capacity. The system engineer wants to move data from a disk named Disk 0 to a new, recently installed Disk 1. Disk 1 has a single partition that is formatted as FAT32. The partition currently contains no data.
You need to configure Disk1 so that it can be extended in the future to increase disk space without moving or deleting data. You also need to configure Disk 1 for optimum write performance.
What should you do?
Take the appropriate actions in the simulation window.
Simulation Window



Answer:
We need to configure Disk 1 (partition E) so that we can extend it in the future without losing data. To do this, the disk must be a dynamic disk and the partition must formatted with the NTFS file system. Furthermore, the partition needs to have been created on a dynamic disk so we'll need to delete the existing partition then convert the disk to a dynamic disk and then recreate the partition. The question states that the partition contains no data so deleting the partition won't cause any data loss.

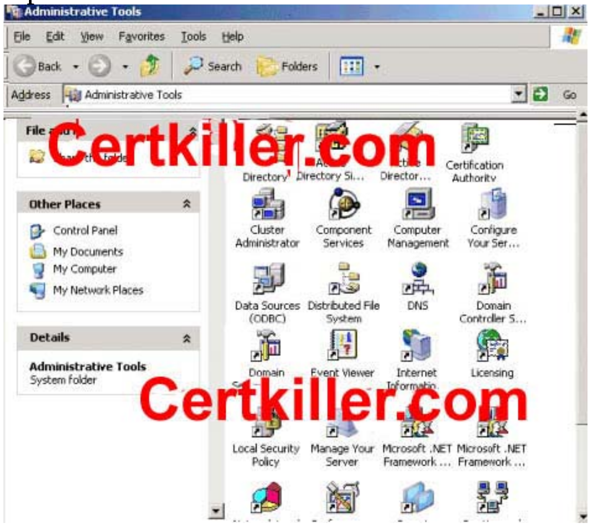
Step #1

Open Control Panel.



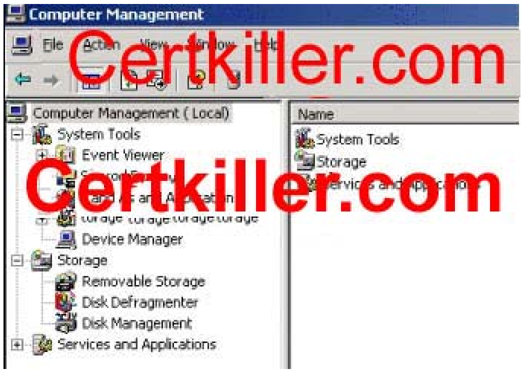
Step #2

Open Administrative Tools.

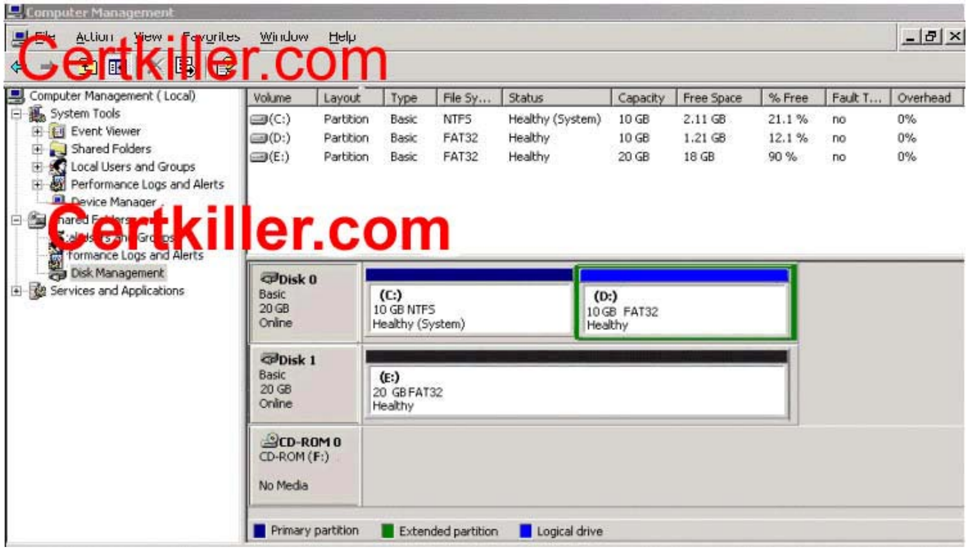


Step #3.

Open Computer Management.

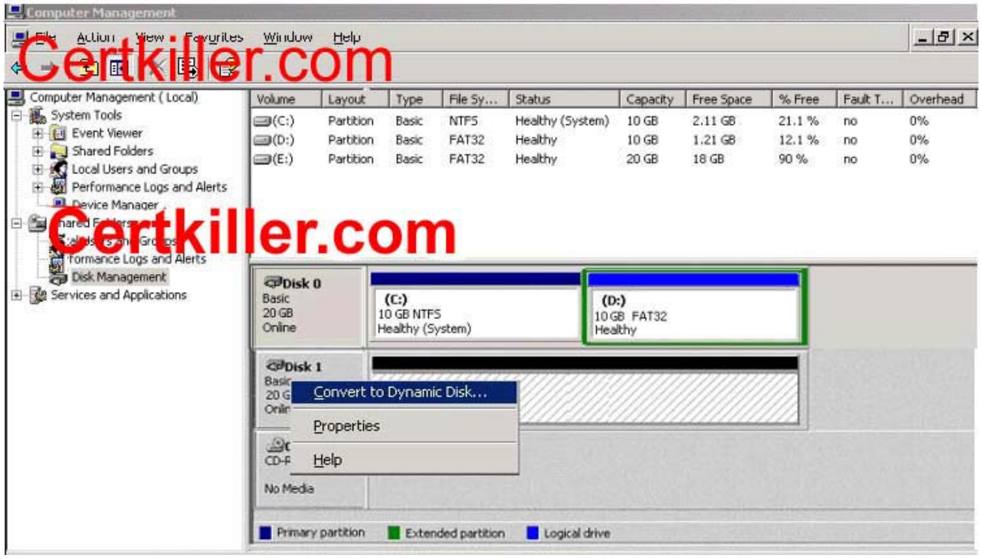


Step #4.
Select Disk Management



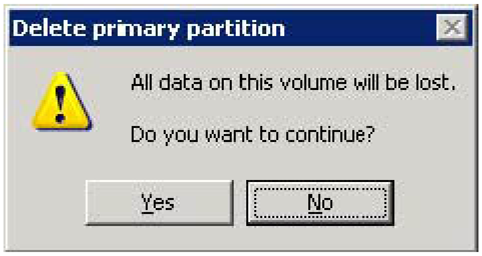
Volume	Layout	Type	File Sy...	Status	Capacity	Free Space	% Free	Fault T...	Overhead
(C:)	Partition	Basic	NTFS	Healthy (System)	10 GB	2.11 GB	21.1 %	no	0%
(D:)	Partition	Basic	FAT32	Healthy	10 GB	1.21 GB	12.1 %	no	0%
(E:)	Partition	Basic	FAT32	Healthy	20 GB	18 GB	90 %	no	0%

Step #5.
Right click on partition E and select Delete Partition.



Volume	Layout	Type	File Sy...	Status	Capacity	Free Space	% Free	Fault T...	Overhead
(C:)	Partition	Basic	NTFS	Healthy (System)	10 GB	2.11 GB	21.1 %	no	0%
(D:)	Partition	Basic	FAT32	Healthy	10 GB	1.21 GB	12.1 %	no	0%
(E:)	Partition	Basic	FAT32	Healthy	20 GB	18 GB	90 %	no	0%

Step #6.
Confirm the deletion.

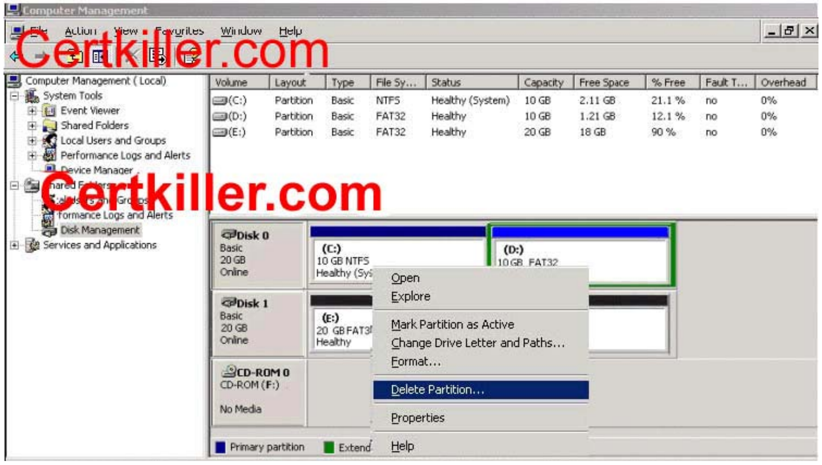


Delete primary partition

All data on this volume will be lost.

Do you want to continue?

Step #7.
Right click on Disk one and select "Convert to dynamic disk".



Computer Management

Volume	Layout	Type	File Sy...	Status	Capacity	Free Space	% Free	Fault T...	Overhead
(C:)	Partition	Basic	NTFS	Healthy (System)	10 GB	2.11 GB	21.1 %	no	0%
(D:)	Partition	Basic	FAT32	Healthy	10 GB	1.21 GB	12.1 %	no	0%
(E:)	Partition	Basic	FAT32	Healthy	20 GB	18 GB	90 %	no	0%

Disk 0
Basic
20 GB
Online

(C:)
10 GB NTFS
Healthy (Sys

(D:)
10 GB FAT32

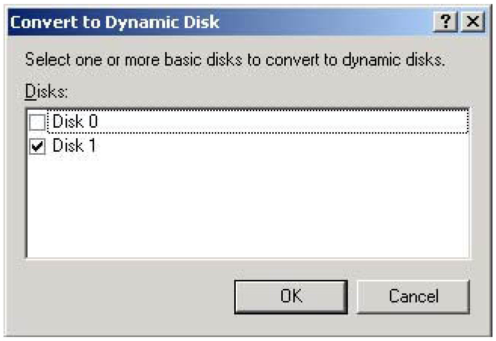
Disk 1
Basic
20 GB
Online

(E:)
20 GB FAT3
Healthy

CD-ROM 0
CD-ROM (F:)

No Media

Step #8.
Ensure that Disk 1 is checked and click OK.



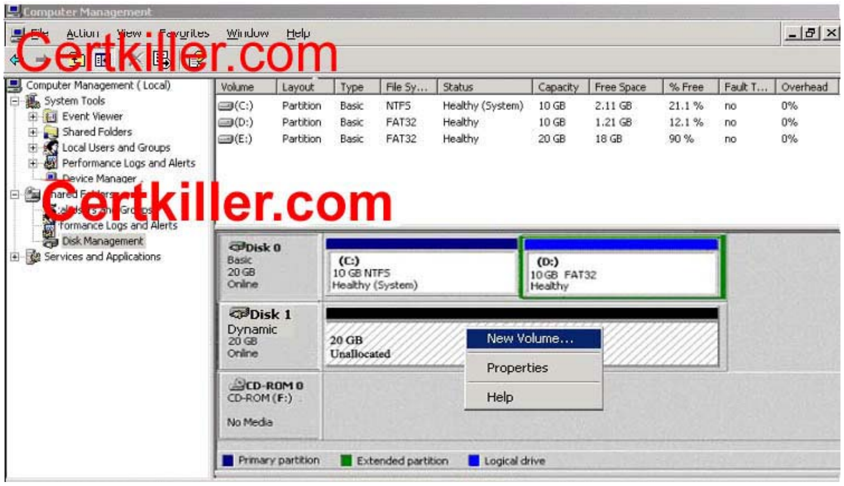
Convert to Dynamic Disk

Select one or more basic disks to convert to dynamic disks.

Disks:

□ Disk 0
☑ Disk 1

Step #9.
Right click on the unallocated disk space and select "New Volume".



Volume	Layout	Type	File Sy...	Status	Capacity	Free Space	% Free	Fault T...	Overhead
(C:)	Partition	Basic	NTFS	Healthy (System)	10 GB	2.11 GB	21.1 %	no	0%
(D:)	Partition	Basic	FAT32	Healthy	10 GB	1.21 GB	12.1 %	no	0%
(E:)	Partition	Basic	FAT32	Healthy	20 GB	18 GB	90 %	no	0%

Disk 0
Basic
20 GB
Online

(C:)
10 GB NTFS
Healthy (System)

(D:)
10 GB FAT32
Healthy

Disk 1
Dynamic
20 GB
Online

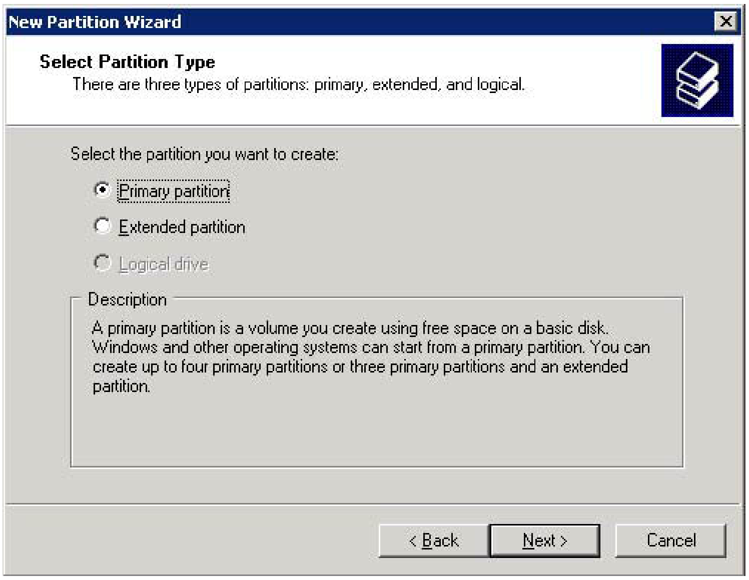
20 GB
Unallocated

CD-ROM 0
CD-ROM (F:)

No Media

Step #10.

The New Volume wizard starts. Click Next.



New Partition Wizard

Select Partition Type

There are three types of partitions: primary, extended, and logical.

Select the partition you want to create:

● Primary partition

○ Extended partition

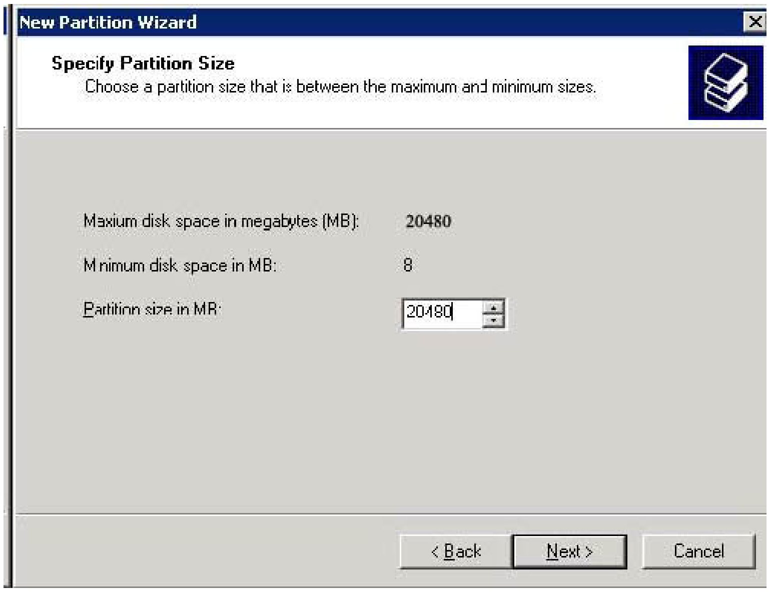
○ Logical drive

Description

A primary partition is a volume you create using free space on a basic disk. Windows and other operating systems can start from a primary partition. You can create up to four primary partitions or three primary partitions and an extended partition.

Step #11.

Select the maximum size.



New Partition Wizard

Specify Partition Size

Choose a partition size that is between the maximum and minimum sizes.

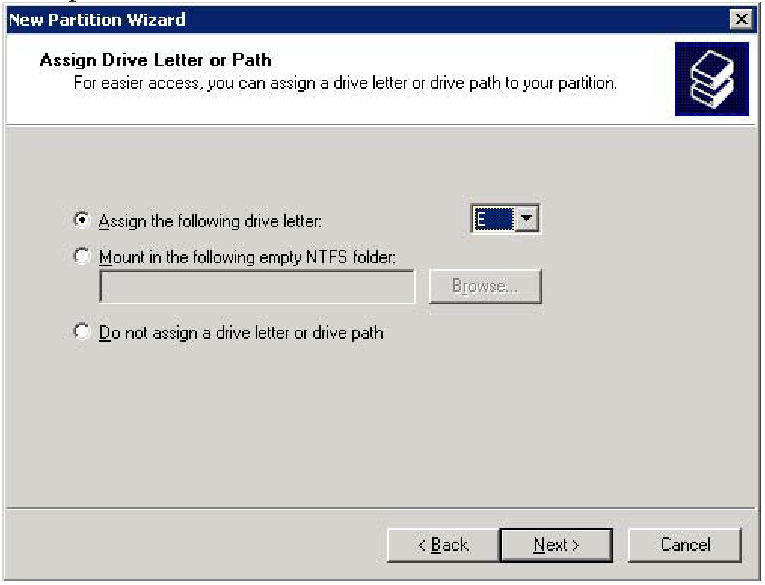
Maxium disk space in megabytes (MB): 20480

M nimum disk space in MB: 8

Partition size in MB: 20480

Step #12.

Accept the default drive letter and click Next.



New Partition Wizard

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

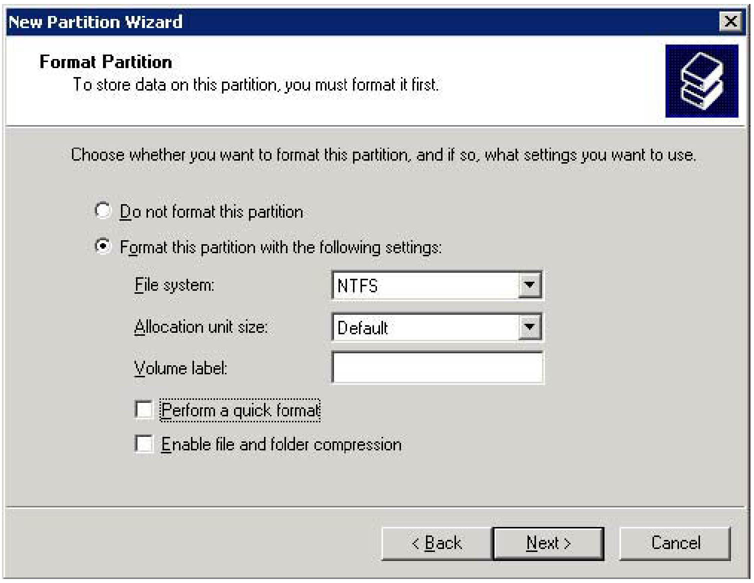
● Assign the following drive letter: E

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

Step #13.

Click Next.



Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this partition, and if so, what settings you want to use.

○ Do not format this partition

● Format this partition with the following settings:

File system: NTFS

Allocation unit size: Default

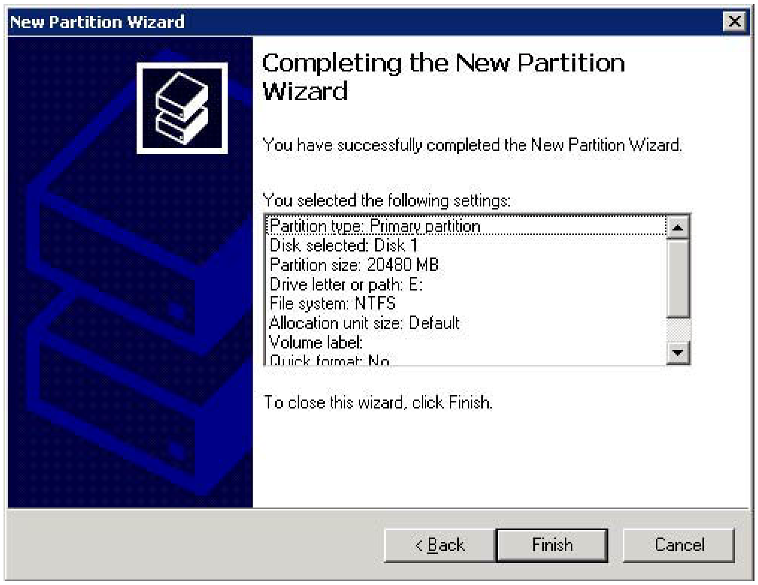
Volume label:

□ Perform a quick format

□ Enable file and folder compression

Step #14.

Click Finish.



Completing the New Partition Wizard

You have successfully completed the New Partition Wizard.

You selected the following settings:

Partition type: Primary partition
Disk selected: Disk 1
Partition size: 20480 MB
Drive letter or path: E:
File system: NTFS
Allocation unit size: Default
Volume label:
Quick format: No

To close this wizard, click Finish.

QUESTION 687

You are the network administrator for Certkiller .com. You administer a Windows Server 2003 named Certkiller 7. Certkiller 7 functions as a file server for Certkiller .com's Sales department.

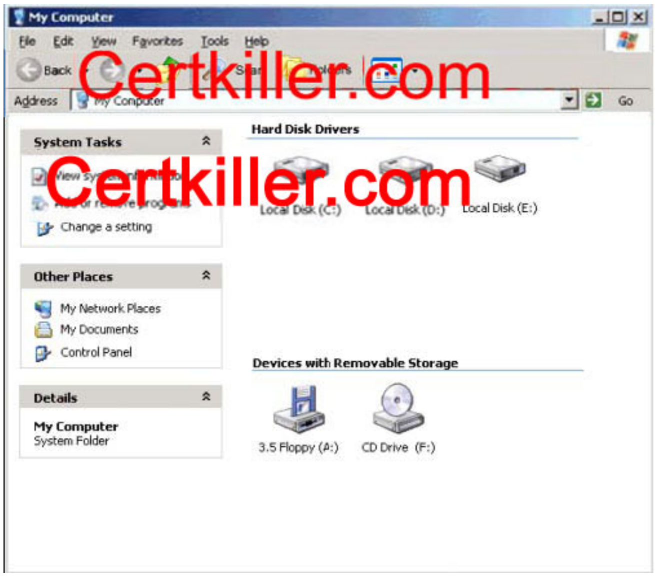
You need to perform the following tasks on Certkiller 7:

- Create a share named Certkiller on the C:\ Certkiller folder.
- On the Certkiller share, configure share permissions so that the SalesGroup has only the Allow-Read permission. No other groups should have access to the share.
- Modify the existing share named Sales to the C:\Sales folder so that the share is hidden.
- On the hidden share, configure share permissions so that the Administrators group has the Allow-Full Control permission. No other groups should have access to the share.

What should you do?

Take the appropriate actions in the simulation window.

Simulation Window



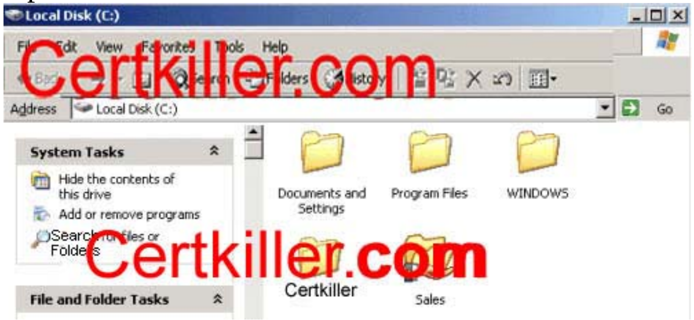
Answer:

The first requirement of this question states: Create a share named Certkiller on the C:\ Certkiller folder.

The second requirement states: On the Certkiller share, configure share permissions so that the SalesGroup has only the Allow-Read permission. No other groups should have access to the share.

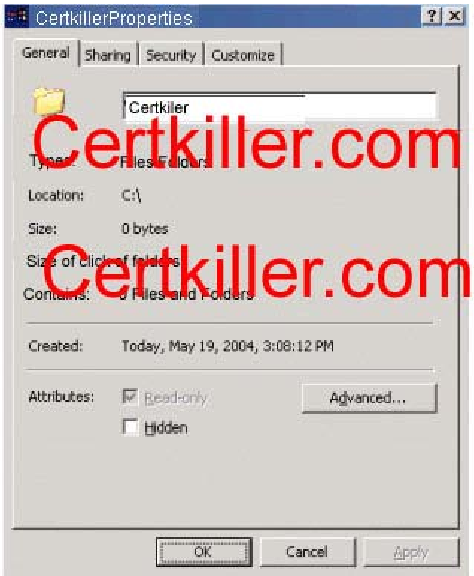
Step #1.

Open Disk C:



Step #2.

Right-click on folder Certkiller and select Properties



CertkillerProperties

Certkiller

Type: Files Folders

Location: C:\

Size: 0 bytes

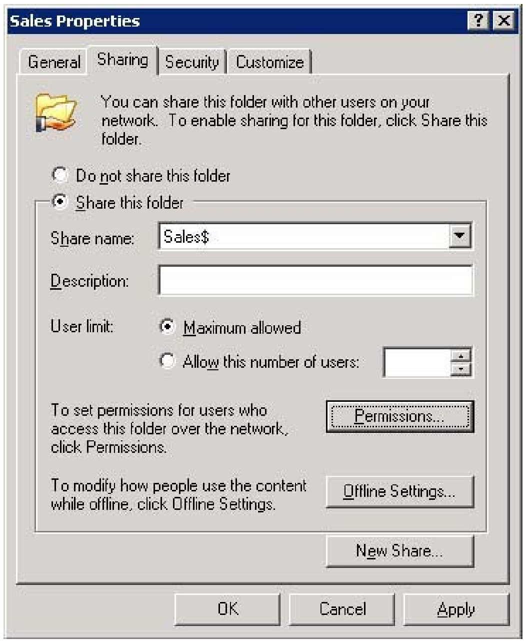
Size of click of folders

Contains: 0 Files and Folders

Created: Today, May 19, 2004, 3:08:12 PM

Attributes: ☑ Read-only
□ Hidden

Step 3: Click the Sharing tab, select Share this folder and enter the share name Certkiller . Then click the Permissions button.



Sales Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Sales$

Description:

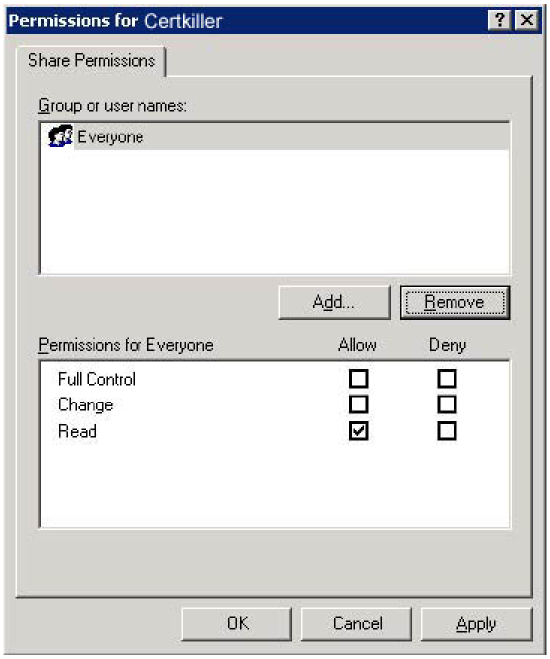
User limit: ● Maximum allowed
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

Step 4:

Click Add.



Permissions for Certkiller

Share Permissions

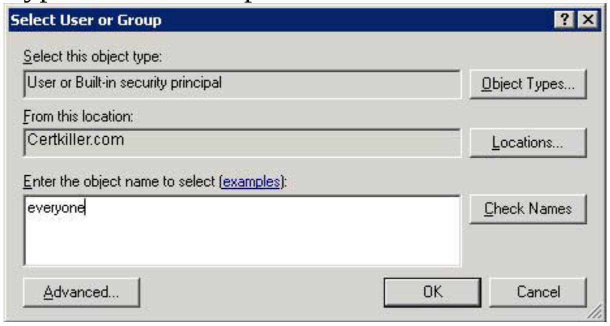
Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Step #5.

Type in SalesGroup and click ok.



Select User or Group

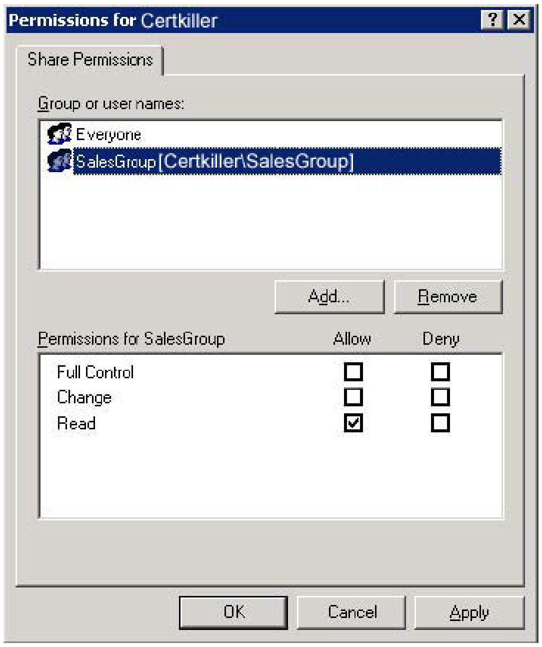
Select this object type:
User or Built-in security principal

From this location:
Certkiller.com

Enter the object name to select (examples):
everyone

Step#6.

Select the Everyone group and click Remove.



Group or user names:

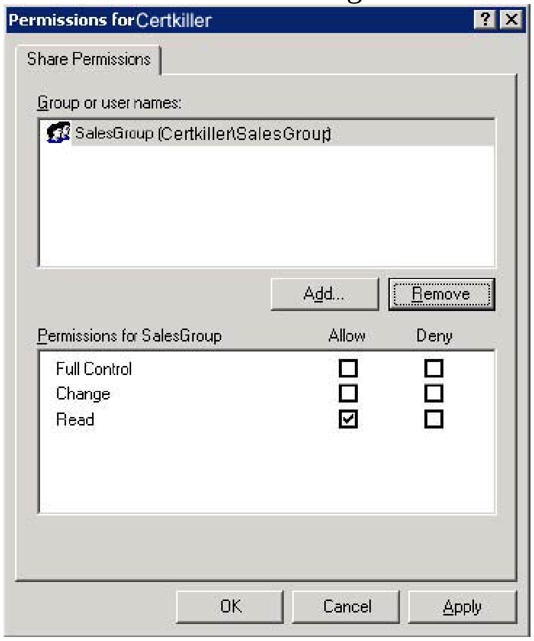
Everyone

SalesGroup [Certkiller\SalesGroup]

Permissions for SalesGroup	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Step #7.

Click Ok to close the dialog box.



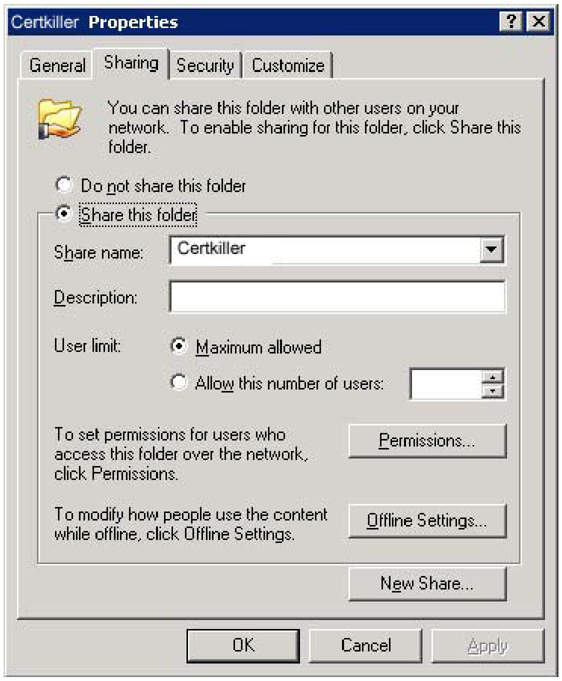
Group or user names:

SalesGroup (Certkiller\SalesGroup)

Permissions for SalesGroup	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Step #8.

Click Ok to close the dialog box.



Certkiller Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Certkiller

Description:

User limit: ● Maximum allowed ○ Allow this number of users:

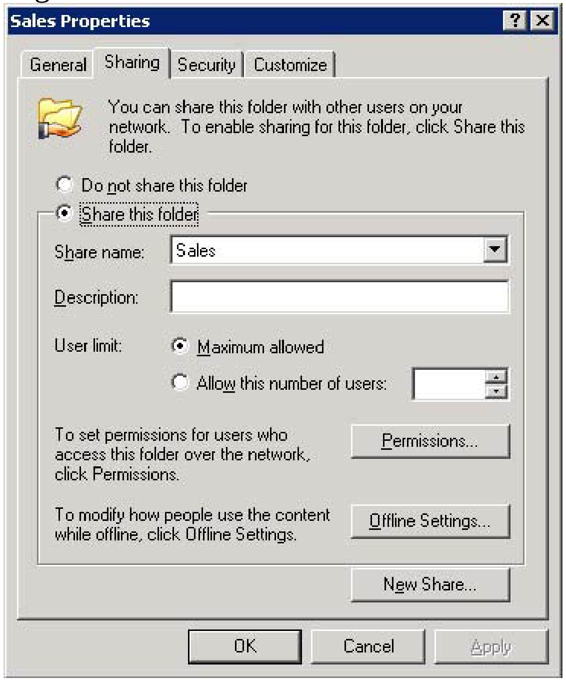
To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

The third requirement of this question states: Modify the existing share named Sales to the C:\Sales folder so that the share is hidden. We can do this by creating a new share named Sales$ and deleting the existing 'Sales' share (note: it is not possible to rename a share).

Step #1.

Right-click on the Sales folder and select Properties. On the Sharing tab, click New Share.



Sales Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Sales

Description:

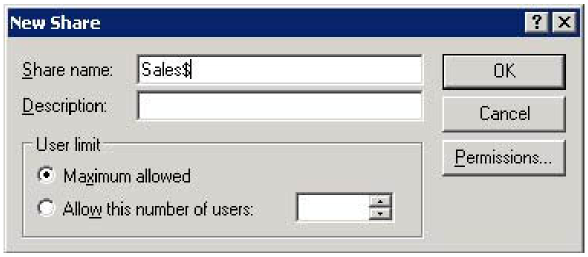
User limit: ● Maximum allowed ○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

Step #2.

Enter the new share name and click OK.



New Share

Share name: Sales$

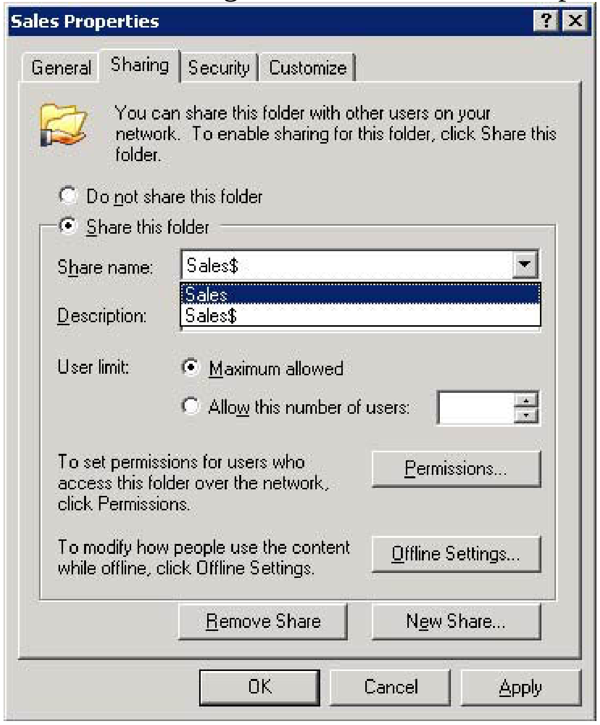
Description:

User limit

● Maximum allowed

○ Allow this number of users:

Step #3.
Select the existing Sales share from the drop down list. Click the Remove Share button.



Sales Properties

General | Sharing | Security | Customize

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Sales$

Sales
Sales$

Description:

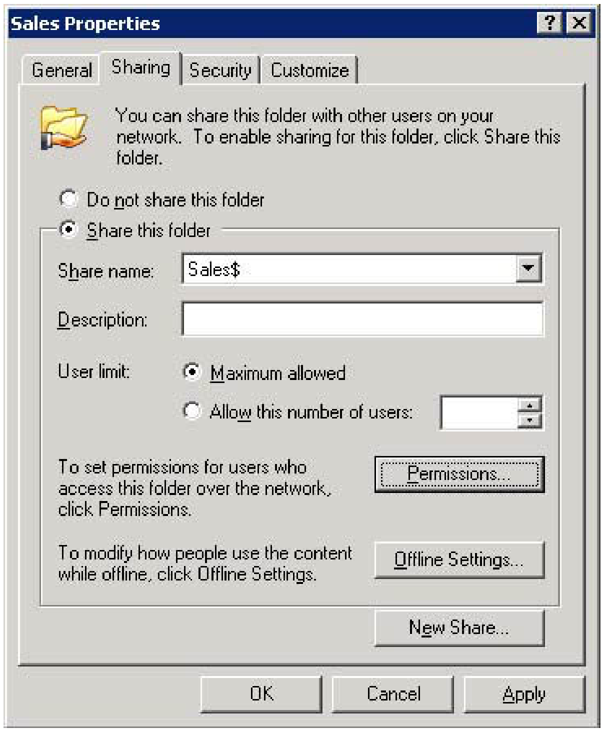
User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

The fourth requirement of this question states: On the hidden share, configure share permissions so that the Administrators group has the Allow-Full Control permission. No other groups should have access to the share.
Step #1.
Right click on the Sales folder and select properties. Go to the Sharing tab (if you closed the dialog box after the previous step. Click the Permissions button.



Sales Properties

General | Sharing | Security | Customize

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Sales$

Description:

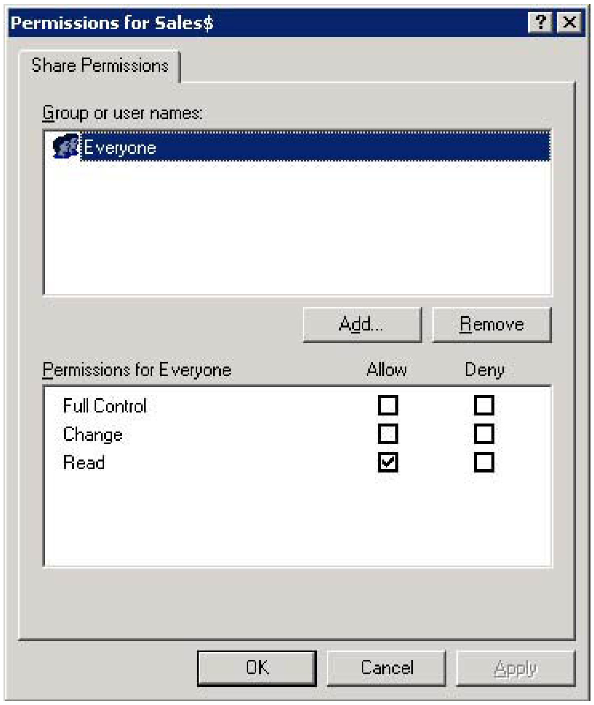
User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

Step #2.
Click Add.



Permissions for Sales$

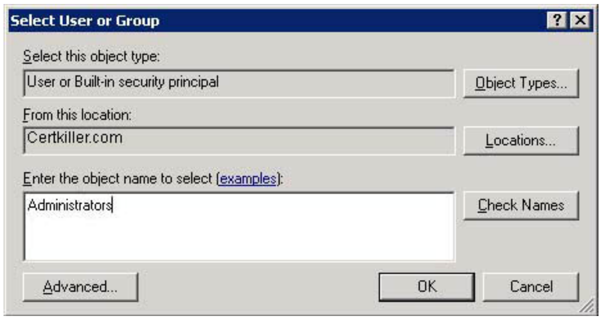
Share Permissions

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Step #3.
Type Administrators and click OK.



Select User or Group

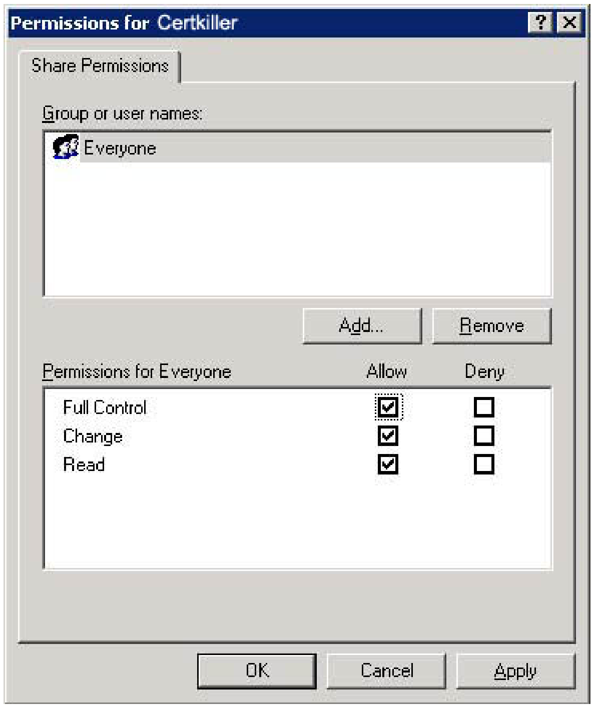
Select this object type: User or Built-in security principal

From this location: Certkiller.com

Enter the object name to select (examples): Administrators

Step #4.

Select the Full Control check box for the Administrators group.



Permissions for Certkiller

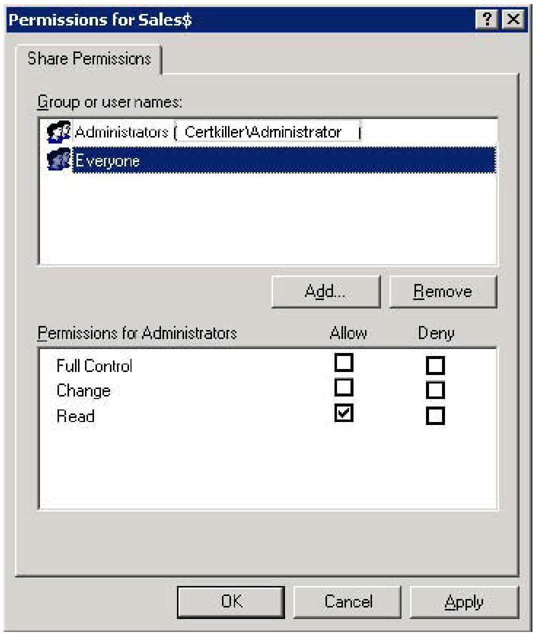
Share Permissions

Group or user names: Everyone

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Step #5.

Select the Everyone group and click Remove.



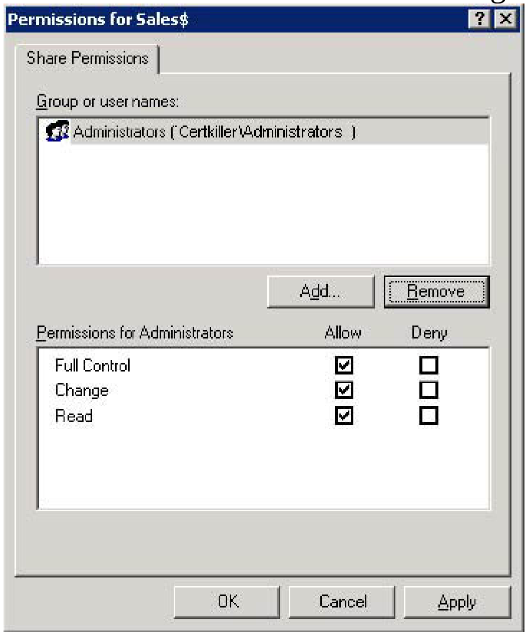
Permissions for Sales$

Group or user names:

Administrators (Certkiller\Administrator)
Everyone

Permissions for Administrators	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Step #6.
Click the OK button to close the dialog box.



Permissions for Sales$

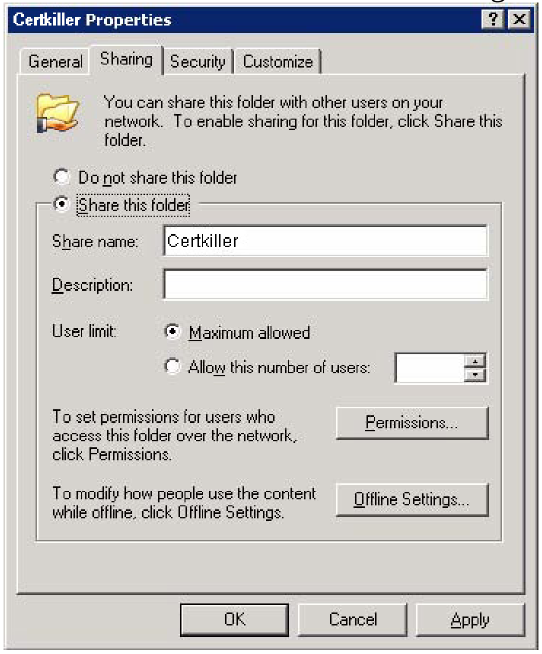
Group or user names:

Administrators (Certkiller\Administrators)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Step #7.

Click the OK button to close the dialog box.



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Certkiller

Description:

User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

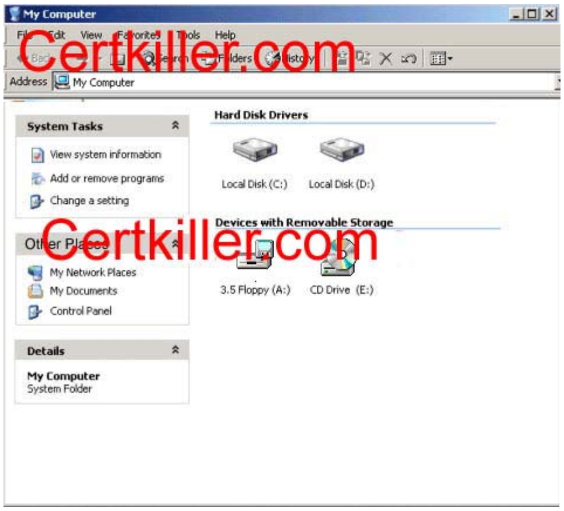
To modify how people use the content while offline, click Offline Settings.

QUESTION 688

You are the network administrator for Certkiller . The network consists of a single Active Directory Domain named Certkiller .com. Certkiller operates call centers in multiple cities around the world.
The network contains a Windows Server 2003 computer named Certkiller 6. All client computers run Windows XP Professional.
You are responsible for creating and managing user accounts.
Certkiller 's written security policy states that new employees must create new personal and confidential passwords the first time they log on to the network.
The fax number for employees whose user accounts are in the Sales OU has changed to (555) 555-5555.
A new employee named Jack King is hired to work in Certkiller 's Oxfort office.
You need to perform the following tasks:

- Create a user account for Jack King in the Sales OU that contains the same information as the user for an employee named Sandra Green. The user name for Jack's account should be TessK. The password should be set to Password12!. Jack should be allowed to log on to only a single client computer, which is named Certkiller 1.
- Ensure that all employees in the Sales OU have the correct fax number listed in their user accounts.

What should you do?
Take the appropriate actions in the simulation window.
Simulation Window

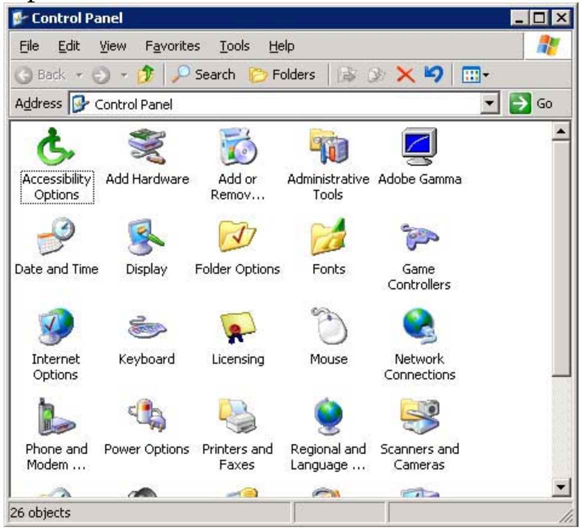


Answer:

The first requirement of this question states: Create a user account for Jack King in the Sales OU that contains the same information as the user for an employee named Sandra Green. The user name for Tess's account should be TessK. The password should be set to Password12!. Jack should be allowed to log on to only a single client computer, which is named Certkiller 1.

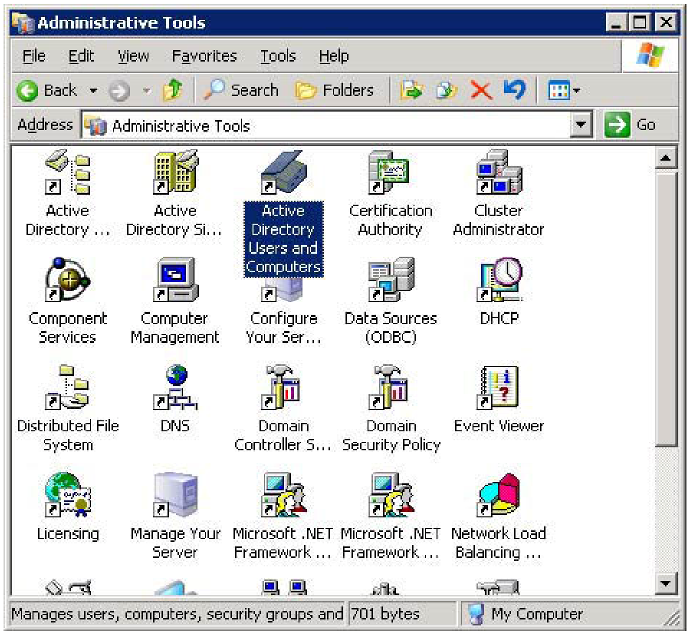
Step #1.

Open Control Panel



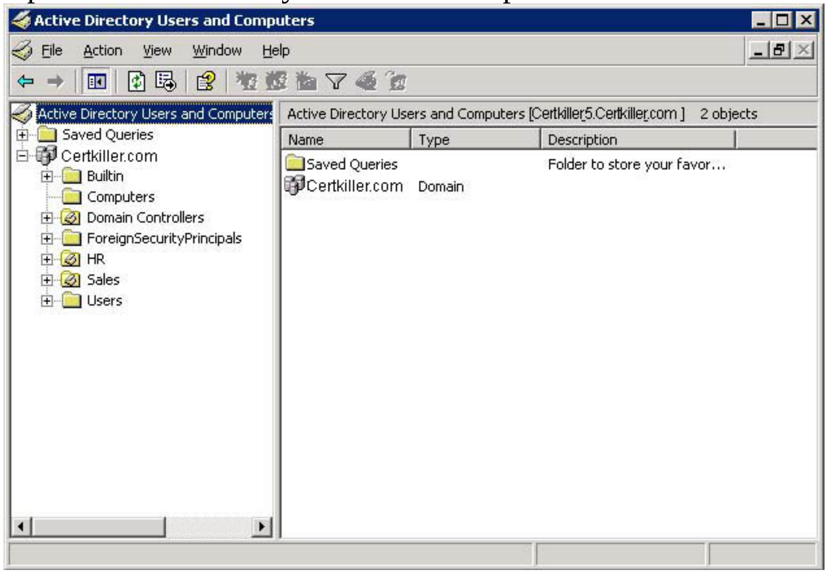
Step #2.

Open Adminstrative Tools



Step #3.

Open Active Directory Users and Computers

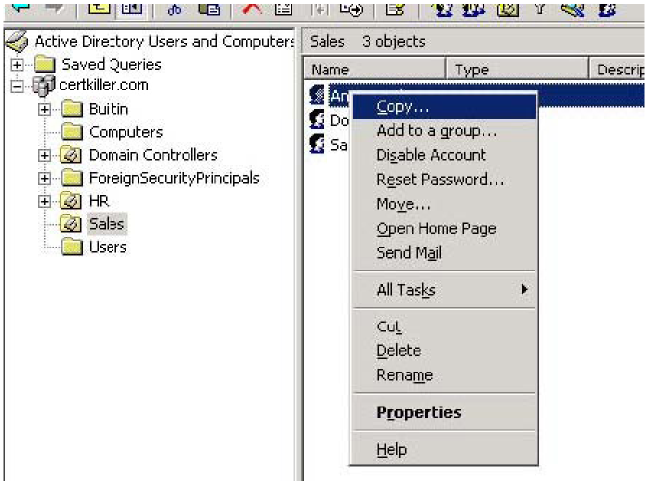

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computers
Saved Queries
Certkiller.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
HR
Sales
Users

Active Directory Users and Computers [Certkiller5.Certkiller.com] 2 objects

Name	Type	Description
Saved Queries		Folder to store your favor...
Certkiller.com	Domain	

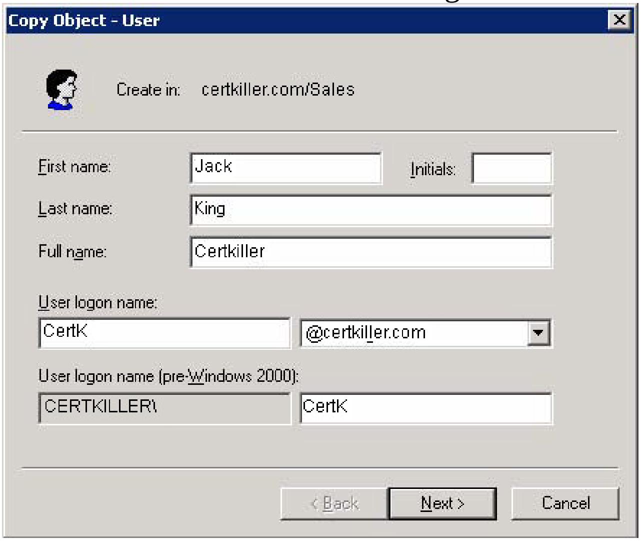
Step #4.

In the Sales OU, right click on Anna Smith user object and select "Copy".



Step #5.

Enter the information for Jack King and click Next.



Copy Object - User

Create in: certkiller.com/Sales

First name: Jack

Initials:

Last name: King

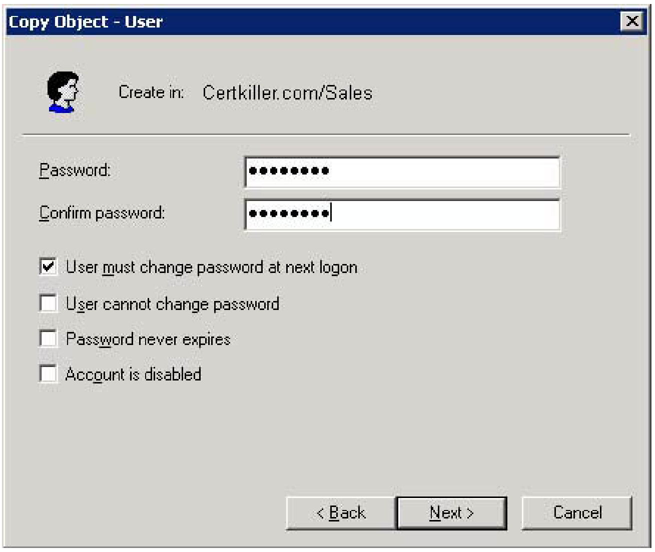
Full name: Certkiller

User logon name: CertK @certkiller.com

User logon name (pre-Windows 2000): CERTKILLER\ CertK

Step #6.

Enter Password12! for the password and select the "User must change password at next logon" checkbox.



Copy Object - User

Create in: Certkiller.com/Sales

Password: ••••••••

Confirm password: ••••••••

☑ User must change password at next logon

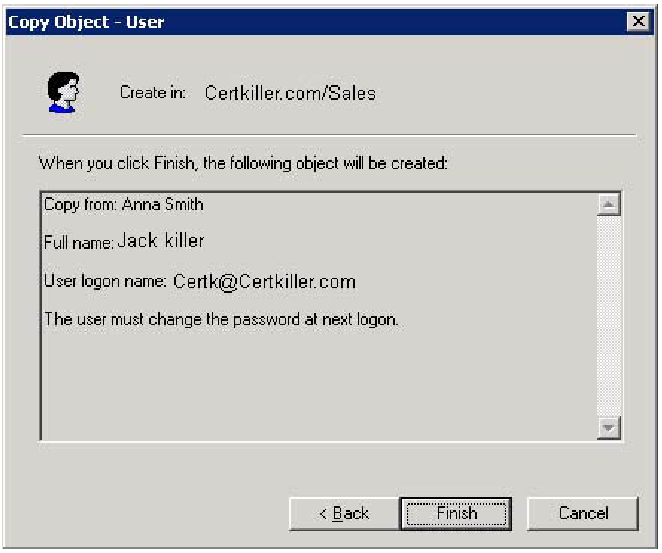
□ User cannot change password

□ Password never expires

□ Account is disabled

Step #7.

Click Finish.



Copy Object - User

Create in: Certkiller.com/Sales

When you click Finish, the following object will be created:

Copy from: Anna Smith

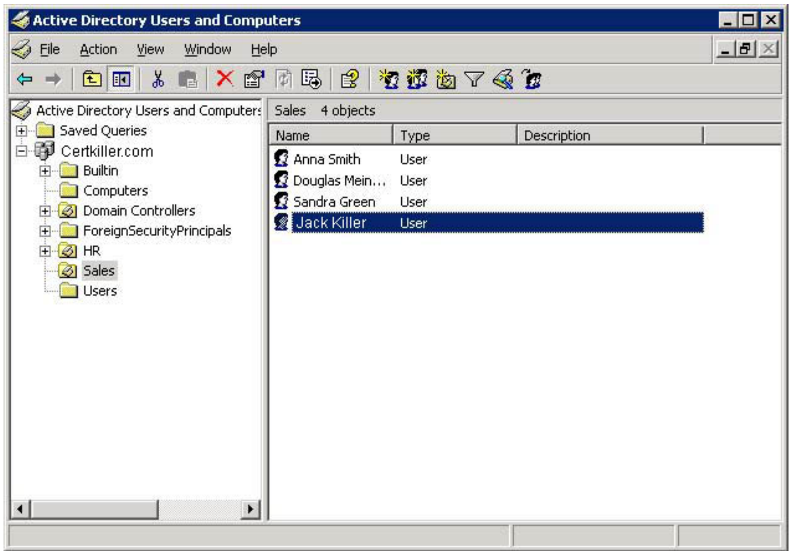
Full name: Jack killer

User logon name: Certk@Certkiller.com

The user must change the password at next logon.

Step #8.

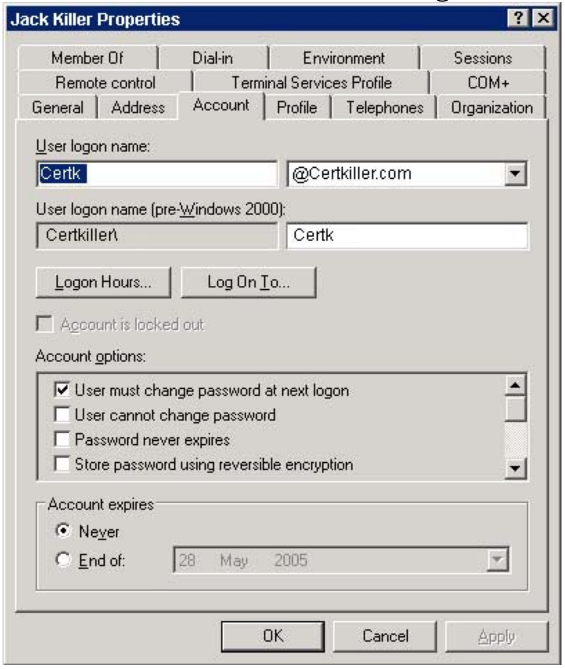
Double click the Jack King user object.


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computers
Saved Queries
Certkiller.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
HR
Sales
Users
Sales 4 objects

Name	Type	Description
Anna Smith	User	
Douglas Mein...	User	
Sandra Green	User	
Jack Killer	User	

Step #9.

On the Account tab, click the "Log On To" button.



User logon name: Certk @Certkiller.com

User logon name (pre-Windows 2000): Certkiller\ Certk

□ Account is locked out

Account options:

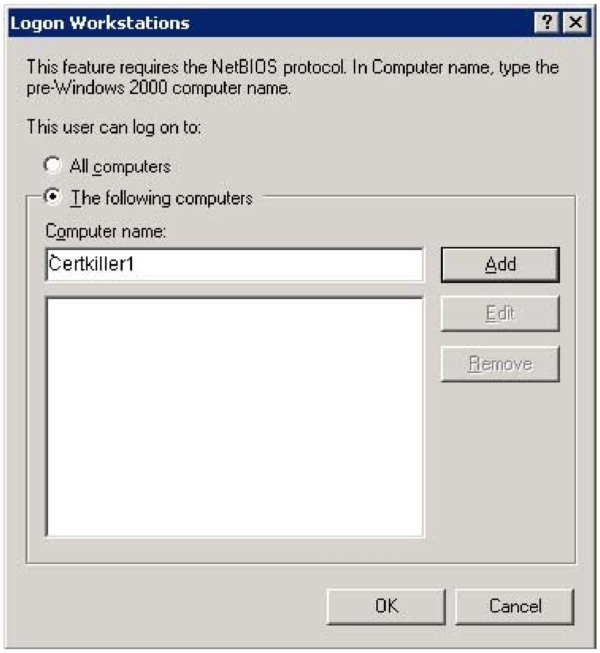
- ☑ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: 28 May 2005

Step #10.

Select "The following computers", type in Certkiller 1 and click Add.



Logon Workstations

This feature requires the NetBIOS protocol. In Computer name, type the pre-Windows 2000 computer name.

This user can log on to:

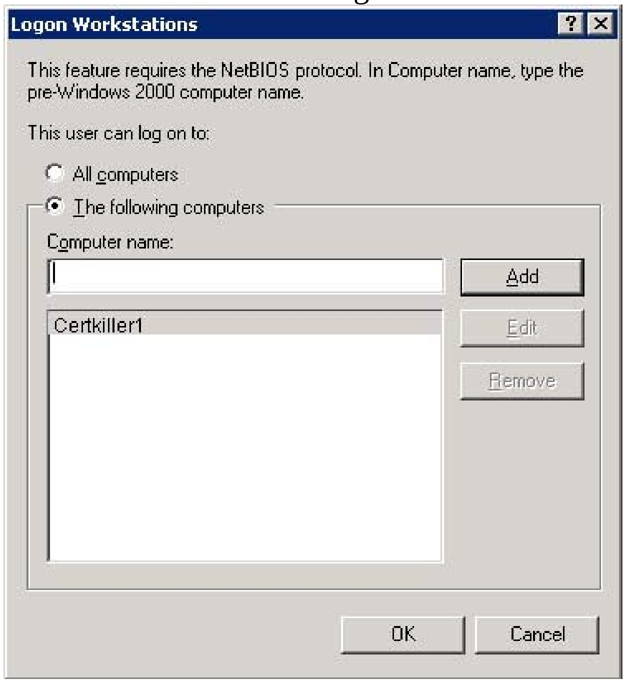
○ All computers

● The following computers

Computer name: Certkiller1

Step #11.

Click OK to close the dialog box.



Logon Workstations

This feature requires the NetBIOS protocol. In Computer name, type the pre-Windows 2000 computer name.

This user can log on to:

○ All computers

● The following computers

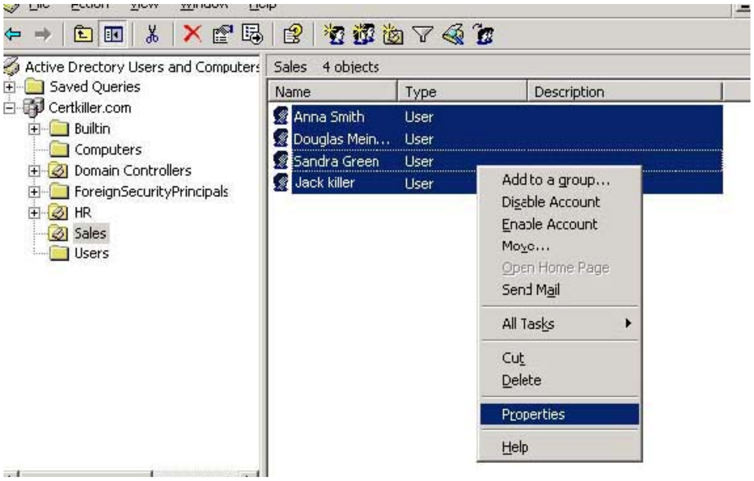
Computer name:

Certkiller1

The second requirement of this question states: Ensure that all employees in the Sales OU have the correct fax number listed in their user accounts.

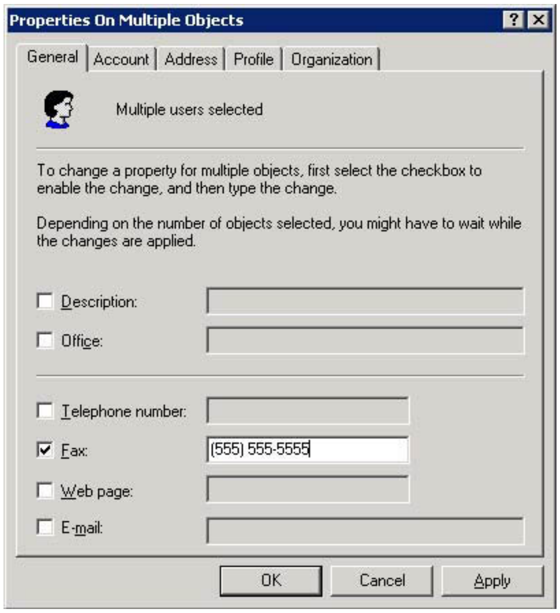
Step #1.

Select all the user accounts in the Sales OU. Right click and select Properties.



Step #2.

Tick the Fax checkbox and enter the fax number, then click OK to close the dialog box.



Properties On Multiple Objects

Multiple users selected

To change a property for multiple objects, first select the checkbox to enable the change, and then type the change.

Depending on the number of objects selected, you might have to wait while the changes are applied.

□ Description:	
□ Office:	
□ Telephone number:	
☑ Fax:	(555) 555-5555
□ Web page:	
□ E-mail:	

QUESTION 689

You are the network administrator for Certkiller .com. You administer a Windows Server 2003 computer named Certkiller 5. Certkiller 5 functions as a file server for Certkiller 's Sales department.

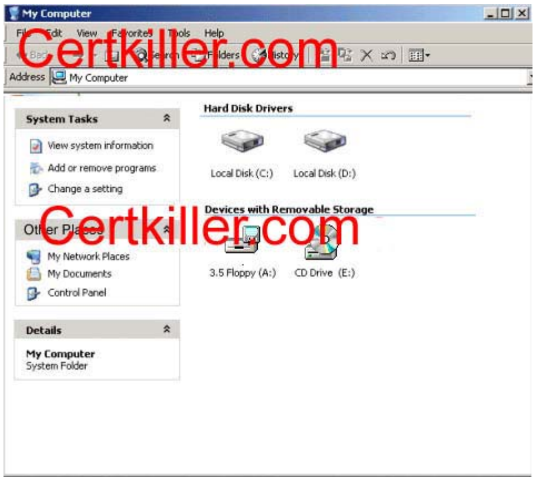
You need to perform the following tasks on Certkiller 5:

- Create a share named Certkiller on the C:\ Certkiller folder.
- On the Certkiller shared folder, configure share permissions so that the SalesGroup group has the Allow-Full Control permission.
- On the Certkiller shared folder, configure share permissions to prevent a member of the SalesGroup named SalesUser from making modifications to any documents in the shared folder without impacting SalesUser's access to other resources. SalesUser must continue to be able to read files in the Certkiller shared folder.

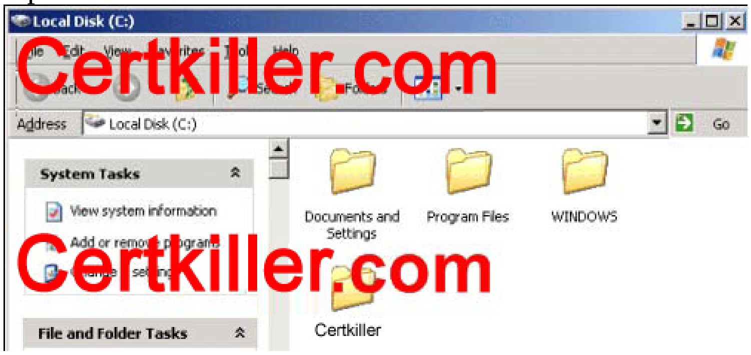
What should you do?

Take the appropriate actions in the simulation window.

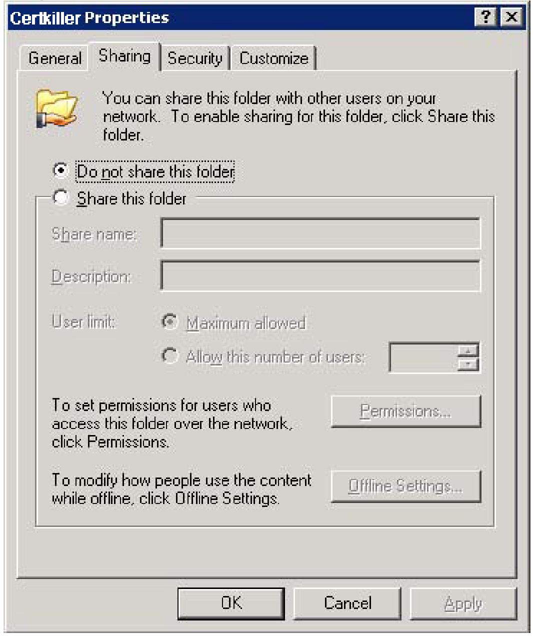
Simulation Window



Answer:
Step #1.
Open the C: disk.



Step #2.
Right-click on the Certkiller folder and select Sharing and Security.



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

● Do not share this folder
○ Share this folder

Share name:

Description:

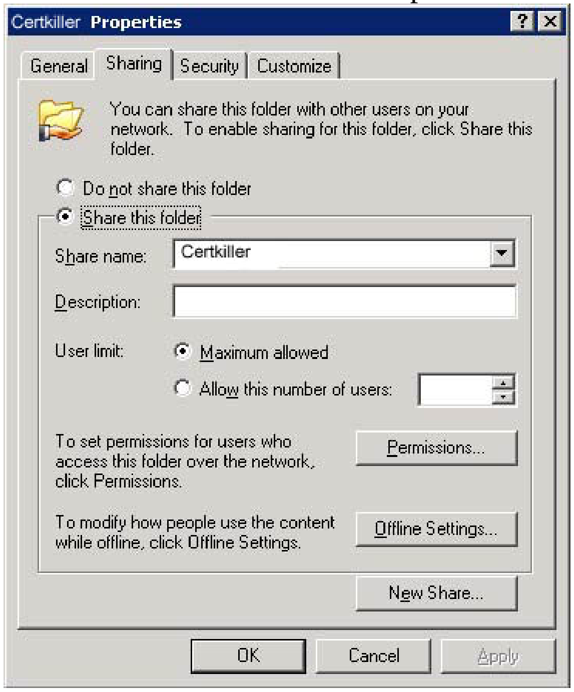
User limit: ● Maximum allowed
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

Step #3.

Select "Share this folder". Accept the default share name and click the Permissions button.



Certkiller Properties

General | Sharing | Security | Customize

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Certkiller

Description:

User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions. [Permissions...]

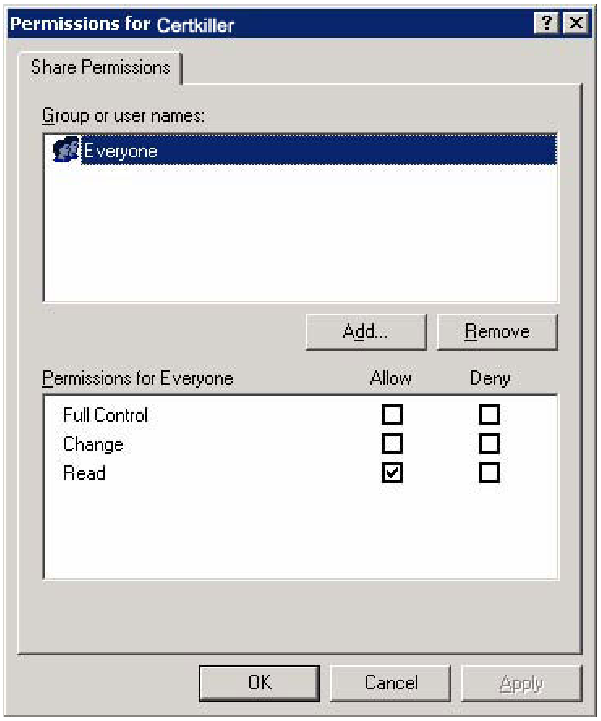
To modify how people use the content while offline, click Offline Settings. [Offline Settings...]

[New Share...]

[OK] [Cancel] [Apply]

Step #4.

Click Add.



Permissions for Certkiller

Share Permissions

Group or user names:

Everyone

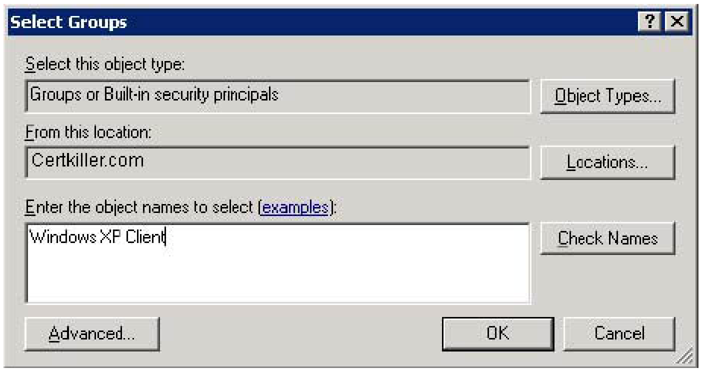
[Add...] [Remove]

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

[OK] [Cancel] [Apply]

Step #5.

Type in SalesGroup and click OK.



Select Groups

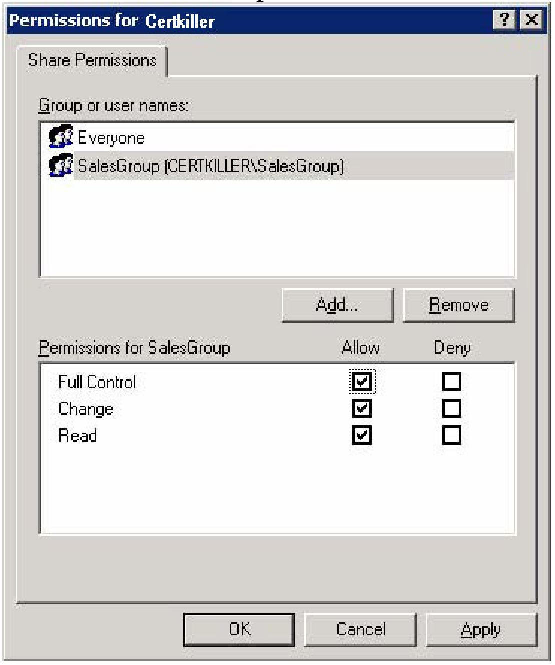
Select this object type:
Groups or Built-in security principals

From this location:
Certkiller.com

Enter the object names to select (examples):
Windows XP Client

Step #6.

Allow Full Control permission for SalesGroup.



Permissions for Certkiller

Share Permissions

Group or user names:

- Everyone
- SalesGroup (CERTKILLER\SalesGroup)

Permissions for SalesGroup	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□