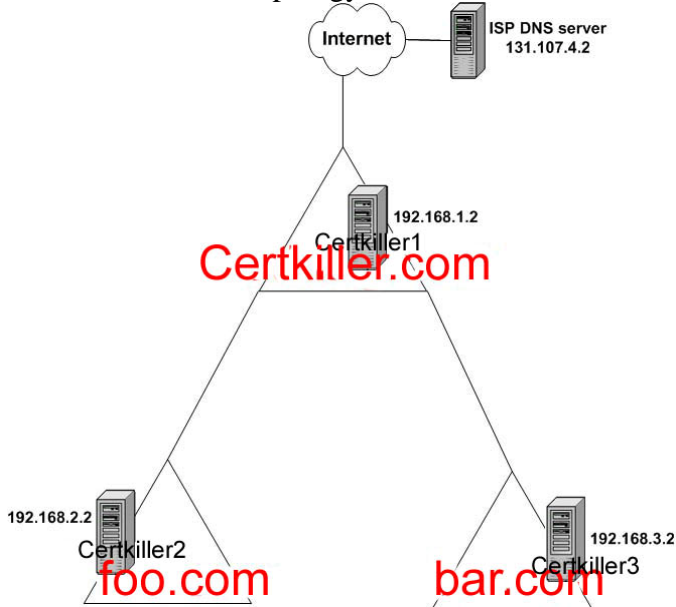**QUESTION** 501
Exhibit, Network Topology

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest named Certkiller .com.
The forest has two additional domain trees named foo.com and bar.com. Servers named Certkiller 1, Certkiller 2, and Certkiller 3 are domain controllers and DNS servers for their respective domains. The relevant portion of the network is shown in the exhibit.
You are using Active-Directory integrated storage of the DNS database. All zones are set to replicate to all the DNS servers in the forest. All references to root servers have been removed from Certkiller 1. Certkiller 3 forwards DNS requests to Certkiller 2. Certkiller 2 forwards DNS requests to Certkiller 1.
You need to ensure that Certkiller 1 can resolve names within Certkiller .com, foo.com, bar.com, and the Internet.
How should you configure DNS forwarding on Certkiller 1?

A. Forward all other DNS requests to 192.168.3.2.
B. Forward all other DNS requests to131.107.4.2.
C. Forward all other DNS requests to 192.168.2.2.
D. Add 192.168.2.2 and 192.168.3.2 to the root hints on Certkiller 1.

Answer: B

Explanation: The Forwarders tab allows you to forward DNS queries received by the local DNS server to upstream DNS servers, called forwarders. Using this tab, you can specify the IP addresses of the upstream forwarders, and you can specify the domain names of queries that should be forwarded.
In addition to the top-level domains on the Internet, organizations can also have a private namespace: a DNS namespace based on a private set of root servers independent of the Internet's DNS namespace. Within a private namespace, you can name and create your own root server or servers and any subdomains as needed. Private names cannot be seen or resolved on the Internet. Since all references to root servers have been removed from Certkiller 1 and Root servers are DNS servers that are authoritative for the root of the namespace. If you want to ensure that Certkiller 1 can resolve names within the given domains as well as the

Internet, then you should configure Certkiller 1 DNS forwarding requests to 131.107.4.2
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. 5:4

QUESTION 502
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain named Certkiller .com. All domain controllers are configured as DNS servers and host
an Active Directory integrated zone for Certkiller .com.
A local ISP provides users with access to the Internet. All Web sites for Certkiller .com are located in the
perimeter network. A secondary DNS zone for Certkiller .com is located on the internal netwkr on a
Windows Server 2003 computer named Certkiller 4. All client computers refer only to this DNS server
for name resolution.
You need to configure DNS resolution to ensure that all client computers can log on to the network,
access the Web sites, and browse the Internet. You must also ensure that the Certkiller .com zone is
stored as securely as possible.
Which two actions should you perform? (Each correct answer presents part of the solution. Select
two.)

A. Configure a secondary DNS zone for Certkiller .com on Certkiller 4.
B. Configure a primary DNS zone for Certkiller .com on Certkiller 4.
C. Configure conditional forwarding for Certkiller .com to point to the IP addresses of the domain
controllers.
D. Configure conditional forwarding for all other DNS domains to point to the IP address of the ISP
DNS server.

Answer: C, D

Explanation: The Forwarders tab allows you to forward DNS queries received by the local DNS server to
upstream DNS servers, called forwarders. Using this tab, you can specify the IP addresses of the upstream
forwarders, and you can specify the domain names of queries that should be forwarded.
Being able to selectively set up different forwarders for different domain names queried, is referred to as
conditional forwarding. At the same time, you are able to enable or disable recursion for each of those
domains separately.
Options C and D suggests configuring conditional forwarding for Certkiller .com to point to the domain IP
addresses anf forwarding for all other DNS domain to point to the ISP's DNS server. This shouls ensure that
the Certkiller .com zone is stored as securely as possible while ensuring that all client computers can log on to
the network, access the Web sites and browse the Internet.
Incorrect answers:
A: Secondary zone is a read-only copy of the zone database used to provide fault tolerance and faster name
resolution across the network. The database is updated via the zone transfer process. This is not goung to
comply with the requirements of the question.
B: Primary zones hold the master copy of the zone database and are replicated to secondary zones. All
changes to the zone are made to the primary zone. This option will not ensure that client computers can
connect to the necessary Web sires, domains and the Internet as is required in this question with the

correct measure of safety for the Certkiller .com zone.
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. 5:4
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, Rockland, 2003, pp. 424, 494

QUESTION 503
Exhibit, network topology
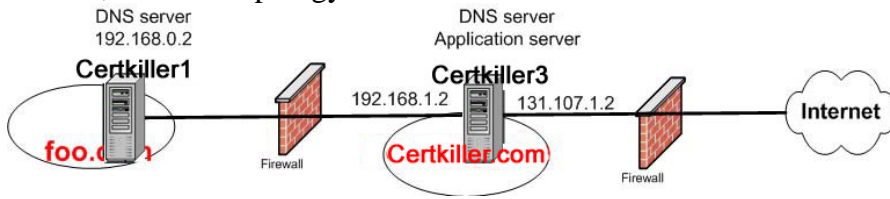
You are the network administrator for Certkiller . The network consists of two DNS domains named
foo.com and Certkiller .com.
foo.com is an intranet domain. A Windows Server 2003 named Certkiller 1 is the DNS server for
foo.com.
Certkiller .com can be publicly accessed from the Internet. A Windows Server 2003 computer named
Certkiller 3 is the DNS server for Certkiller .com.
The relevant partition of the network is shown in the network topology exhibit.
You need to configure name resolution so that the computers that are DNS clients of Certkiller 3 can
resolve names in foo.com and the Internet, and so that the computers that are DNS clients of
Certkiller 1 can resolve names only the foo.com domain.
Which two actions should you perform? Each correct answer presents part of the solution. Select two.

A. Configure Certkiller 1 to forward all requests for Certkiller .com to 192.168.1.2.
B. Configure Certkiller 3 to forward all requests for foo.com to 192.168.0.2
C. Remove all references to root servers on Certkiller 3.
D. Remove all references to root servers on Certkiller 1.

Answer: B, D

Explanation: The Forwarders tab allows you to forward DNS queries received by the local DNS server to
upstream DNS servers, called forwarders. Using this tab, you can specify the IP addresses of the upstream
forwarders, and you can specify the domain names of queries that should be forwarded.
Root servers are DNS servers that are authoritative for the root of the namespace. Thus if you want the
Certkiller 3 DNS clients to resolve names in the foo.com domain and the Internet and that Certkiller 1 DNS
clients can resolve only foo.com domain names, then you should remove all rerefences to root servers on
Certkiller 1 as this would lead to the cache.dns file and you should configure Certkiller 1 to forward all
requests for foo.com to 192.168.0.2
Incorrect answers:
A: It is Certkiller 1 and not Certkiller 3 that should be reconfigured appropriately.
C: Thereis no need to remove the references to root servers on Certkiller 3 in this case.

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. 5:4

QUESTION 504
Exhibit, Network Topology ** MISSING ***
You are the network administrator for Certkiller .com. The network consists of two Active Directory
forests. Each forest contains a single domain. The domain names are Certkiller .com and foo.com. All
servers run Windows Server 2003.
The domain controllers in each domain are configured as DNS servers. The DNS servers are
configured to forward all requests for host names on the Internet to a DNS server located at the
company's ISP. The relevant portion of the network is shown in the exhibit.
Users in the Certkiller .com domain report that they cannot connect to the intranet Web sites in the
foo.com domain. When they try to connect to the Web sites, they receive the following error message:
"Cannot find server or DNS error." Users in the foo.com domain can connect to the intranet Web
sites in the foo.com domain.
You need to ensure that users in the Certkiller .com domain can connect to intranet Web sites in the
foo.com domain. You want to accomplish this goal by making the minimum amount of changes to the
current network configuration.
What should you do?

A. On the DNS servers in the Certkiller .com domain, configure a conditional forwarder to one of the
DNS servers in the foo.com domain.
B. On the DNS servers in the foo.com domain, configure a conditional forwarder to one of the DNS
servers in the Certkiller .com domain.
C. On the DNS servers in the Certkiller .com domain, remove the forwarder configuration. Configure the
DNS servers to use root hints.
D. On the DNS servers in the Certkiller .com domain, change the forwarder configuration so that all
requests for host names are forwarded to the DNS servers in the foo.com domain.
E. On the DNS servers in the foo.com domain, configure a stub zone for the Certkiller .com domain.

Answer: A

Explanation: The Forwarders tab allows you to forward DNS queries received by the local DNS server to
upstream DNS servers, called forwarders. Using this tab, you can specify the IP addresses of the upstream
forwarders, and you can specify the domain names of queries that should be forwarded. When, after
receiving and forwarding a query from an internal client, the local forwarding server receives a query
response back, the local forwarding server then passes this query response back to the original querying
client. The process of forwarding selected queries in this way is known as conditional forwarding.
Conditional forwarding will ensure that the Certkiller .com users can connect to intranet Web sites in the
foo.com domain.
Incorrect answers:
B: The conditional forwarders should be configured on the Certkiller .com domain and not the foo.com
domain.
C: Making use of root hints after removing the forwarder configuration is not going to ensure that

Certkiller .com users will be able to connect to the Intranet Web sites in the foo.com domain.
D: There is no need to change the forwarder configuration.
E: Configuring a stub zone will not have the desired effect in this case.
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. 5:4

QUESTION 505
You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest. The forest contains two domains named Certkiller .com and corp. Certkiller .com. All zones are configured to replicate to all DNS servers in the forest.
The DNS servers are described in the following table.

Server name	Server roles	Zones hosted	Zone type	Active Directory Site
Certkiller 1. Certkiller .com	Domain controller, DNS server	Certkiller .com corp. Certkiller .com	Active Directory-integrated primary	MainOffice
Certkiller 2. Certkiller .com	DNS server	Certkiller .com, corp. Certkiller .com	Secondary	BranchOffice
Certkiller 3.corp. Certkiller .com	Domain controller	None	Not applicable	MainOffice
Certkiller 4.corp. Certkiller .com	Domain controller, DNS server	corp. Certkiller .com	Active Directory-integrated primary	BranchOffice

The properties sheet of the start of authority (SOA) resource record for the zone is shown in the exhibit.

You remove Certkiller 2 from the network for hardware maintenance. Two days later, you bring Certkiller 2 back on the network.

You need to ensure that the DNS zone information for corp. Certkiller .com is immediately updated on Certkiller 2.

What should you do?

A. Use NTDS setting on Certkiller 1 to initiate replication between the MainOffice site and the BranchOffice site.

B. Use NTDS settings on Certkiller 4 to initiate replication between the MainOffice site and the BranchOffice site.

C. Use the DNS console on Certkiller 1 to increment the serial number for corp. Certkiller .com

D. Use the DNS console on Certkiller 2 to initiate a zone transfer from the master server for corp. Certkiller .com.

E. Use the DNS console on Certkiller 2 to reload corp. Certkiller .com

Answer: D

Explanation: Active Directory integrated zone transfers; accomplished via Active Directory replication, is a push transfer, initiated by the domain controller hosting the primary DNS server function. When changes to the database occur, the domain controller sends updates to other domain controllers. This allows the changes to be updated more quickly and more efficiently. DNS servers do not need to check for updates constantly since updates will be received as changes are made on the primary DNS server. A secondary zone is a copy

of the zone that is copied from the master server when replication of the zone takes place through zone transfer. Secondary DNS servers obtain their zone databases through zone transfers. To ensure that DNS zone information for corp. Certkiller .com is immediately updated on Certkiller 2, use the DNS console on Certkiller 2 to initiate a zone transfer from the master server for corp. Certkiller .com. A secondary server typically initiates a zone transfers when the secondary server boots or the refresh interval for the zone expires.

Incorrect Answers:

A, B: Initiating replication through the NTDS setting does not necessarily mean immediate updating. Taking the zone types of the servers into account, the best way to ensure that the DNS zone information for corp. Certkiller .com is immediately updated on Certkiller 2 is to initiate a zone transfer.

C: Incrementing the serial number for corp. Certkiller .com on the DNS console on Certkiller 1 will not ensure immediate updates of the DNS zone information of corp. Certkiller .com on Certkiller 2.

E: Reloading corp. Certkiller .com using the DNS console on Certkiller 2 will not work in this scenario.

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. 435

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 5, pp 274-279.

QUESTION 506

You are the network administrator for Certkiller .com. The network contains Windows NT Server 4.0 computers, Windows Server 2003 computers, Windows NT Workstation 4.0 computers, and Windows XP Professional computers.

The Certkiller .com DNS namespace is used on the company's intranet. The Certkiller .com DNS zone is hosted on a Windows Server 2003 computer and is configured to allow secure dynamic updates. All Windows Server 2003 computers and Windows XP Professional computers are configured to dynamically register their host names in the Certkiller .com DNS zone.

The Windows NT Server computers and Windows NT Workstation computers use WINS and DNS for name resolution. Host (A) records for the Windows NT Server computers have not been created in the Certkiller .com DNS zone. The Windows Server 2003 computers and Windows XP Professional computers cannot connect to the Windows NT Server computers when using computer names.

You need to implement a mechanism that allows the Windows Server 2003 and Windows XP Professional computers to resolve the computer names of the Windows NT Server computers. To reduce administrative overhead, you must choose a solution that will not need to be configured when the IP address of any computer is changed.

What should you do?

A. Configure WINS reverse lookup on the DNS zones.
B. Configure WINS forward lookup on the DNS zones.
C. Configure nonsecure and secure updates in the DNS zone Certkiller .com.
D. Install the Active Directory Client Extensions on the Windows NT Server computers.

Answer: B

Explanation: The WINS and DNS services are used to provide name resolution for the NetBIOS namespace and the DNS domain namespace, respectively. Although both DNS and WINS can provide a separate and useful name service to clients, WINS is mainly needed to provide support for older clients and programs that require support for NetBIOS naming. However, the DNS service can work with WINS to provide combined name searches in both namespaces when resolving a DNS domain name not found in zone information. To provide this interoperability, a new record (the WINS record) is defined as part of the zone database file.

The WINS resource record is specific to computers running Windows NT 4.0 and earlier, Windows 2000, and Windows Server 2003 operating systems, and can be attached only to the domain of origin for a zone. The presence of a WINS resource record can instruct the DNS service to use WINS to look up any forward queries for host names or names that are not found in the zone database. This functionality is particularly useful for name resolution required by clients that are not WINS-aware (for example, UNIX) for the names of computers not registered with DNS, such as Windows 95 or Windows 98 computers.

Incorrect Answers:

A: Configuring WINS forward lookup for your DNS implementation is zone independent. It is the WINS forward lookup that had to be configured on the DNS zones and not the reverse lookup.

C: Configuring secure and non-secure updates in the DNS zone Certkiller .com will not allow Windows NT Server access.

D: Installing Active Directory Client Extensions on the Windows NT server computers will not allow computer names to be resolved.

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. 363

QUESTION 507

You are the network administrator for Certkiller . The company's main office is located in Lima, and branch offices are located in five other cities. The network consists of a single DNS domain named Certkiller .com. The network configuration is shown in the exhibit.
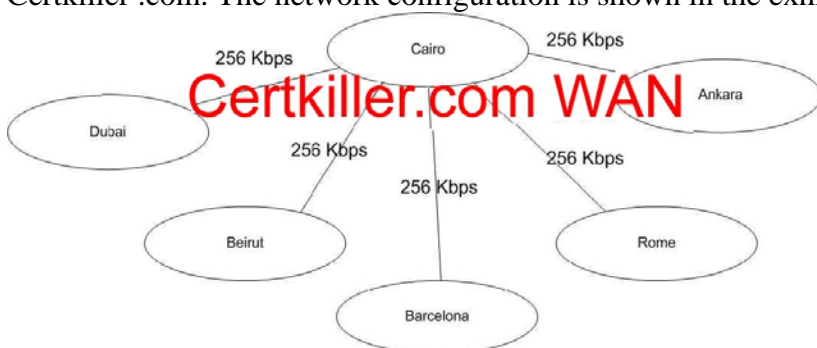
All network servers run Windows Server 2003. All client computer IP addresses are assigned by using a DHCP server that is located in each office. Client computers are reimaged often and are assigned new names each time they are reimaged. All client computers are configured to reference their local DNS server as the preferred DNS server and to reference the central DNS server as the alternate DNS server.

A primary zone for Certkiller .com is configured on a server in the Lima office. Secondary zones are configured on a server in each branch office. The retry interval, the refresh interval, the expiration

interval, and the default minimum Time to Live (TTL) interval are configured with the default settings.

Network bandwidth utilization averages 40 percent. The network connection between the Lima office and the Bogota office fails on average of twice per day.

Users in the Bogota office occasionally receive incorrect responses to queries against the local DNS server when the network connection is interrupted during a zone transfer.

You need to change the configuration of the start of authority (SOA) resource record for Certkiller .com. In addition, you need to reduce the possibility that users can query local DNS zones before successful zone transfers occur.

What should you do?

A. Change the retry interval to 12 hours.
B. Change the default minimum Time to Live (TTL) to 2 days.
C. Change the refresh interval to 2 days.
D. Change the expiration interval to 12 hours.

Answer: D

Explanation: Expiration interval is the time, in seconds, before a secondary server stops responding to queries after a lapsed refresh interval where the zone was not refreshed or updated. Expiration occurs because at this point in time, the secondary server must consider its local data unreliable. The default value is 86,400 seconds (24 hours). Reducing the expiration interval will thus reduce the possibility of users querying the local DNS zones before a successful zone transfer occurs.
Incorrect Answers:
A: Retry interval is the time, in seconds, that a secondary server waits before retrying a failed zone transfer. This is not the value that has to be changed.
B: Minimum (default) TTL is the minimum Time-To-Live (TTL) value applied to all resource records in the zone with unspecified record-specific TTLs. This value is supplied in query responses by servers for the zone to inform others how long they should cache a resource record provided in an answer. However, it is the Expiration interval that should be changed.
C: Refresh interval is the time, in seconds, that a secondary DNS server waits before querying its source for the zone to attempt renewal of the zone. When the refresh interval expires, the secondary DNS server requests a copy of the current SOA record for the zone from its source, which answers this request. The secondary DNS server then compares the serial number of the source server's current SOA record (as indicated in the response) with the serial number in its own local SOA record. If they are different, the secondary DNS server requests a zone transfer from the primary DNS server. But you need to change the expiration interval to be able to reduce the possibility of users querying the local DNS zones before successful zone transfers can occur.
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. 28, 204

QUESTION 508
You are the network administrator for Certkiller .com. The network consists of an Active Directory forest with two domains named Certkiller .com and europe. Certkiller .com. Both domains contain

Windows Server 2003 domain controllers and Windows 2000 Server domain controllers.
DNS is installed on all domain controllers. No other computers function as DNS servers. The DNS
zones Certkiller .com and europe. Certkiller .com are Active Directory-integrated zones.
Certkiller 's Web administrator asks you to create a new, separate DNS zone that will be used to
register host names for intranet Web sites. This zone must be replicated to all DNS servers in the
company. The new zone must be named intranet. Certkiller .com.
You must create and configure the intranet. Certkiller .com zone to fulfil these requirements.
What should you do?

A. Set up and Active Directory-integrated zone on one Windows Server 2003 domain controller in the
Certkiller .com domain.
Choose the replication scope To all domain controllers in the Active Directory domain
Certkiller .com.
B. Set up an Active Directory-integrated zone on one Windows Server 2003 domain controller in the
Certkiller .com domain.
Choose the replication scope To all DNS servers in the Active Directory domain Certkiller .com.
C. Create an Active Directory application partition named intranet. Certkiller .com.
Set up an Active Directory-integrated zone on one Windows Server 2003 domain controller in the
Certkiller .com domain.
Specify the intranet. Certkiller .com application partition as the replication scope of the zone.
D. Set up and Active Directory-integrated zone on one Windows Server 2003 domain controller in the
Certkiller .com domain.
Choose the replication scope To all DNS servers in the Active Directory forest Certkiller .com.
Set up a secondary zone on all Windows 2000 domain controllers in the forest.

Answer: D

Explanation: Active Directory integrated zone data is stored as an Active Directory object and is replicated
as part of domain replication.
This provides the following advantages: No single point of failure, Fault tolerance, Single replication
topology and Secure dynamic.
Incorrect Answers:
A: The replication scope, To all domain controllers in the Active Directory domain Certkiller .com, is the
wrong option.
B: This option is correct but you also need a secondary zone on all the domain controllers in the forest to be
able to fulfill all the requirement.
C: There is no need to create an Active Directory application partition and have that partition be specified
as the replication scope.
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. 480

QUESTION 509
You are the administrator of the Certkiller .com company network. The network consists of a single
Active Directory domain named Certkiller .com. The network includes 15 servers running Windows

Server 2003 and 300 client computers running Windows XP Professional.
A domain controller named Certkiller SrvA is the primary DNS server for the Certkiller .com domain.
The company opens a new branch office. The new office network will be a subdomain of
Certkiller .com. The domain will be named east. Certkiller .com. You install a domain controller named
Certkiller SrvB in the branch office. Certkiller SrvB hosts the DNS zone for east. Certkiller .com.
You need to ensure that computers in Certkiller .com can resolve host names in east. Certkiller .com on
Certkiller SrvB.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution.
Choose two)

A. Use dnsmgmt.msc to add a start-of-authority (SOA) record to Certkiller SrvA that refers to
Certkiller SrvB.east. Certkiller .com.
B. Use dnsmgmt.msc to add a new delegation on Certkiller SrvA for east. Certkiller .com to Certkiller SrvB.
C. Use dnsmgmt.msc to add a new stub zone to Certkiller SrvA named east. Certkiller .com.
D. Use dnsmgmt.msc to add a service locator (SRV) record to Certkiller SrvA that refers to
Certkiller SrvB.east. Certkiller .com.

Answer: B, C

Explanation: A delegation or a stub zone will enable Certkiller SrvA to forward resolution requests for
east. Certkiller .com to Certkiller SrvB.
Stub zone is a partial copy of a zone that can be hosted by a DNS server and used to resolve recursive or
iterative queries. Stub zones contain the Start of Authority (SOA) resource records of the zone - the DNS
resource records that list the zone's authoritative servers; and the glue A (address) resource records that are
required for contacting the zone's authoritative servers.
Delegation is the process of distributing responsibility for domain names between different DNS servers in
the network. For each domain name delegated, you have to create at least one zone. The more domains you
delegate, the more zones you need to create.
Incorrect Answers:
A: The SOA record must exist in the delegated zone.
D: You need NS records to point to Certkiller SrvB, and not SRV records.
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. 426, 528

QUESTION 510
You are the Network Administrator for Certkiller .com. The network consists of a single Windows
Server 2003 DNS zone named Certkiller .com. The network topology is shown in the exhibit.
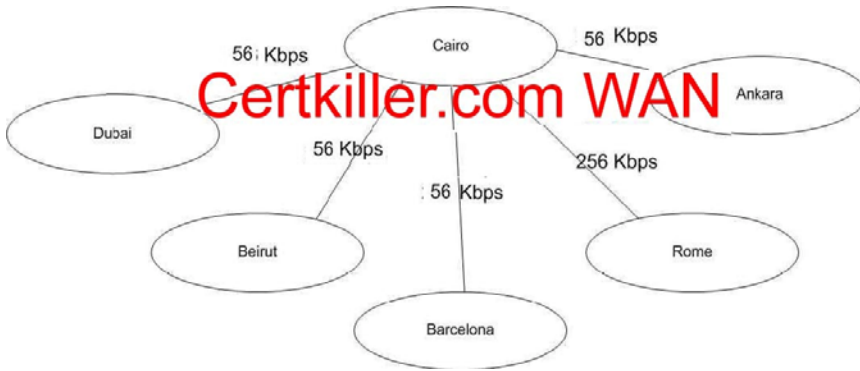
All network servers run Windows Server 2003. All IP Addresses are statically aasigned. The primary DNS zone for Certkiller .com is hosted in a server at the company's main office in Cairo secondary zones for Certkiller .com are hosted on servers in the branch offices.

Another administrator reports that network utilization is at 90% of company. You reconfigure the refresh interval and the minimum default. Time To Live (TTL) intervals for the Certkiller .com zone, as shown in the following table.

Refresh interval   3 hours
Minimum default Time To Live(TTL)   1 day

You need to configure the start of authority (SOA) resource record properties for the Certkiller .com zone. You also need to ensure that the server in the Cairo office will continue to attempt zone transfers if an initial attempt fails.
What should you do?

A. Configure the Certkiller .com zone to expire after 1 hour
B. Configure the Certkiller .com zone to expire after 4 hours.
C. Configure the Certkiller .com zone to expire after 20 seconds.
D. Configure the retry interval to be 1 hour.
E. Configure the retry interval to be 4 hours.
F. Configure the retry interval to be 20 seconds.

Answer: D

Explanation: One can configure the refresh interval between updates from a secondary DNS server. The refresh interval should be tuned accordingly to avoid wasting bandwidth, and to ensure that the content on the secondary server is constantly accurate. If DNS record changes occur infrequently, increase the default value. If DNS record changes occur often, decrease the default value.
A retry interval is where a secondary DNS server may be unable to refresh data from the primary server because of a connection or service failure. The secondary DNS server attempts to refresh data once the interval specified for retrying lapses.
Thus it would be logical that the retry interval should be less than the refresh interval.
Incorrect Answers:
A: After the interval specified for expiry, the secondary server stops serving name requests. Therefore, the zone expiry interval has no effect on the bandwidth used by zone transfers.
B: After the interval specified for expiry, the secondary server stops serving name requests. Therefore, the zone expiry interval has no effect on the bandwidth used by zone transfers.
C: After the interval specified for expiry, the secondary server stops serving name requests. Therefore, the zone expiry interval has no effect on the bandwidth used by zone transfers.

E: The Retry interval should be less than refresh interval. In this question, the refresh interval is set to 3 hours.
F: This value is too low.
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. 506

QUESTION 511
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain DNS servers are configured as shown in the following table.

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

You uninstall DNS from Certkiller 2 and reconfigure Certkiller 2 as a file server. Then you reconfigure Certkiller 4 as a caching-only server. Next, you reconfigure the domain controllers to use Active Directory-integrated DNS zones.
You need to eliminate unnecessary zone transfer activity on the network.
What should you change in the Notify dialog box?
To answer, select the setting or settings that need to be changed. Select the IP address of addresses that need to be removed from the list.
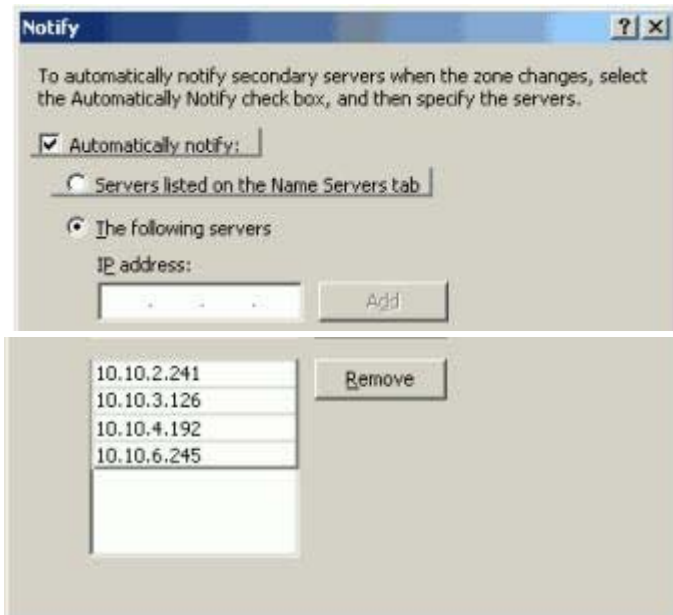
Answer: Remove all the IP addresses

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

Note: You may need to clear the Automatically notify box because notification is no longer required. Zone transfers are no longer performed when all the servers are Active Directory Integrated zones. Zone transfer is then included in Active Directory replication.
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. 28, 204

QUESTION 512
You are a network administrator for Certkiller . All servers run Windows Server 2003. The DNS domain structure is configured as shown in the following diagram.
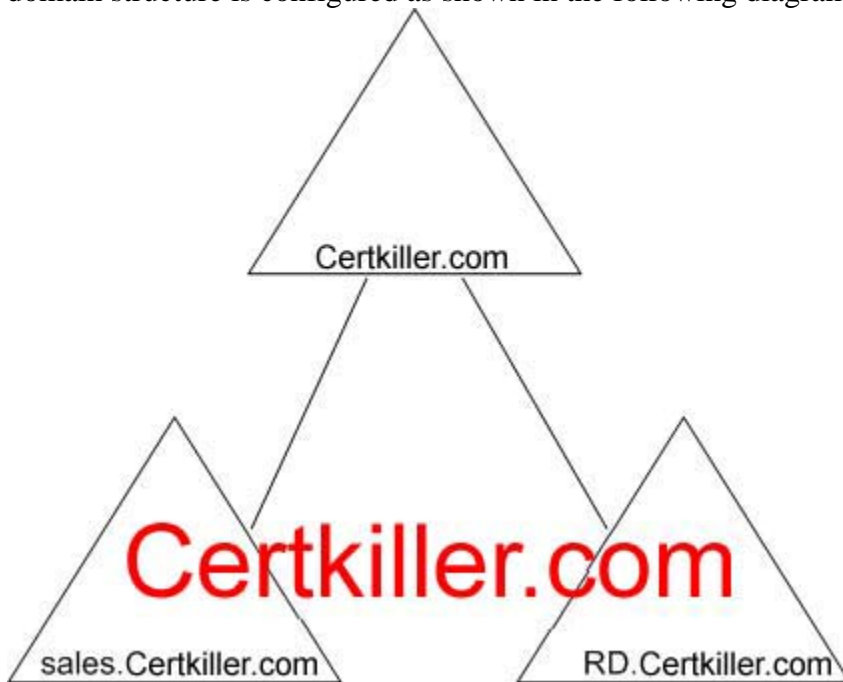
The network administrator for the RD. Certkiller .com domain maintains separate DNS servers that are authoritative for that domain. You create a delegation entry the Certkiller .com domain for the RD. Certkiller .com domain.
The network administrator for the RD. Certkiller .com domain maintains separate DNS servers that are authoritative for that domain. You create a delegation entry in the Certkiller .com domain for the RD. Certkiller .com domain.
The network administrator for the RD. Certkiller .com domain will use the new DNS servers when they are added.
What should you do?

A. Delete the delegation entry. Create a stub zone for the RD. Certkiller .com domain.
B. Delete the delegation entry. Add a conditional forwarding entry for the RD. Certkiller .com domain.
C. In the Certkiller .com domain, disable recursion on the DNS servers.
D. In the Certkiller .com domain, create a new root hint that includes the DNS servers in the RD. Certkiller .com domain.

Answer: A

Explanation: Delegation and glue records are records added to the zone to delegate a subdomain into a separate zone. A stub zone contains only the resource records needed to identify the authoritative DNS servers for the zone. The stub zone is used to keep a parent zone up-to-date as to the authoritative DNS servers for a child zone. Stub zones are unique and contain a small subset of typical zone data. Thus a stub zone contains only the SOA, NS, and glue records for the zone.This helps the parent domain remain up-todate with regard to the authority of delegated zones.The delegation record is a Name Space (NS) record in the parent zone that lists the parent zone as authoritative for the delegated zone.The glue record is an A type record (A RR) for the DNS server authoritative for the delegated zone.

Option A will thus be the way forward.

Incorrect answers:

B: Deleting the delegation entry will be correct under the circumstances, but then you should not add a conditional forwarder fpor the RD. Certkiller .com domain since the network administrator will be using the new DNS servers.

C: Recursion: If you select to check the Do not use recursion for this domain option check box, you are in essence telling the server to not try any other means of name resolution if it cannot resolve a query using its list of forwarders. This is not desired.

D: The root hints file (cache hints file) contains host information needed to resolve names external of the authoritative DNS domains. It holds names and addresses of root DNS servers which are normally located on the Internet. Creating new root hints that includes the DNS servers in the RD. Certkiller .com domain will thus not be advisable in the 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, Rockland, 2003, pp. 424. 431

QUESTION 513

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The network topology is shown in the exhibit.

The configurations of the DNS servers that host the stone named Certkiller .com are shown in the following table.

Server	*Zone type*	*Server role*	*Location*
Certkiller 1	Active Directory-integrated	Domain controller	New York
Certkiller 2	Active Directory-integrated	Domain controller	Chicago

4.   Certkiller 3   4.   Secondary   4.   Member server   4.   Caracas

The refresh interval for the zone is one hour. The zone contains 10,000 records.
The network connection to Caracas is operating at 90 percent of capacity.
You remove Certkiller 3 from the network to perform hardware maintenance. Two hours later, you
bring Certkiller 3 back on the network.
You need to ensure that Certkiller 3 can immediately provide accurate responses to client computer
requests for data. You also need to ensure that no unnecessary traffic is generated by the DNS servers.
What should you do on Certkiller 3?

A. Transfer the zone from the master server.
B. Reload the zone from the master server.
C. Update server data files.
D. Scavenge stale resource records.

Answer: A

Explanation: A DNS zone transfer is the process by which the zone's resource records are copied, or
replicated, to other DNS servers. The resource records in the zone are stored in a database that is copied at
specified intervals to other DNS servers to ensure reliable host name resolution. Thus transferring the zone
from the master server will have the desired effect.
Incorrect answers:
B: Reloading the zone is not going to make sure that unnecessary traffic is not generated by the DNS
servers.
C: Updating server data files is not going to ensure that unnecessary trasffic is generated on the DNS
servers. It is irrelevant in this case.
D: Be careful when enabling DNS scavenging and understand that it is disabled by default for a reason. If it
is set up incorrectly, vital DNS resource records could be deleted accidentally, causing more problems
than an abundance of stale records. Scavenging stale resource records is not advised in this case.
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, Rockland, 2003, pp. 434, 501

QUESTION 514
Exhibit

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 Certkiller .com zone is configured as shown in the exhibit.

Certkiller 1 also hosts a DNS zone named Certkiller .internal. The domain controllers are configured as shown in the following table.

Domain controller	Services and applications installed
Certkiller 1	DNS, WINS
Certkiller 2	DNS, DHCP
Certkiller 3	WINS

You create a global group named Certkiller DNS.

You need to be able to assign the Certkiller DNS global group necessary permissions to create and delete the child entries in the Certkiller .com zone.

What should you do first?

A. Change the Certkiller .internal zone to an Active Directory-integrated primary zone.
B. Change the Certkiller .internal zone to an Active Directory-integrated stub zone.
C. Change the Certkiller .com zone to an Active Directory-integrated primary zone.
D. Change the Certkiller .com zone to an Active Directory-integrated stub zone.

Answer: C

Explanation: An Active Directory Integrated zone is a zone where zone information held in the Windows Active Directory and replicated using Active Directory replication, providing greater flexibility in the replication process. Only primary DNS zones can be stored in the Active Directory. Secondary zones must

be stored in the old standard text format. This might seem odd at first, but secondary DNS zones are essentially obsolete in light of the multi-master replication model of the Active Directory-integrated DNS zone. Secondary zones might still be needed if some zones will not be stored in the Active Directory, or will be maintained during the migration period. In the light of the above, changing the Certkiller .com zone to an Active Directory Integrated primary zone would enable you to assign the Certkiller DNS global group the needed permissions to create and delte child entried on the Certkiller .com zone.
Incorrect answers:
A: You should rather be changing the Certkiller .com zone and not the tesetking.internal zone. As this option suggests, it would not enable you to assign the correct permissions to the Certkiller DNS global group.
B: A stub zone is not authoritative for the zones they copy. You would thus not be able to assign the correct permissions.
D: This is the wrong zone type to be changing the Certkiller .com zone into.
Reference:
Michael Cross and Jeffery
A. Martin, MCSE Exam 70-294: Planning, Implementing, and Maintaining a
Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, 2003, p. 368

QUESTION 515
You are the network administrator for the Oslo branch office of Certkiller .
The Oslo office has a Windows Server 2003 DNS server named Certkiller 3. Certkiller 3 hosts a DNS primary zone named Certkiller .com. All computers in the Oslo office are configured to use Certkiller 3 as their preferred DNS server.
The Budapest branch office of Certkiller has a UNIX DNS server named Certkiller 4. Certkiller 4 hosts a primary zone named engineering. Certkiller .com. The refresh interval of the engineering. Certkiller .com zone is set to 24 hours.
In the Budapest office, a firewall filters all incoming network traffic from other offices. A rule on this firewall prevents all computers from the Oslo office network, except Certkiller 3, from performing DNS lookups against Certkiller 4.
There is a business requirement that no delay should occur between the time that a new record is created in the engineering. Certkiller .com zone and the time that the record can be resolved from any computers in the Oslo office. All computers in the Oslo office must be able to resolve names in the enginnering. Certkiller .com namespace.
You need to configure DNS on Certkiller 3 to meet the requirements.
What should you do?

A. Set up a stub zone named engineering. Certkiller .com.
B. Set up conditional forwarding to Certkiller 4 for the engineering. Certkiller .com namespace.
C. In the Certkiller .com zone, set up a delegation to the engineering. Certkiller .com zone on Certkiller 4.
D. Set up a secondary zone named engineering. Certkiller .com that has Certkiller 4 as its master.

Answer: B

Explanation: With Windows Server 2003 you can through conditional forwarding, configure forwarding on Certkiller 3 to Certkiller 4 for the engineering. Certkiller .com namespace. DNS forwarders can be set up for

different domains for forwarding name resolution requests.
Incorrect Answers:
A: A stub zone maintains only a list of authoritative name servers for a particular zone. The purpose of a stub zone is to ensure that DNS servers hosting a parent zone are aware of authoritative DNS servers for its child zones. Setting up a stub zone would thus not work in this scenario.
C: Delegation is the ability of an administrator to distribute certain administrative tasks to other individuals or groups. In terms of DNS, a portion of a domain namespace can be delegated to another server that will then be responsible for resolving name-resolution requests. However, what is needed in this case is conditional forwarding.
D: Secondary zones are zone types that stores a copy of an existing zone in a read-only text file. To create a secondary zone, the primary zone must already exist, and you must specify a master name server. This is the server from which the zone information is copied. Thus this option will not meet the stated requirements.
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 5, p. 246

QUESTION 516
You are the administrator of the Certkiller .com company network. The network consists of a single Active Directory domain named Certkiller .com. The network includes 10 member servers running Windows Server 2003, 4 domain controllers running Windows Server 2003 and 150 client computers running Windows XP Professional.
The domain controllers are also configured as DNS servers.
You configure a new UNIX server to act as a secondary DNS server that is authoritative for the DNS zone. You create a host (A) record for the UNIX server in the DNS zone. You configure the DNS zone to allow zone transfers to all servers.
You need to configure the DNS zone to accommodate the new UNIX server.
What should you do?

A. Use dnsmgmt.msc to add a name server (NS) resource record for the UNIX server to the DNS zone.
B. Use dnsmgmt.msc to add the UNIX server to the start of authority (SOA) resource record for the DNS zone.
C. Use dnsmgmt.msc to add a service locator (SRV) resource record that includes the UNIX server as a host.
D. Use dnsmgmt.msc to add a LDAP service locator (SRV) resource record that includes the UNIX server as a host.
E. Use dnsmgmt.msc to add an alias (CNAME) record that includes the UNIX server as a host

Answer: A

Explanation: When adding DNS servers to the domain, you must add name server (NS) resource record to the zone.
A name server (NS) resource record is used to map a DNS domain name as specified in owner, to the name of hosts operating DNS servers specified in the name_server_domain_name field.
Incorrect Answers:

B: Adding to the DNS zone is proper, though not adding the UNIX server to the start of authority resource record.

C: You should not be adding a service locator resource record is this will not allow zone transfers to the UNIX server.

D: If the client and server configurations do not match in this case, the client will receive an LDAP BIND request failed and the client will be unable to connect to the server. Thus adding a LDAP service locator resource record will not accommodate the new UNIX server.

E: The UNIX server as host should not be included and you should not be adding an alias record.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp 594-5, 786

QUESTION 517

You are the network administrator for Certkiller .com. The network consists of a DNS domain named Certkiller .com.

A Windows Server 2003 computer named Server CK1 is the primary DNS server for Certkiller .com.

The network also contains a UNIX server named Server CK2 .

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

MISSING

A user named Anne uses a Windows XP Professional computer named Client CK1 . Anne reports that Client CK1 can ping Server CK2 by its IP address but not by its name. Client CK1 can successfully connect to Server CK1 . Other hosts on the same subnet as Client CK1 exhibit the same behaviour. You need to ensure that all client computers can connect to Server CK2 by its name. You need to minimize administrative effort.

What should you do?

A. Add an alias (CNAME) record to 192.168.1.2 that references Server CK2 .

B. Add a host (A) record to 192.168.1.2 that references Server CK2 .

C. Add a reference to Server CK2 in the Hosts file of each client computer in the network.

D. Add a reference to Server CK2 in the Lmhosts file of each client computer in the network.

Answer: B

Explanation: A Host Address Record (A) also referred to as a Host Record, associates a host name to its IP address. It is a record used to map machine or resource host names to IP addresses.

Incorrect Answers:

A: A canonical name serves as an alias when you want to hide your network details from the clients that connect to it. This is not what is required.

C, D: The Hosts file provides host name resolution on an IP-based network, while LMHosts is used for NetBIOS name resolution. This option should also work, but both cases involve more administrative effort than option B.

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. 427-428, 874

QUESTION 518
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Client computers run either Windows XP Professional or Windows 2000 Professional. The network includes a single DNS server. The DNS server hosts the Certkiller .com zone.
You are deploying an intranet site that will be accessed by all company users. The site will be heavily utilized. You deploy three Web servers named Web1, Web2, and Web3 to host the site. All users must be able to access the intranet site by using intranet. Certkiller .com as the address.
You need to ensure that the three Web servers are equally utilized.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Create a host (A) resource record named intranet. Certkiller .com.
B. Configure a host (A) resource record for each of the three Web servers.
C. Create an alias (CNAME) resource record for each of the three Web servers.
Configure each record to refer to Certkiller .com.
D. Configure three alias (CNAME) resource records for intranet. Certkiller .com.
Configure each record to refer to one of the Web server host (A) resource records.

Answer: B, D

Explanation: You have to configure a host (A) resource record for each of the three Web servers. This record will be used to associate the hostname to a specific IP address. Domains use DNS alias records so that they can use more than one name to point to a single host. Therefore, to ensure that users can access the intranet site by using intranet. Certkiller .com as the address, you have to set up three alias (CNAME) resource records for intranet. Certkiller .com and enable each one to refer to one of the Web server host (A) resource records.
Incorrect Answers:
A: The host (A) resource record has to be created for the intranet. Certkiller .com only and not on all three Web servers. You only need to refer to one of the Web server host (A) resource records.
C: The Canonical Name (CNAME) resource record is used to create aliases that hide your network details from the clients that connect to it. In this scenario you need to create aliases for intranet. Certkiller .com and not for the three Web servers.
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 4, pp. 205 - 210, 428

QUESTION 519
You are the Network Administrator for Certkiller .com. The network consists of two Active Directory domains named corp. Certkiller .com and engineering. Certkiller .com. DNS zones named corp. Certkiller .com and engineering. Certkiller .com have been created on the internal DNS servers. The company also uses a separated DNS zone named Certkiller .com to register the host names for the internal company Web sites. All DNS zones are configured to allow dynamic updates.
The network contains two DNS servers. One has IP address 192.168.1.10 and the other has IP address

192.168.1.11. All DNS zones that are used by the company are replicated to both DNS servers.
You install Windows Server 2003 on a computer named Server10.corp.capandl.com, which is a
member of the corp. Certkiller .com domain. Server10.corp. Certkiller .com will host an internal Web site.
The internal web site must be accessible on the USL http://server10. Certkiller .com/.
You must configure the DNS client settings on Server10.corp. Certkiller .com to ensure that its DNS host
(A) record is automatically registered in the correct DNS zone. Server10.corp. Certkiller .com must be
able to resolve the computer names of all hosts in the Certkiller .com zone, corp. Certkiller .com zone, and
the engineering. Certkiller .com zone without specifying their domain names. There are no duplicate
host names on the network.
What should you do?
To answer, configure the appropriate option in the dialog box, and drag the appropriate DNS suffix
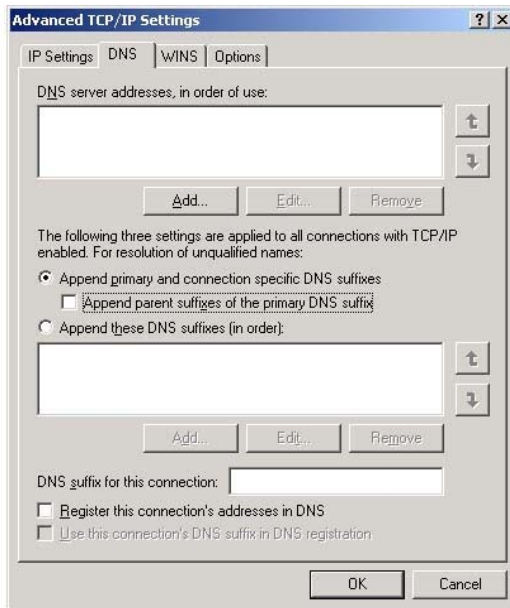or suffixes to the correct location or locations.

Select from these

DNS Suffixes
Certkiller.com
corp.Certkiller.com
engineering.Certkiller.com

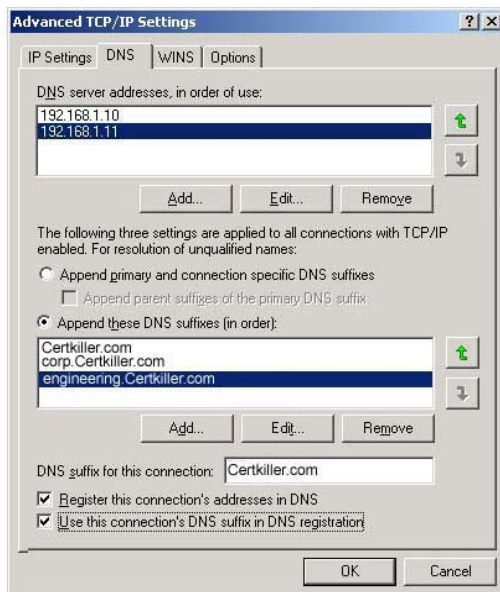**IP Addresses**
192.168.1.10
192.168.1.11

Advanced TCP/IP Settings   ? ×

IP Settings | DNS | WINS | Options

DNS server addresses, in order of use:

[   ]   ↑
                          ↓

Add...   Edit...   Remove

The following three settings are applied to all connections with TCP/IP
enabled. For resolution of unqualified names:

☉ Append primary and connection specific DNS suffixes
  ☐ Append parent suffixes of the primary DNS suffix
○ Append these DNS suffixes (in order):

[   ]   ↑
                          ↓

Add...   Edit...   Remove

DNS suffix for this connection: [   ]

☐ Register this connection's addresses in DNS
☐ Use this connection's DNS suffix in DNS registration

OK   Cancel

Answer:

Select from these

DNS Suffixes
Certkiller.com
corp.Certkiller.com
engineering.Certkiller.com

IP Addresses
192.168.1.10
192.168.1.11

Advanced TCP/IP Settings   ? ×

IP Settings | DNS | WINS | Options

DNS server addresses, in order of use:

192.168.1.10
192.168.1.11   ↑
                      ↓

Add...   Edit...   Remove

The following three settings are applied to all connections with TCP/IP
enabled. For resolution of unqualified names:

○ Append primary and connection specific DNS suffixes
  ☐ Append parent suffixes of the primary DNS suffix
☉ Append these DNS suffixes (in order):

Certkiller.com
corp.Certkiller.com   ↑
engineering.Certkiller.com   ↓

Add...   Edit...   Remove

DNS suffix for this connection: Certkiller.com

☑ Register this connection's addresses in DNS
☑ Use this connection's DNS suffix in DNS registration

OK   Cancel

Explanation: You need to configure Server10 to register an A record in the Certkiller .com domain because the internal web site has to be accessible on the URL http://server10. Certkiller .com/. Setting the DNS suffix to Certkiller .com, and selecting the Register this connection's address in DNS checkbox, and the Use this connection's DNS suffix in DNS registration checkbox will achieve this. Server10.corp. Certkiller .com must be able to resolve the computer names of all hosts in the Certkiller .com zone, corp. Certkiller .com zone, and the
engineering. Certkiller .com zone without specifying their domain names. You can ensure this by entering Certkiller .com, corp. Certkiller .com and engineering. Certkiller .com in the Append these DNS suffixes (in order)
box.
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. 552

QUESTION 520
You are the Network Administrator for Certkiller .com. The network consists of a single active directory domain named Certkiller .com. The domain contains three Windows Server 2003 computers, which are described in the following table:

Name	Role
Certkiller 1	Domain controller and primary DNS server
Certkiller 2	Accounting application server
Certkiller 3	Inventory application server

Two hundred Windows 2000 Professional computers use the accounting and inventory applications. The client computers connect to Certkiller 2 and Certkiller 3 by using TCP/IP and the names of the servers. The relevant portion of the network is shown in the exhibit.
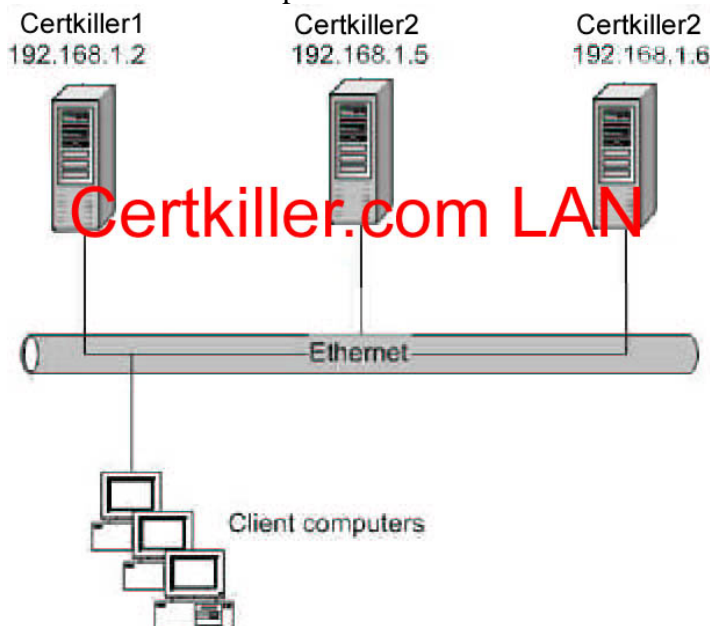
You need to consolidate servers. You move the inventory application to Certkiller 2 and then remove
Certkiller 3 from the network.
You need to ensure that all client computers can connect to Certkiller 2 for both the accounting and
inventory application and you do not want to modify the client computers. You need to minimize
administrative time.
What should you do?

A. Configure the network adapter on Certkiller 2 to use IP addresses 192.168.1.5 and 192.168.1.6.
B. On Certkiller 1, add a CNAME DNS record that refers Certkiller 3 to Certkiller 2.
C. Add a line to the Hosts file on Certkiller 2 that identifies 192.168.1.5 as Certkiller 3.
D. On Certkiller 1, add an HINFO DNS record that refers to Certkiller 2.

Answer: B

Explanation: You can enter an alias (CNAME) record in DNS to ensure that requests sent to
Certkiller 3. Certkiller .com are forwarded to Certkiller 2. Certkiller .com. Alias (CNAME) resource records are
sometimes called canonical names. These records allow you to use more than one name to point to a single
host. This makes it simpler to perform tasks such as hosting both an FTP server and a Web server on the
same computer. For instance, the well-known server names (ftp, www) are registered using CNAME RRs
that map to the DNS host name, such as "server-1" for the server computer that hosts these services.
Incorrect Answers:
A: This could work but it is not the recommended solution. Using a CNAME record in DNS is an easier
method.
C: The hosts file on Certkiller 2 is not used. DNS is used in this scenario.
D: An HINFO DNS record lists the hardware and operating system that is running at the listed host. This is
irrelevant.
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. 415

QUESTION 521
You are the Network Administrator for Certkiller .com. The Network consists of a single Active
Directory domain named Certkiller .com.
The domain contains 125 Windows 2000 Professional computers and two Windows Server 2003
Computers. The network has no direct connection to the internet.
A server named Certkiller A is a domain controller and the primary DNS Server for the Certkiller .com
domain. The network use Certkiller A as the authoritative root server for the Certkiller .com domain. A
server named Certkiller B is a domain controller and DHCP server. Server2 is also used as a web
server and it runs an intranet application.
Users report that when then try to connect to URLs outside of the Certkiller .com domain, their Web
Browsers are very slow to report that the URLs cannot be reached.
You need to ensure that DNS name resolution is as fast as possible.
What should you do?

A. Delete the cache.dns file from Certkiller A.
B. Delete the netlogon.dns file from Certkiller A.
C. In the Hosts file on Certkiller A, add a reference to Certkiller B.
D. In the Lmhosts file on Certkiller A, add a reference to Certkiller B.

Answer: A

Explanation: The cache.dns file contains a list of the Internet root DNS servers. From the question, it can be concluded that the DNS server is unaware that the network is not connected to the Internet. When the DNS server receives a name resolution request for an external hostname, it attempts to connect to an Internet root server. When the connection attempt times out, the DNS server attempts to contact another Internet root server. The process is repeated until an attempt has been made to contact all the root servers listed in the cache.dns file. This is the reason for DNS name resolution being slow. You can solve this problem by deleting the cache.dns file.
Incorrect Answers:
B: The netlogon.dns file allows you access to manually configure DNS, but this is not what is required, you need to ensure that DNS name resolution is as fast as possible and for this to occur you need to get rid of the cache.dns.
C, D: Adding a reference to Certkiller B in the Hosts file or even Lmhosts file on Certkiller A is not the same as purging information out of the cache. In fact it adds to the already populated cache.
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. 479


QUESTION 522
You are the administrator of an organizational unit (OU) named Finance. Certkiller 's network consists of two Windows 2003 Active Directory domains named Certkiller .com and main. Certkiller .com. The Finance OU is in the main. Certkiller .com domain.
The network contains a Windows 2003 Server computer named ServerA, which runs the DNS Server service. ServerA contains Active Directory integrated zones for both Certkiller .com and main. Certkiller .com.
A Windows 2000 Professional computer named Client1 must be moved from the Certkiller .com domain to the Finance OU in the main.tes tking.com domain. The domain administrator of Certkiller .com moves Client1 from Certkiller .com to a workgroup named Temp.
You join Client1 to the main. Certkiller .com domain. You move Client1 into the Finance OU. You discover that you cannot resolve Client1 by using Client1's fully qualified domain name (FQDN) when you run the ping command. You can resolve other client computers in the main. Certkiller .com domain by using a FQDN when you run the ping command.
You need to be able to resolve Client1 by using the FQDN. What should you do?

A. Run the ipconfig /registerdns command on Client1.
B. Run the ipconfig /flushdns command on Client1.
C. Ask the DNS administrator to configure the DNS server to require secure dynamic updates.
D. Ask the DNS administrator to configure main. Certkiller .com on ServerA as a standard primary zone.

Answer: A

Explanation: To resolve the fully qualified domain name of client1.main. Certkiller .com, you need an A record in the DNS zone for main. Certkiller .com. You can manually enter the A record (not given as an option in these answers) or you can force Client1 to register it's own A record by running the ipconfig /flushdns command on Client1.
Incorrect Answers:
B: This would clear the DNS cache on Client1. The question does not indicate that Client1 is experiencing problems resolving hostnames. Other computers are having problems resolving Client1's hostname.
C: It is immaterial whether the DNS server requires secure updates or insecure updates.
D: Whether the DNS zone is a standard primary zone or an Active Directory Integrated zone, is irrelevant.
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. 516

QUESTION 523
You are the network administrator for Certkiller .com. The network consists of a single DNS domain named Certkiller .com.
You replace a UNIX server with a Windows Server 2003 computer named Certkiller 1.
Certkiller 1 is the DNS server and start authority (SOA) for Certkiller .com. A UNIX server named Certkiller 2 is the mail server for Certkiller .com.
You receive reports that Internet users cannot send e-mail to the Certkiller .com domain. The host addresses are shown in the following window.
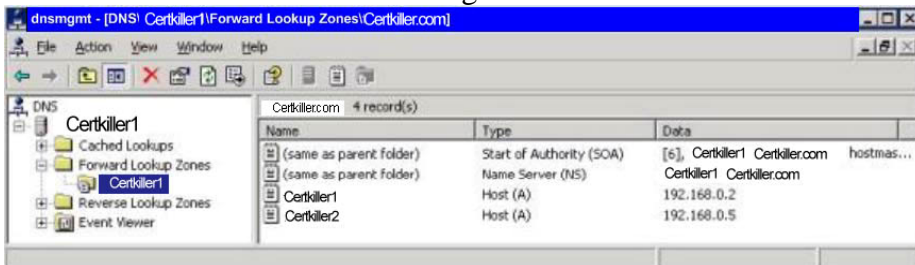
You need to ensure that Internet users can send e-mail to the Certkiller .com domain.
What should you do?

A. Add an _smtp service locator (SRV) DNS record for Certkiller 2.
B. Add a mail exchange (MX) DNS record for Certkiller 2.
C. Add an alias (CNAME) record for mail. Certkiller .com.
D. Enable the SMTP service on Certkiller 1.

Answer: B

Explanation: Email servers on the Internet query Certkiller 1 for the address of the mail server for the domain. The address of the mail server is held in a MX (Mail Exchange) DNS record.
Incorrect Answers:
A: Email servers find other email servers by using MX records, not SRV records.
C: Email servers find other email servers by using CNAME records.

D: The SMTP service should be running on the mail server and not on 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, p. 426

QUESTION 524
You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest named Certkiller .com. The forest contains two domains named Certkiller .com and corp. Certkiller .com. The network consists of 15 subnets.
The domain controllers are configured as shown in the following table.

Domain controller name	Domain	Zone	Zone type	Stub zone
CertkillerSrvA	Certkiller.com	Certkiller.com	Active Directory-integrated	corp.Certkiller.com
CertkillerSrvB	Certkiller.com	Certkiller.com	Active Directory-integrated	corp.Certkiller.com
CertkillerSrvC	corp.wingtiptous.com	corp.Certkiller.com	Active Directory-integrated	None
CertkillerSrvD	corp.Certkiller.com	corp.Certkiller.com	Active Directory-integrated	None

Certkiller SrvA and Certkiller SrvB are registered in Certkiller .com. All other computers are registered in corp. Certkiller .com.
You create reverse lookup zones for all subnets.
The corp. Certkiller .com domain contains a Windows NT Server 4.0 file and print server named Certkiller SrvE. You change the static IP address for Certkiller SrvE.
You need to ensure that this change is reflected in DNS.
Which two resource records should you modify? (Each correct answer presents part of the solution. Choose two)

A. The pointer (PTR) record in the corp. Certkiller .com zone.
B. The host (A) record in the corp. Certkiller .com zone.
C. The alias (CNAME) record in the corp. Certkiller .com zone.
D. The pointer (PTR) record in the stub zone.
E. The host (A) record in the stub zone.
F. The alias (CNAME) record in the stub zone.

Answer: A, B

Explanation: The NT server cannot register its own DNS records; therefore, you need to perform this manually. The two records that should be created are the 'A' record and the 'PTR' record. These records should be created in the corp. Certkiller .com zone because the NT server is a member of that domain.
Incorrect Answers:
C: You do not need a CNAME record. You only need to modify two resource records.
D: Stub zones are updated automatically, and only contain the names and IP addresses of DNS servers. Certkiller Srv5 is a File and Print server.
E: Stub zones are updated automatically, and only contain the names and IP addresses of DNS servers. Certkiller Srv5 is a File and Print server.
F: Stub zones are updated automatically, and only contain the names and IP addresses of DNS servers. Certkiller Srv5 is a File and Print 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, p. 424


QUESTION 525
You are the network administrator for Certkiller . The network contains eight DNS servers.
You use a DNS namespace named Certkiller .com in the network. All eight DNS servers must be configured to allow host named in the contoso.com namespace to be resolved. The following table specifies how each server will be configured to support the Certkiller .com namespace.

Server name	Support for contoso.com
CERTKILLERDNS01	Primary zone (Active Directory-integrated)
CERTKILLERDNS02	Primary zone (Active Directory-integrated)
CERTKILLERDNS03	Secondary zone
CERTKILLERDNS04	Secondary zone
CERTKILLERDNS05	Stub zone
CERTKILLERDNS06	Stub zone
CERTKILLERDNS07	Conditional forwarding to CERTKILLERDNS01
CERTKILLERDNS08	Conditional forwarding to CERTKILLERDNS01

There are currently many incorrect name server (NS) records in the Certkiller .com zone. You delete all the existing records.
You now need to add back the NS records for only the other servers that will host the Certkiller .com zone.
Which server or servers should be added as name servers to the Certkiller .com zone?
To answer, drag the appropriate server or servers to the correct location or locations in the dialog box.

Answer:

Servers
Select from these

Dialog box
Place here

Certkiller.com

Properties of the Certkiller.com Zone

| General | | Start of Authority (SOA) |
| Name Servers | WINS | Zone Transfers |

To add name servers to the list, click Add.

CERTKILLERDNS05.Certkiller.com
CERTKILLERDNS06.Certkiller.com
CERTKILLERDNS07.Certkiller.com
CERTKILLERDNS08.Certkiller.com

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
CERTKILLERDNS01.Certkiller.com	
CERTKILLERDNS02.Certkiller.com	
CERTKILLERDNS03.Certkiller.com	
CERTKILLERDNS04.Certkiller.com	

Explanation: You need to add the NS records to the DNS servers hosting the primary and secondary zones for Certkiller .com. Certkiller DNS01 and Certkiller DNS02 are primary servers. Certkiller DNS03 and Certkiller DNS04 are the secondary servers.
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. 427

QUESTION 526
You are the network administrator for Certkiller .com. The network consists of two DNS domains named Certkiller .com and west. Certkiller .com.
The company opens a new branch office. The network in the new office is configured as the east. Certkiller .com DNS domain.
The three domains now contain the Windows Server 2003 computers that are described in the following table.

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

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

Certkiller1
192.168.0.2

Certkiller.com
Certkiller.com WAN

Certkiller2
192.168.3.2

Certkiller3
192.168.5.2

west. Certkiller.com

east. Certkiller.com
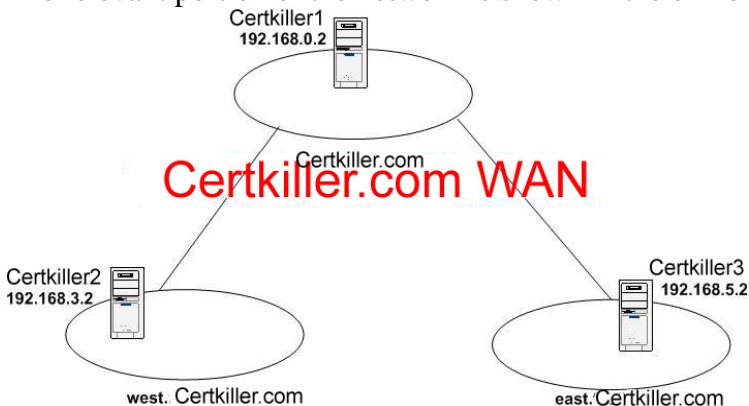
You start the New Delegation wizard to create a new delegation resource record for the east. Certkiller .com domain to the Certkiller .com domain.
How should you configure the delegation resource record?
To answer, drag the appropriate server name and IP address to the correct locations in the dialog

box.

Answer:

Explanation: When creating a delegation resource record, you must configure the fully qualified domain name (FQDN) of the DNS server that is authoritative for the delegated domain. In this case, the server's name is Certkiller 3.east. Certkiller .com and its IP address is 192.168.5.2.
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. 431

QUESTION 527
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains 100 Windows 2000 Professional

computers and three Windows Server 2003 computers. Information about the three servers is shown in the following table.

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

You add a network interface print device named Certkiller Printer1 to the network. You manually configure the IP address for Certkiller Printer1. Certkiller Printer1 is not currently registered on the DNS server. The relevant portion of the network is shown in the exhibit.
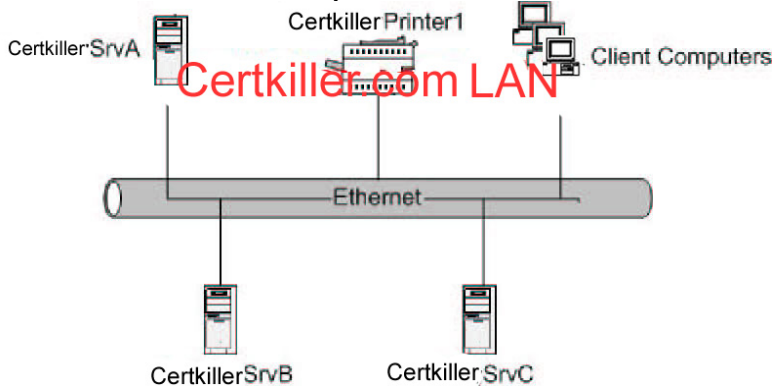
You need to ensure that client computers can connect to Certkiller Printer1 by using its name. What should you do?

A. On Certkiller SrvA, add an alias (CNAME) record that references Certkiller Printer1.
B. In the Hosts file on Certkiller SrvC, add a line that references Certkiller Printer1.
C. On Certkiller SrvA, add a service locator (SRV) record that reference Certkiller Printer1.
D. On Certkiller SrvA, add a host (A) record that references Certkiller Printer1.
E. In the Hosts file on Certkiller SrvB, add a line that references Certkiller Printer1.

Answer: D

Explanation: A host (A) record is utilized in a DNS zone to map DNS domain names of hosts or computers to their IP addresses. Therefore, adding a host (A) record in the DNS zone would ensure that client computers can connect to Certkiller Printer1 by using its name.
Incorrect Answers:
A: An alias (CNAME) resource record only points to an A record. Alias (CNAME) resource records enable you to utilize more than one name to point to a particular host.
B: DNS should be utilized in this case. A Hosts file associates host names to IP addresses and is typically stored in the WINDOWS\System32\Drivers\folder.
C: Service (SRV) records associate the location of a service such as a domain controller with information on the manner in which to contact the service. The printer does not require a SRV record.
E: A Hosts file associates host names to IP addresses. You should use DNS in this case.
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. 426

QUESTION 528
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain Certkiller .com. All domain controllers have the DNS service installed.
You configure a new UNIX server to act as a secondary DNS server that is authoritative for the DNS
zone. You create a host (A) record for the UNIX server in the DNS zone. You configure the DNS zone
to allow zone transfers to all servers.
You need to configure the DNS zone to accommodate the new UNIX server.
What should you do?

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

Answer: A

Explanation: You must add a name server (NS) resource record to the DNS zone when adding DNS servers
to the domain. The name server (NS) resource record is used in the DNS zone to assign the DNS domain
names for authoritative DNS servers for the DNS zone.
Incorrect Answers:
B: The SOA resource record defines the general parameters for the DNS zone such as Source host and
Refresh time, as well as the authoritative server is for the zone. A secondary zone's SOA tab indicates
the contents of the master SOA record.
C, D: SRV records basically associate the location of a service with information on how to contact the
service.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and
Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress
Publishing Inc., Rockland, 2003, pp 594-5, 786

QUESTION 529
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain named Certkiller .com. The domain contains 10 Windows Server 2003 computers.
The domain controllers are also configured as DNS server. Each DNS server hosts an Active
Directory-integrated forward lookup zone named Certkiller .com. The DNS servers are also configured
with a reverse lookup zone named 192.168.1.x Subnet.
The DHCP server is configured with a scope that has the following properties:
• An IP address range from 192.168.1.1 - 192.168.1.254
• A subnet mask of 255.255.255.0
• An exclusion range from 192.168.1.1 - 192.168.1.55
• Scope options that include the assignment of a DNS server and a WINS server.
The existing servers have static IP addresses within the range of 192.168.1.1 - 192.168.1.10.
You assign a static IP address to a new UNIX server named Server1.
You need to create a new host (A) resource record for Server1. In addition, you need to ensure that
the DNS servers will respond to reverse lookup queries against the IP address for Server1. You also
need to maximize the security and availability of the A record for Certkiller Srv13.

What should you do?

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

Answer:

Explanation:

A) IP Address

192.168.1.0 & 192.168.1.255: These are broadcast addresses and would therefore not be used.

192.168.1.1: Existing servers are 1-10. This address is already being used.

192.168.1.58: This address is already in the scope (remember that 1-55 are excluded, so 56-254 are dynamic and can only be used when a reservation is set).

192.168.1.25: This is therefore the only usable and available address remaining.

B) Also enable the Create associated pointer (PTR) record option.

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. 642

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. 440-444

QUESTION 530
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain named Certkiller .com. A Windows Server 2003 computer named Server1 is currently
the only domain controller for Certkiller .com. Server1 is also the DNS server for the Active
Directoryintegrated
zone named Certkiller .com.
You configure a new Windows Server 2003 computer named Server2 to query Server1 for DNS name
resolution. You run the Active Directory Installation Wizard on Server2 and restart Server2.
Forty-five minutes later, you inspect the service location (SRV) resource records, which are shown in
the exhibit.

Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268] server1 Certkiller.com
_kerberos	Service Location (SRV)	[0][100][88] server1 .Certkiller.com
_kpasswd	Service Location (SRV)	[0][100][464] server1 .Certkiller.com
_ldap	Service Location (SRV)	[0][100][389] server1 .Certkiller.com

SERVER1
Forward Lookup Zones
  _msdcs .Certkiller.com
  Certkiller.com
    _msdcs
    _sites
    _tcp
    _udp
    corp
    DomainDnsZones
    ForestDnsZones

You need to ensure that the SRV records on Server1 are complete.
What should you do?

A. Restart the Net Logon service on Server1.
B. Restart the Net Logon service on Server2.
C. Run the ipconfig /registerdns command on Server1.
D. Run the ipconfig /registerdns command on Server2.

Answer: B

Explanation: The Net Logon service on a domain controller registers the DNS resource records required for
the domain controller, to be located in the network every 24 hours. You can manually initiate the registration
performed by the Net Logon service by restarting the Net Logon service.
Incorrect Answers:
A: The exhibit shows that the SRV records for Certkiller A do exist. The records for Certkiller B are missing.
C: The exhibit shows that the SRV records for Certkiller A do exist. The records for Certkiller B are missing.
D: The command ipconfig /registerdns refreshes all DHCP address leases, and registers all related DNS
names configured and used by the client computer. This option will register client settings (A and PTR
records), but not server resource (SRV) records.
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, Chapters 4 & 17, p. 208, 977

QUESTION 531
You are the network administrator for Certkiller .com. All network servers run either Windows Server
2003, Windows 2000 Server, or Windows NT Server 4.0. All client computers run either Windows XP
Professional, Windows 2000 Professional, Windows NT Workstation 4.0, or Windows 98.
The network consists of an Active Directory domain named Certkiller .com. All domain controllers in
the domain run Windows Server 2003. All domain controllers also have the DNS service installed and

host an Active Directory-integrated zone named Certkiller .com. A Windows Server 2003 member server assigns IP addresses to all computers in the company. All IP addresses are assigned from the 10.1.0.0/24 scope.

All computers in the company must always be registered automatically in the Certkiller .com zone, regardless of the local TCP/IP configuration settings. Only computers that have valid computer accounts in the Active Directory domain must be able to register host (A) records in the zone. If a computer is removed from the network, the associated name registration must be removed from DNS. You are configuring the Certkiller .com DNS zone and the 10.1.0.0/24 DHCP scope to comply with the stated requirements.

Which configuration settings should you use?

To answer, configure the appropriate option or options in the dialog boxes.
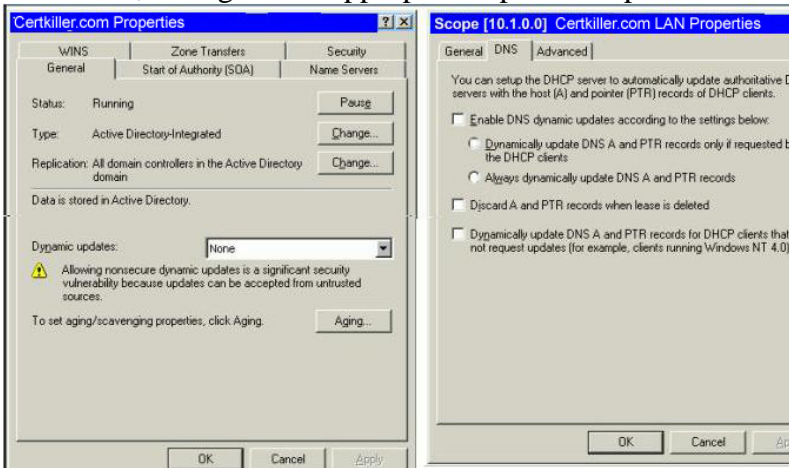
Answer:
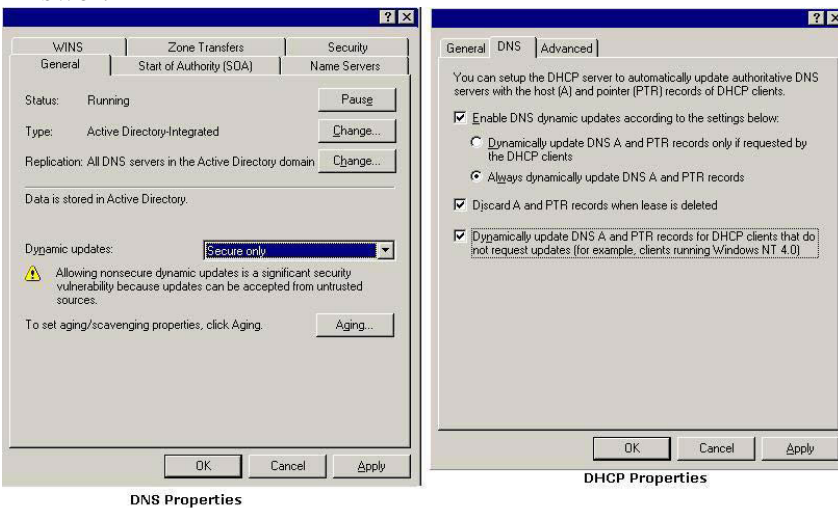
Explanation: Secure updates are applicable only to the DNS zones that are integrated into Active Directory. In this case access to the records is controlled by access control lists. The question states that the domain controllers have the DNS service installed and host an Active Directory-integrated zone named Certkiller .com. You can therefore select the Secure Only option to ensure that valid computers in the Active Directory domain are able to register host (A) records in the zone. For those client computers running Windows NT Workstation 4.0, or Windows 98, the DNS client computer - the DHCP server, can perform

dynamic updates for these clients. There is a Windows Server 2003 member server that assigns IP addresses to all computers in the company. When the Secure Only option is selected, only the owner of a record can update that record. You thereby enable the client computers to automatically create or update their own resource records.

Always Dynamically Update DNS A And PTR Records has to be enabled to allow client computers running Windows NT to have their DNS information automatically updated. Recall that the requirement states that the computers in the company must always be registered automatically in the Certkiller .com zone. Checking the Discard A And PTR Records When Lease Is Deleted would ensure that the associated name registration is removed from DNS when a computer is removed from the network. Enabling this checkbox ensures that DNS has the correct data.

To configure the DHCP server, the Windows Server 2003 member server, to update A resource records and PTR resource records for the Windows NT 4 Client, the Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request checkbox has to be enabled.

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 5, p. 179

QUESTION 532

You are the administrator of a Windows Server 2003 computer named Certkiller 3. Certkiller 3 is a domain member server that has the DNS service installed.

Certkiller 3 is configured with two network interfaces named NIC1 and NIC2. Routing is not enable between the two network interfaces. NIC1 and NIC2 are configured as shown in the following table.

Network interface	IP address	Subnet mask	Preferred DNS server	Purpose
NIC1	192.168.2.10	255.255.255.0	192.168.2.10	Connect to production network
NIC2	192.168.3.10	255.255.255.0	192.168.3.2	Connect to isolated preproduction network segment

Resources on the preproduction network segment use the same fully qualified domain names (FQDNs) as resources in the production network. The TCP/IP properties on client computers in the preproduction environment are controlled by individual testers.

You need to ensure that the users in the preproduction environment cannot resolve FQDNs from the production network. You want to accomplish this goal by using the DNS console on Certkiller 3. What should you do?

A. Configure the interfaces properties on Certkiller 3 to listen on 192.168.2.10 only.
B. Configure the forwarders on Certkiller 3 to refer requests to 192.168.3.2.
C. Configure Certkiller 3 to disable recursion.
D. Configure Certkiller 3 to disable round robin.

Answer: A

Explanation: When configuring Your DNS Server, the first tab, Interfaces, is used to tell your DNS server on which Network Interface Cards (NIC), and IP addresses attached those cards, it will listen for DNS queries. The default is to pick up all IP addresses assigned to the DNS server during installation.To limit the IP addresses on which your DNS server will listen, Only the following IP addresses, type the IP addresses you want in the IP Address field, and click the Add button.

Thus configuring the Certkiller 3 interfaces properties to listen to 192.168.2.10 only will result in the preproduction segment not being able to resolve FQDN's from the production network.

Incorrect answers:

B: Configuring the forwarders to refer requests to 192.168.3.2 will not prevent the preproduction segment from resolving the FQDNs from the production network.

C: One uses the Do not use recursion for this domain option check box when you are sure that the forwarder to which you are pointing the domain for resolution requests will be able to resolve queries for that domain. Otherwise, you will be faced with a lot of failed queries because no other resolution methods will be attempted. This is not the way to prevent preproduction from resolving FQDNs from the production section.

D: Round robining enables DNS entries that have multiple IP addresses sharing the same host name to be alternately sequenced through when clients query that host name for name resolution. This means that clients querying the same host name will be directed to different IP addresses in a load balancing fashion. Thus disabling round robin is not going to prevent the preproduction segment from resolving production FQDNs.

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, Rockland, 2003, pp. 492-497

QUESTION 533

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains five servers and 2,500 Windows XP Professional computers. The servers are described in the following table.

Server name	Operating System	Server roles	IP address
Certkiller 1	Windows Server 2003	Domain controller, DNS server	192.168.0.2
Certkiller 2	Windows Server 2003	Domain controller, DHCP Server	192.168.0.5
Certkiller 3	Windows 2000 Advanced Server	Member server, order entry application server	192.168.0.100
Certkiller 4	Windows 2000 Advanced Server	Member server, order entry application server	192.168.0.101
Certkiller 5	Windows Server 2003	Member server, database server	192.168.0.102

DNS round robin is enabled on Certkiller 1.

You want client computers to connect to Certkiller 3 and Certkiller 4 by using the host name Certkiller Server. You need evenly distribute connections to Certkiller 3 and Certkiller 4 to distribute the load.

What resource records should you create?

To answer, drag the appropriate host names, record types, and IP addresses to the correct locations.
Drag and Drop

Resource Records, Place here

Host name	Record Type	IP Address
Host Name	Record Type	IP Address
Host Name	Record Type	IP Address

Select from the these:
Host names

Certkiller1	Certkiller2	Certkiller3
Certkiller4	CertkillerServer	Certkiller5

Record Types

A	PTR	MX

IP Addresses

192.168.0.100	192.168.0.101	192.168.0.102
192.168.0.2	192.168.0.5	

Answer:

Resource Records, Place here

Host name	Record Type	IP Address
CertkillerServer	A	192.168.0.100
CertkillerServer	A	192.168.0.101

Select from the these:
Host names

Certkiller1	Certkiller2	Certkiller3
Certkiller4	CertkillerServer	Certkiller5

Record Types

A	PTR	MX

IP Addresses

192.168.0.100	192.168.0.101	192.168.0.102
192.168.0.2	192.168.0.5	

Explanation: The Address (A) Resource Record associates an FQDN or host name to an IP address.
This provides information for resolvers to request an IP address for a given FQDN.
PTR record is just the opposite of a type A record. It resolves an IP address to a host name.
The Mail Exchange (MX) resource record specifies a mail exchange server that will process e-mail for the domain name. Only mail servers use the MX record type. Mail exchange servers can either send the mail directly or forward it to another mail server that is closer to the final destination.
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, Rockland, 2003, pp. 427-428

QUESTION 534
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 acquires a company named Foo. Foo's network consists of a single Active Directory domain named foo.com.

A server named Certkiller 9 is a network-management application server in the foo.com domain. Certkiller 9 accesses all of the desktop client computers to perform automated software upgrades and hardware inventory. The network-management software on Certkiller 9 references desktop computers by unqualified host names, which are resolved to clientname.foo.com by using a DNS server.

You join Certkiller 9 to your domain to become Certkiller 9. Certkiller .com. The Certkiller 9 IP address is 10.10.10.90.

You gradually migrate all foo.com desktop client computer to your domain to become clientname. Certkiller .com. You do not have access to the foo.com DNS server. When Certkiller 9 attempts to apply an update to the client computers, the network-management software returns many alerts that say that desktop computers cannot be found.

You want to allow the network-management software on Certkiller 9 to resolve unqualified client host named in foo.com or Certkiller .com, and you want to use the minimum amount of administrative effort. What should you do?

A. On the DNS server for Certkiller .com, add a zone for foo.com. Create a host (A) record for Certkiller 9.foo.com that points to 10.10.10.90.
B. On Certkiller 9, in System Properties, type foo.com in the Primary DNS suffix of this computer field in the DNS Suffix and NetBIOS Computer Name setting.
C. On Certkiller 9, configure a Hosts file that contains the name and IP address of every network computer.
D. On Certkiller 9, in Advanced TCP/IP Settings, add foo.com and Certkiller .com to the Append these DNS suffixes (in order) setting.

Answer: D

Explanation: If you choose Append the DNS suffixes (in order), only domain names listed in that window will be tried for resolution purposes. Both the connection-specific and primary DNS suffix are ignored. This is exactly what is necessary if you want to allow the network management software on Certkiller 9 to resolve unqualified client host name in foo.com or Certkiller .com with the least amount of administrative effort. You should thus add the foo.com and Certkiller .com names in that setting.
Incorrect answers:
A: There is no need to add new zones or creating a host (A) record when all that is needed is to add the foo.com and Certkiller .com names to the Append these DNS suffixes (in order) setting through the Advanced TCP/IP setting.
B: The System properties do not host this option. The Advanced TCP/IP Settings is the place where you will find the appropriate settings.
C: A hosts file is a static file. If any names or addresses change, they must be changed manually in the hosts file. This is not what is required.
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, Rockland, 2003, pp. 69, 515

QUESTION 535
You are the network administrator for Certkiller .com. You administer a Windows Server 2003 computer named Certkiller 6. Certkiller 6 is a filer server that contains sensitive company data. Client

computers on the network run either Windows XP Professional or Windows NT Workstation 4.0. All users who need to connect to the shared folders on Certkiller 6 run Windows XP Professional.
Sandra, another network administrator, reports that all legacy application have been decommissioned on Certkiller 6 and that there is no longer any need to use anything other than DNS for name resolution on Certkiller 6.
You want to ensure that only the Windows XP Professional client computers can browse or map to shared folders on Certkiller 6.
What should you do?

A. Install the DNS Server service on Certkiller 6. Configure Certkiller 6 to refer to itself as the preferred DNS Server.
B. Configure Certkiller 6 to disable NetBIOS over TCP/IP.
C. Uninstall File and Print Sharing for Microsoft Networks.
D. Disable the computer browser service on Certkiller 6.

Answer: B

Explanation: NetBIOS works by broadcasting network resource information. Enable NetBIOS over TCP/IP - Enables the use of NetBIOS. Disable NetBIOS over TCP/IP - Disables the use of NetBIOS, in effect making settings useless.
Since NetBIOS packets aren't routable, you should disable NetBIOS over TCP/IP to ensure that only the Windows XP Professional clients can browse or map shared folders on Certkiller 6.
Incorrect answers:
A: The DNS client queries its preferred DNS server. The preferred DNS server contacts the DNS server that is authoritative for that zone. The authoritative server for that zone forwards that request to it's configured for resolution. The server resolves the name lookup and forwards the IP address back to the authoritative zone server. The authoritative zone server returns the IP address back to the preferred DNS server. The preferred DNS server returns the IP address back to the DNS client. However, this is not what is required.
C: Uninstalling File and Print Sharing for Microsoft Networks will not ensure that the Windows XP Professional client omputers can exclusively browse or map to shared folder on Certkiller 6.
D: Disabling computer browser service on Certkiller 6 is not the solution. You need to disable NetBIOS over TCP/IP on Certkiller 6.
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. 56
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, Rockland, 2003, p. 281


QUESTION 536
You are a network administrator for Certkiller .com. The network consists of three Active Directory domains.
You are responsible for managing a single Active Directory domain that contains five DNS servers.
You use the DNS console to manage all five DNS servers.

Some of the users on your network report that they cannot connect to network resources. You discover that the users' client computers are configured to use a DNS server named DC2 as their primary DNS server.
You view the DNS console, as shown in the exhibit.
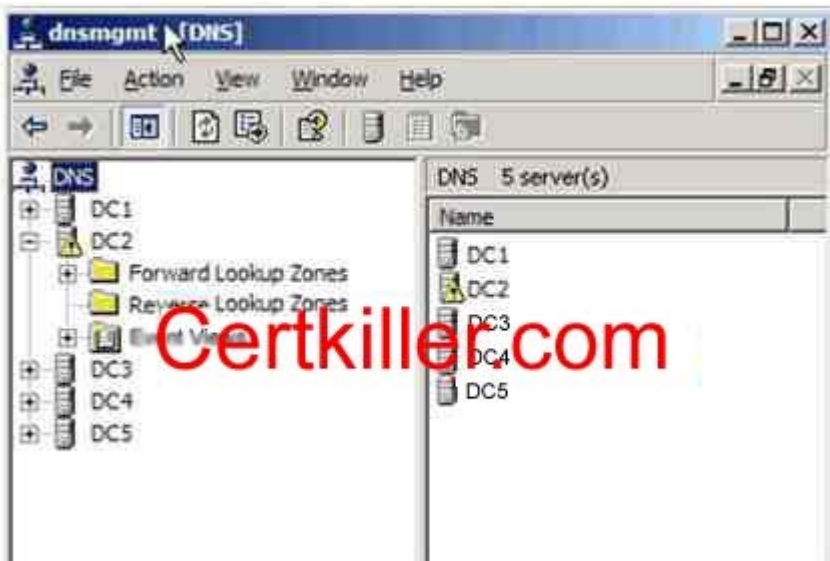
You need to identify the problem that is preventing users from connecting to network resources.
What should you do?

A. In the DNS event logs, look for error events.
B. In the DNS properties on DC2, look at the Event Logging tab.
C. In the system event logs, look for warning events.
D. In the DNS properties on DC2, look at the Monitoring tab.

Answer: A

Explanation: Windows Server 2003 automatically logs DNS events in the event log beneath a separate DNS server heading. DNS events are logged to the DNS event log, DNS Events, which is located either in the DNS console or the Event Viewer MMC console. Simply select DNS Events and look for any detailed DNS warnings and alerts to identify the problem that is preventing users from connecting to network resources.
Incorrect Answers:
B: The Event Logging tab enables you to configure the type of events that should be written to the DNS event log. You can log errors, warnings, and all events. This is a very wide parameter, making identification of the problem a lengthy process.
C: Events related to Windows system components are stored in this log file. This includes entries regarding failure of drivers and other system components during startup and shutdown. Thus this option will not enable you to view problems regarding connectivity.
D: The Monitoring tab can be used to test and verify the configuration by manually sending queries against the server. You can perform a simple query that uses the DNS client on the local server to query the DNS service to return the best possible answer. You can also perform a recursive query in which the local DNS server can query other DNS servers to resolve the query. Hence this tab will be used to resolve queries and not help you in identifying what prevents users from connecting to network

resources.

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. 762

Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 3

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 6, pp. 340-342

QUESTION 537

Exhibit

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest. The IT department manages the forest root domain, which is named Certkiller .com. The root domain contains three Windows Server 2003 domain controllers named Certkiller 1, Certkiller 2, and Certkiller 3. These three domain controllers have the DNS Service installed. The configuration of Certkiller .com zone is shown in the exhibit.

You view the event logs of the domain controllers. You notice that there are frequent failures of Active Directory transactions, which are caused by DNS lookup failures against the Certkiller .com zone. You discover that the data in the DNS zone on Certkiller 3 is out of date.

What should you do on Certkiller 3?

A. Use the Replmon utility to look for Active Directory replication errors.
B. Use Event Viewer to examine the DNS Server log for zone transfer errors.
C. Enable debug logging and examine the log file for transfer packets.
D. Use System Monitor to monitor the DNS\Zone Transfer Failure counter.

Answer: A

Explanation: The Active Directory Replication Monitor, replmon.exe, is part of the Windows 2000 Support Utilities available on the Windows 2000 Server CD in the \SUPPORT\TOOLS folder. The replmon command allows you 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.

Incorrect answers:

B: Examining the DNS server log for zone transfer errors through the Event Viewer will not yield the proper information for your purposes.

C: Debug logging logs every packet in and out of the DNS server. DNS debug logging collects information by logging any DNS traffic that fits the debug logging criteria. Thus this option will not do since you need to make use of the Replmon utility to look for the Active Directory Replication errors that is causing the DNS lookup failures.

D: System Monitor will reveal the live performance to you, but not those that has already taken place. Thus this option is not the answer.

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. 343, 477, 551, 961

Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 4

QUESTION 538

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

Three network servers are configured as DNS servers. The DNS servers are configured as shown in the exhibit.
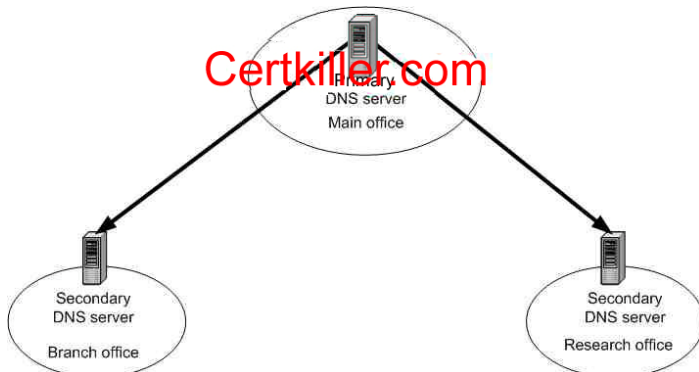
You need to verify that the DNS data on all DNS servers is up to date.

What should you do on each DNS server?

A. Review the event log.
B. View the Certkiller .com zone properties.
C. Use Replication Monitor.
D. Use System Monitor.

Answer: B

Explanation: The General tab of the zone properties allows you to determine what the status of your DNS server service is. Zone properties include: General, Start of Authority (SOA), Name Servers, WINS, Zone Transfers and Security.

DNS zone data is kept updated during the zone transfer process by using a number of configurable time intervals such as the Refresh interval, Retry interval, Expires after, Minimum (default) TTL and TTL for this record interval setting. These settings would be located on the Start of Authority (SOA) tab of the Certkiller .com zone properties. You can manually initiate a zone transfer by incrementing the Serial Number field. This is done by selecting the Increment button.

Incorrect Answers:

A: Reviewing the event log enables you to configure the type of events that should be written to the DNS event log. You can log errors, warnings, and all events. You can also turn off logging by selecting No Events. This would not be necessary as all you need to do is to view the Certkiller .com zone properties.

C: Making use of the Replication you can 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. Monitoring replication does not mean that you will be able to verify that DNS data on all DNS servers is up to date.

D: Using System monitor System Monitor can be used to actively monitor live performance statistics for your DNS server using over 60 different DNS-related performance counters. This means you still need to view the Certkiller .com zone properties.

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 5, pp. 262-279.

QUESTION 539

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

One network server is a DNS server named DNS1. Client computers query DNS1 to locate information on Active Directory.

A user that is using a client computer named Certkiller 1 reports that he cannot access network resources. You discover that this problem is caused by incorrect name resolution. You verify that DNS is configured correctly on Certkiller 1. You also verify that other client computers can query DNS1.

You need to view the complete queries and response between Certkiller 1 and DNS1.

What should you do?

A. Enable debug logging on DNS1.
B. Use System Monitor to monitor queries and responses on DNS1.
C. Review the event logs on DNS1 for errors relating to the DNS service.
D. On Certkiller 1, run the nslookup command to view the zone records on DNS1.

Answer: A

Explanation: DNS debug logging is an optional logging tool for DNS that stores the DNS information that you select.

Because debug logging consumes server resources, it is disabled by default. Debug logging is configured at the DNS server level. The debug logging settings therefore affect all zones hosted on the DNS server. DNS

debug logging collects information by logging any DNS traffic that fits the debug logging criteria.
Logging continues until either the log file size specified is met or the drive where the log file is stored runs out of space.
Incorrect Answers:
B: System Monitor 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.
C: Queries and responses do not necessarily mean errors in the DNS service.
D: The nslookup command can be used to determine the hostname associated with a specific IP address. To use the nslookup command, PTR records must exist. Thus this option is not the answer.
Reference:
D1iana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 3


QUESTION 540
You are the network administrator for the IT department of Certkiller . The company network consists of an Active Directory forest named Certkiller .com.
The IT department manages the forest root domain named Certkiller .com. This domain contains two Windows Server 2003 domain controllers named DC02 and DC03. Both domain controllers have the DNS service installed. All DNS zones are Active Directory-integrated.
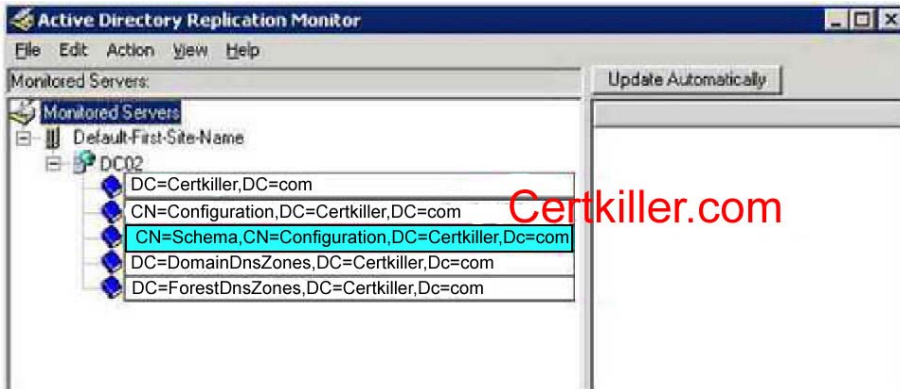You notice that recent changes to the _mcdcs. Certkiller .com zone were not replicated to DC02. The configuration of the _mcdcs. Certkiller .com zone is shown in the exhibit.
MISSING
You need to verify that the _msdcs. Certkiller .com zone is being successfully replicated. You want to use Active Directory Replication Monitor to monitor DC02
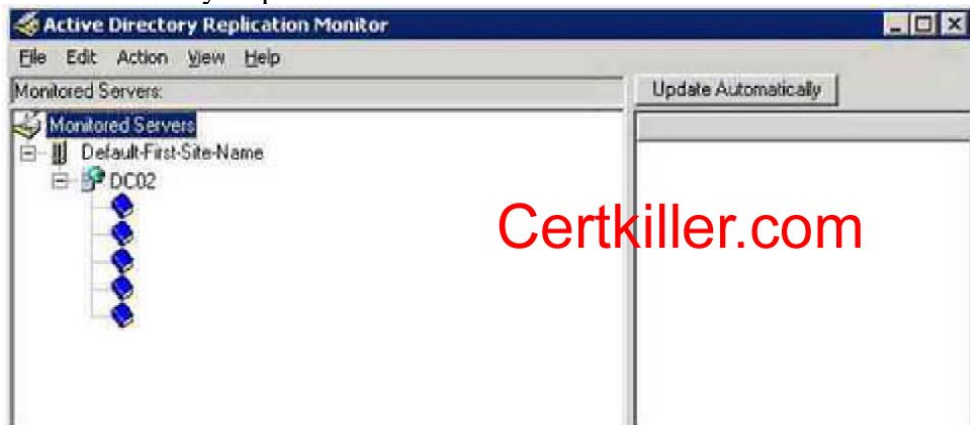
Answer:

Explanation: The Active Directory Replication Monitor, replmon.exe, is part of the Windows 2000 Support Utilities available on the Windows 2000 Server CD in the \SUPPORT\TOOLS folder.
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. 477

QUESTION 541
You are the network administrator for Certkiller .com. Certkiller uses the Certkiller .com DNS namespace. The primary name server for the Certkiller .com zone is a Windows Server 2003 computer named DNS01. The Certkiller .com zone on DNS01 is enabled for dynamic updates.
You notice that some hosts that should be registered in the Certkiller .com zone are not listed. You need to find the cause of the problem. You need to find out which computers are attempting to perform dynamic registrations and which DNS records they are attempting to register.
What should you do?

A. Use Event Viewer to examine the DNS Server to log on DNS01.
B. Use Event Viewer to examine the System log on DNS01.
C. Enable DNS debug logging on DNS01 and examine the log file.
D. Use System Monitor to look for client registrations on DNS01.

Answer: C

Explanation: Debug logging logs every packet in and out of the DNS server. DNS debug logging is an optional logging tool for DNS that stores the DNS information that you select.
Because debug logging consumes server resources, it is disabled by default. Debug logging is configured at the DNS server level. The debug logging settings therefore affect all zones hosted on the DNS server. Debug logging can be resource intensive, by affecting overall server performance and consuming disk space. Therefore, it should only be used temporarily, in cases where more detailed information about server performance is needed. DNS debug logging collects information by logging any DNS traffic that fits the debug logging criteria. Logging continues until either the log file size specified is met or the drive where the log file is stored runs out of space. After the file limit is reached, the logging process will begin to overwrite the oldest entries. Because log files can grow quite large, it is recommended that they be located on a separate drive.
Incorrect Answers:

A: Examining the DNS server to log on DNS01 through the Event Viewer will not yield the proper information for your purposes.

B: The system log on DNS01 contains events generated by Windows system components.

D: To look for client registrations on DNS01 using System Monitor will reveal the live performance to you, but not those that has already taken place. Thus this option is not the answer.

Reference:

Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 4

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. 343, 551, 961

QUESTION 542

You are the DNS administrator for Certkiller .com. Certkiller is an (ISP) that host web sites for many companies. Certkiller DNS server hosts multiple DNS zones for customers. Several Certkiller administrators are allowed to add DNS zones.

You want to produce a weekly report that will list all the zones that are hosted on each DNS server. What should you do?

A. Use the dnslint utility to query each DNS server.
B. Use the dnscmd utility to query each DNS server.
C. Use the nslookup utility to query each DNS server.
D. Use the adsiedit utility to query Active Directory for a list of DNS zones.

Answer: B

Explanation: The dnscmd utility can be found with the support tools on the Windows Server 2003 CDROM. The dnscmd /unumzones list all the zones on a DNS server.

Incorrect Answers:

A: The dnslint utility can be used to verify DNS records from a list. It does not list all the zones on a DNS server.

C: The nslookup utility can be used to list all records in a zone, but it does not list all the zones on a DNS server.

D: The adsiedit utility is used to edit Active Directory attributes. It does not list all the zones on a 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, 858

QUESTION 543

You are the network administrator for Certkiller .com. The network consists of two DNS domains named Certkiller .com and south. Certkiller .com.

A Windows Server 2003 computer named Certkiller SrvA is a domain controller and DNS server for Certkiller .com. Certkiller SrvA is also a secondary zone server for south. Certkiller .com.

A Windows 2000 Server computer named Certkiller SrvB is a domain controller and the DNS server for south. Certkiller .com.

The two DNS domains are connected through an ISDN line.
You need to monitor the successful incremental zone transfers from south. Certkiller .com to
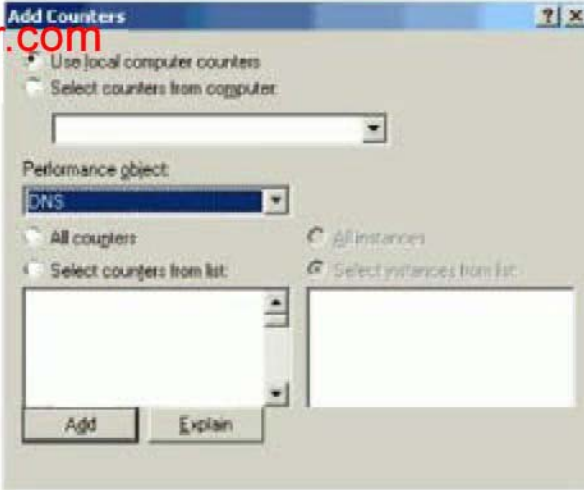Certkiller .com.
What should you do?

Computers

CertkillerSrvA

CertkillerSrvB

Counters

AXFR Success Received

IXFR Success Received

Dynamic Update Received

Secure Update Received

WINS Reverse Lookup

Dialog Box Place here

Add Counters

Use local computer counters
Select counters from computer:

Performance object:
DNS

All counters   All instances
Select counters from list: Select instances from list:

Add   Explain

Answer:

Computers

CertkillerSrvB

Counters

AXFR Success Received

Dynamic Update Received

Secure Update Received

WINS Reverse Lookup

Dialog Box Place here

Add Counters

Use local computer counters
Select counters from computer:

CertkillerSrvA

Performance object:
DNS

All counters   All instances
Select counters from list: Select instances from list:

IXFR Success Received

Add   Explain

Explanation: The IXFR Success Received counter indicates the number of successful incremental zone
transfers received by a secondary DNS server.
AXFR relates to an all zone transfer.

The Dynamic Update Received counter is typically for determining whether DNS clients are attempting to update their DNS addresses.

The Secure Update Received counter is for determining the number of systems that is successfully performing secure updates in DNS.

The WINS Reverse Lookup counter relates to WINS reverse lookups.

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. 539

QUESTION 544

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. A Windows Server 2003 computer named Certkiller C functions as the DNS server for the domain.

Wingtip Toys is a division of Certkiller . The Wingtip Toys network consists of a single Active Directory domain named wingtiptoys.com. Certkiller C is a secondary zone server for wingtiptoys.com. You are monitoring notification traffic between the two domains. You need to keep a record of when the primary DNS server for wingtiptoys.com informs Certkiller C if available changes in the wingtiptoys.com zone.

What should you do?

A. Use the Performance console to create a log of the DNS performance counter Notification Received on Certkiller C.
B. Enable debug logging on Certkiller C.
Configure the log to record Notification events.
C. Run the replmon command to monitor replication events on Certkiller C.
D. Run the dcdiag command to check DNS registration on Certkiller C.

Answer: B

Explanation: Debug logging is disabled by default and has to be enabled on Certkiller C. Select the Log packets for debugging check box to configure Debug Logging. To receive useful debug logging information, you should select a Packet direction, a Transport protocol, and at least one more option. You can also specify the file path and name, and the maximum size for the log file. Enabling Debug Logging slows DNS server performance.

Incorrect Answers:

A: The debug logging logs every packet in and out of the DNS server; you do not want to create a log of the DNS performance counter.

C: The debug logging logs every packet in and out of the DNS server, whereas the replmon command allows you 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.

D: The debug logging logs every packet in and out of the DNS server; you do not need to check DNS registration on Certkiller C.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder, Chad Todd and Laura Hunter, MCSA/MCSE : Exam

---

QUESTION 545
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.
The domain contains a single DNS server named Certkiller 8. Root hints are enabled on Certkiller 8. Internet access for company is provided by a Network Address Translation (NAT) server named Certkiller 9. Certkiller 9 is connected to the Internet by means of a permanent connection the company's ISP.
Users report that they can no longer connect to http://www. Certkiller .com. Users can connect to internal resources and to other Internet Web sites. You can successfully access http://www. Certkiller .com from a computer outside the corporate network.
You need to ensure that the users can access http://www. Certkiller .com. You must also ensure that users retain their ability to access internal resources.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Disable Routing and Remote Access on Certkiller 9.
B. Create a root zone on Certkiller 8.
C. On all affected users' computers, run the ipconfig /flushdns command.
D. Configure all affected users' computers to use the ISP's DNS server.
E. Use the DNS console on Certkiller 8 to clear the DNS cache.

Answer: C, E

Explanation: To clear the DNS resolver cache, you can enter ipconfig /flushdns at the command prompt. Alternatively, you can restart the DNS Client service by using the Services console, an administrative tool accessible through the Start menu. The Ipconfig /flushdns command purges the contents of the DNS client cache. Thus running this command on the affected users' computers will ensure that users can access the sites that they need access to and retain their ability to access internal resources.
Incorrect answers:
A: It is not a matter of disabling Routing and Remote Access on Certkiller 9. Certkiller 9 is responsible for NAT and you will be shooting yourirself in the foot is you disable Routing and Remote Access.
B: This approach creates an empty root zone and makes the internal server a root server. It would then never use forwarders and would resolve only internal queries. This approach is not a solution to this problem.
D: Merely configuring all affected computers to use the ISP's DNS server is not going to achieve your goal here. It is impractical.
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. 4:54

QUESTION 546
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.
A Windows Server 2003 computer named Certkiller 5 is the only DNS server in the domain. It hosts no other zones.
Users report that connecting to computers within the Certkiller .com domain is slow.
You need to find out whether DNS client traffic on Certkiller 5 is causing this problem.
What should you do?

A. Use System Monitor to create a log of the DNS counters Dynamic updates/sec and Total queries/sec.
B. Use System Monitor to create a log of the NetworkInterface counter Total bytes/sec.
C. Enable debug loggin on Certkiller 5. Configure the log to capture Notification events.
D. Enable debug loggin on Certkiller 5. Configure the log to capture Update events.

Answer: A

Explanation: The System Monitor utility is used to collect and measure the real-time performance data for a local or remote computer on the network. Through System Monitor, you can view current data or data from a log file. When you view current data, you are monitoring real-time activity. When you view data from a log file, you are importing a log file from a previous session.
Using the System Monitor, you can generate statistics on the following types of information regarding DNS services:
AXFR requests (all-zone transfer requests), IXFR requests (incremental zone transfer requests), DNS server memory usage, Dynamic updates, DNS Notify events, Recursive queries, TCP and UDP statistics, WINS statistics and Zone transfer issues. Thus to find out where DNS client traffic is responsible for the slow speed at which computers connect within the Certkiller .com domain, then you should create a log of the Dynamic Updated/sec and the Total queries/sec given the fact that Certkiller 5 is the only DNS server in the domain.
Incorrect answers:
B: The NetworkInterface counter Total bytes/sec is not going to yield the information that you need to check.
C, D: This is inappropriate in the given circumstances as it willnot yield the proper information that you will need to check to see if DNS client traffic on Certkiller 5 is responsible for the slow connections within the domain.
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. 70-73, 304

QUESTION 547
You are the network administrator in the New York office of Certkiller . The company network consists of a single Active Directory domain Certkiller .com. The New York office currently contains one Windows Server 2003 file server named Certkiller A.
All file servers in the New York office are in an organizational unit (OU) named New York Servers.
You have been assigned the Allow - Change permission for a Group Policy object (GPO) named

NYServersGPO, which is linked to the New York Servers OU.

The written company security policy states that all new servers must be configured with specified predefined security settings when the servers join the domain. These settings differ slightly for the various company offices.

You plan to install Windows Sever 2003, on 15 new computers, which all functions as file servers. You will need to configure the specified security settings on the new file servers.

Certkiller A currently has the specified security settings configured in its local security policy. You need to ensure that the security configuration of the new file servers is identical to that of Certkiller A. You export a copy of Certkiller A's local security policy settings to a template file.

You need to configure the security settings of the new servers, and you want to use the minimum amount of administrative effort.

What should you do?

A. Use the Security Configuration and Analysis tool on one of the new servers to import the template file.
B. Use the default Domain Security Policy console on one of the new servers to import the template file.
C. Use the Group Policy Editor console to open NYServersGPO and import the template file.
D. Use the default Local Security Policy console on one of the new servers to import the template file.

Answer: C

Explanation: Group policy provides us with a simple way of applying settings to multiple computers or users. In this case, we have a template file with the required security settings. We can simple import this file into a group policy object and apply the group policy to the servers.
Incorrect Answers:
A: This would configure the required settings, but only on one server.
B: This would apply the settings to all computers in the domain. We only want the settings to apply to the servers.
D: This cannot be done.
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. 649

QUESTION 548
You are the network administrator for Certkiller . The network consists of a single Active Directory domain Certkiller .com. The domain contains 35 Windows Server 2003 computers; 3,000 Windows XP Professional computers; 2,200 Windows 2000 Professional computers.

The written company security policy states that all computers in the domain must be examined, with the following goals:
• To find out whether all available security updates are present.
• To find out whether shared folders are present.
• To record the file system type on each hard disk.

You need to provide this security assessment of every computer and verify that the requirements of the written security policy are met.

What should you do?

A. Open the Default Domain Policy and enable the Configure Automatic Updates policy.
B. Open the Default Domain Policy and enable the Audit object access policy, the Audit account management policy, and the Audit system events policy.
C. On a server, install and run mbsacli.exe with the appropriate configuration switches.
D. On a server, install and run HFNetChk.exe with the appropriate configuration switches.

Answer: C

Explanation: The Microsoft Baseline Security Analyser can perform all the required assessments.
Mbsacli.exe includes HFNetChk.exe which is used to scan for missing security updates.
In general, the MBSA scans for security issues in the Windows operating systems (Windows NT 4, Windows 2000, Windows XP), such as Guest account status, file system type, available file shares, members of the Administrators group, etc. Descriptions of each OS check are shown in the security reports with instructions on fixing any issues found.
Incorrect Answers:
A: This won't check for missing updates, shared folders or file system type.
B: This won't check for missing updates, shared folders or file system type.
D: This will check for missing updates but not shared folders or file system type.
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, pp. 788-790

QUESTION 549
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.
Security is the highest priority for the network management for Certkiller . All network computers require smart cards to log on. An IPSec policy is implemented to secure network traffic. All servers are physically secured in an off-site location.
You must implement the most secure procedure for server management.
What should you do?

A. Log on to your client computer by using the built-in Administrator account for the domain. Configure a mandatory profile for the Administrator account. Change the password for the Administrator account on a weekly basis.
B. Log on to your client computer by using the built-in Administrator account for the domain. Configure a roaming profile for the Administrator account. Map a drive to the roaming profile by using the net use /smartcard command.
C. Create a new user account and add the account to only the built-in Domain Users groups. Log on to your client computer by using the new user account. Run all administrative tools by using the runas /smartcard command.
D. Create a new user account and add the account to the following built-in groups. Domain Users, Server Operators, and Account Operators. Log on to your client computer by using the new user

account. Run all administrative tools by using the runas /smartcard command.

Answer: C

Explanation: You should first create a new user account and then add it to the built-in Domain Users group and log on to the new user account before doing any server management.
The run as command, also called secondary logon, will allow 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. Since all network computers require smart cards to log on, in this scenario, you should use the runas / smartcard command and run all the administrative tools. This represents the most secure procedure.
Incorrect answers:
A: Configuring a mandatory profile is not the answer. Mandatory profiles do not allow any alterations to desktop settings made by the user to be retained. Additionally, profiles are assigned to users, not computers.
B: A roaming profile is a profile that is stored in a network-accessible location, thus allowing a user to access their desktop, application data, and settings when they log on to any computer. There is no need to configure a roaming profile in this scenario; it is not the most secure option. Also, profiles are assigned to users, not computers. Furthermore roaming profile data cannot be encrypted by the server.
D: You do not have to add the new user account to all those various groups. This can result in an unnecessary security risk.
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: Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 583
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, pp. 5-13

QUESTION 550
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. All client computers run Windows XP Professional.
An application named Certkiller .exe is installed on all computers in the domain to remotely gather software inventory information. The application runs as a service in the security context of the Local System. The startup type of the service is set to Automatic.
In the Default Domain Policy GPO, the security administrator has configured a software restrictive policy that is applied to all computers in the domain. The policy contains a hash rule for the Certkiller .exe application, and the hash rule is configured with a security level of Unrestricted.
The client computers on the network are attacked by a worm that is distributed by e-mail messages received over the Internet. The worm detects the presence of Certkiller .exe on a computer, then starts a new instance of the application in the security context of the logged-on user. The worm exploits a bug in the application to cause the computer to fail.
You need to ensure that Certkiller .exe cannot be started by the worm, while still allowing the application to run as a service.
What should you do?

A. In the computer settings section of the Default Domain Policy GPO, configure a software restriction policy that contains a zone rule for the Internet Zone. Configure the zone rule with a security level of Disallowed.
B. In the user settings section of the Default Domain Policy GPO, configure a software restriction policy that contains a zone rule for the Internet zone. Configure the zone rule with a security level of Disallowed.
C. In the computer settings section of the Default Domain Policy GPO, configure a software restriction policy that contains a hash rule for the Certkiller .exe application. Configure the zone hash rule with a security level of Disallowed.
D. In the user settings section of the Default Domain Policy GPO, configure a software restriction policy that contains a hash rule for the Certkiller .exe application so that the hash rule has a security level of Disallowed.

Answer: D

Explanation: A hash is a fixed-size result that is obtained by applying a one-way mathematical function (sometimes called a hash algorithm) to an arbitrary amount of data. The hash changes if there is a change in the input data. The hash can be used in many operations, including authentication and digital signing. Also called a message digest. We need to prevent unauthorized applications from running. We should set the default security level to Disallowed. If the software restriction policy containing the hash rule for that application is set to the disallowed level in the user settings section of the Default domain Policy GPO, then it will still allow the application to be run whilst ensuring that the worm cannot start the Certkiller .exe.
Incorrect answers:
A: Zone rule is a rule can identify software from the Internet Explorer zone from which it is downloaded. You should be setting a hash rule with the disallowed security setting rather. Also you should be applying the worm prohibiting measure from the user settings section of the Default Domain Policy GPO and not the computer settings section.
B: Applying the measures that you need to take in the user settings section of the Default Domain Policy GPO is correct, but it should be a hash rule rather than a zone rule to make it the appropriate rule with which to contain the worm
C: Applying the correct prohibiting measures through the hash rule, however, you should be applying the worm prohibiting measure from the user settings section of the Default Domain Policy GPO and not the computer settings section.
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, pp. 657 -659

QUESTION 551
Exhibit

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. All computers are members of the domain.

The Secure Server (Require Security) IPSec policy is assigned to a file server named Certkiller 2. The policy is configured as shown in the exhibit.

Users report that they cannot access shared folders on Certkiller 2. Users were able to access shared folders on Certkiller 2 prior to the implementation of the IPSec policy.

You need to ensure that all client computers in the domain can access the shared folders on Certkiller 2. You must ensure that all communications between client computers and Certkiller 2 be encrypted.

What should you do?

A. On Certkiller 2, enable the All ICMP Traffic IP Security rule in the properties of the Secure Server (Require Security) IPSec policy.
B. On Certkiller 2, enable the <Dynamic> IP Security rule in the properties of the Secure Server (Require Security) IPSec policy.
C. On all client computers, assign the Client (Respond Only) IPSec policy.
D. On all client computers, install an IPSec communication certificate in the local machine store.

Answer: C

Explanation: IPSec is used to protect data that is sent between hosts on a network, which can be remote access, VPN, LAN, or WAN. IPSec ensures that data cannot be viewed or modified by unauthorized users while being sent to its destination. Before data is sent between two hosts, the source computer encrypts the information. It is decrypted at the destination computer.

The Client (Respond Only) IPSec policy 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 applying the Client (Respond Only) IPSec policy on the client computers you will be ensure them access

to the shard folders on Certkiller 2 as well as ensure that communications between them and Certkiller 2 be encrypted.
Incorrect answers:
A: When the Server Secure (Require Security) option is selected, the server requires all communications to be secure. If a client is not IPSec-aware, the session will not be allowed. With this setting on Certkiller 2 you will not comply with what is required by the question. You need to apply settings to the client computers rather than the server in this scenario.
B: It does not matter whether you enable the <Dynamic> IP Security rule in the properties of the Secure Server (Require Security) IPSec policy, it will not comply with the requirements of the question.
D: Applying the measures on the client computers is correct, however you need to assign Client (Respond Only) IPSec policy and not install IPSec communication certificate on the local machine.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 552
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named CertK inmg.com. While performing network monitoring, you notice that the confidential files that are stored on Certkiller 8 are being transmitted over the network without encryption.
You must ensure that encryption is always used when the confidential files on Certkiller 8 are stored and transmitted over the network.
What are two possible solutions to accomplish this goal? (Each answer is a complete solution. Choose two)

A. Enable offline files for the confidential files that are stored on Certkiller 8, 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 Certkiller 8 and the client computers of the users who need to access the confidential files.
C. Use Server Message Block (SMB) signing between Certkiller 8 and the client computers of the users who need to access the confidential files.
D. Disable all LM and NTLM authentication methods on Certkiller 8.
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: IPSec provides two services: a way for computers to decide if they trust each other (authentication) and a way to keep network data private (encryption). The IPSec process calls for two computers to authenticate each other before beginning an encrypted connection. At that point, the two machines can use the Internet Key Exchange (IKE) protocol to agree on a secret key to use for encrypting the traffic between them. This option will ensure that encryption will always be in use when confidential files that are stored on Certkiller 8 are transmitted over the network.
IIS 6.0 offers four types of user-authentication methods. In addition to the four basic types of user authentication that are available in IIS 6.0, you can also configure client or server certificates, each of which uses SSL encryption for secure communications. Client certificates allow the server to positively identify the

client based on personal information contained in each client's certificate. Server certificates allow the client to positively identify the server based on specific information contained in each server's certificate. Each of the four basic authentication methods offers different functionality and security; therefore, you need to select an authentication method based on the functionality required for a particular application or purpose. Thus with the confidential files in XML format and enabling SSL on the IIS server, you can ensure that files are encrypted when stored and when transmitted.

Incorrect answers:

A: Enabling offline files is already a security risk. This also does not ensure that encryption is always used when the confidential files on Certkiller 8 are stored and transmitted over the network.

C: SMB was 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 use of SMB signing between Certkiller 8 and the client computers is not the answer.

D: A system configured with the Default security template or not configured with any security modifications will send LAN Manager and NTLM responses. Disabling LM and NTLM authentication methods on Certkiller 8 will thus not help in this scenario.

Reference:

Lisa Donald, Suzan Sage London and James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 171

Dan Balter, MCSA/MCSE Managing and Maintaining a Microsoft Windows Server 2003 Environment Exam Cram 2 (Exam 70-290), Chapter 7

QUESTION 553

You are the network administrator for Certkiller .com. The network contains a Windows Server 2003 computer named Certkiller 1.

Three administrators are members of the Administrators local group on Certkiller 1. Twelve other administrators are members of the Domain Admins group. The Domain Admins group is also a member of the Administrators local group on Certkiller 1.

Someone makes an unauthorized change to the HKEY_LOCAL_MACHINE\SYSTEM key in the registry on Certkiller 1, which causes the computer to fail. You fix the problem.

You need to log all attempts to access the HKEY_LOCAL_MACHINE\SYSTEM key in the registry on Certkiller 1. You decide to enable auditing in the local security policy on Certkiller 1.

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

A. Enable auditing in the local security policy on Certkiller 1.
Select the Audit object access (success and failure) option in the audit policy.
B. Enable auditing in the local security policy on Certkiller 1.
Select the Audit privilege use (success and failure) option in the audit policy.
C. Enable auditing in the local security policy on Certkiller 1.
Select the Audit systems events (success and failure) option in the audit policy.
D. Configure the SACL on the HKEY_LOCAL_MACHINE\SYSTEM key in the registry.
Specify auditing on the Full Control permission for Everyone.
E. Configure the SACL on the HKEY_LOCAL_MACHINE\SYSTEM key in the registry.
Specify auditing on the Set Value permission for Everyone.

Answer: A, D

Explanation: Audit object access - This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified.

Assign permissions to files, folders, and registry keys

Appropriate object manager and Properties page

Access control is the model for implementing authorization. Once a user account has received authentication and can access an object, the type of access granted is determined by either the user rights that are assigned to the user or the permissions that are attached to the object. For objects within a domain, the object manager for that object type enforces access control. For example, the registry enforces access control on registry keys. Every object controlled by an object manager has an owner, a set of permissions that apply to specific users or groups, and auditing information. By setting the permissions on an object, the owner of the object controls which users and groups on the network are allowed to access the object. The permission settings also define what type of access is allowed (such as read/write permission for a file). The auditing information defines which users or groups are audited when attempting to access that object.

Thus you need to enable auditing in the local security policy on Certkiller 1 and select the Audit object access (Success and failure) and then configure the SACL on the HKEY_LOCAL_MACHINE\SYSTEM key in the registry and specify the Full Control permission for Everyone.

Incorrect answers:

B: Enabling auditing in the local security policy of Certkiller 1 is correct, but you should select to Audit object access (success and failure) and not the Audit privilege use (success and failure) as this option will not yield the information needed to check when unauthorized changes are made in the registry on Certkiller 1. Audit Privilege Use tracks each instance of a user exercising a user right.

C: Audit System Events tracks system events such as shutting down or restarting the computer, as well as events that relate to the security log within Event Viewer. You need to audit object access not audit systems events.

E: This option is correct up to the point where it suggests that you specify auditing on the Set Value permission for everyone. This part is wrong because you need to set the auditing on the Full Control permission rather.

Reference:

James Chellis, Paul Robichaux and and Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 115

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 754, 752

QUESTION 554

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain that contains the organizational units (OUs) shown in the work are below. The network contains Windows Server 2003 computers, Windows XP Professional computers, Windows NT Workstation 4.0 computers, and Windows Millennium Edition computers.

An update to the written company security policy states that the NTLMv2 and Kerberos protocols must be the only protocols that are used to authenticate logons to all computers.

You need to configure security settings by using the appropriate security template to ensure that only the NTLMv2 and Kerberos protocols are used when users log on to the domain. You want to link the

minimum number of Group Policy objects (GPOs) to accomplish this goal.
What should you do?
To answer, drag the appropriate .inf template or template to the correct OU or OUs.

Answer:

Explanation: The Secure templates define enhanced security settings that are least likely to impact application compatibility. For instance, the Security templates define stronger password, lockout, and audit settings. In addition to this, the Security templates limit the use of LAN Manager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LAN Manager responses.
The securews.inf template is used to increase security on workstations and servers, not to restore root file system permissions. This is why it is applied to Certkiller .com. The securedc.inf template on the other hand is applied to domain controllers.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291) Chapter 4
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. 798

QUESTION 555
You are an administrator of an Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are joined to the domain.
Certkiller has a main office and five branch offices. At one of Certkiller 's branch offices, a network administrator named John uses Remote Desktop to assign the Secure Server (Require Security) IPSec policy to a domain controller named DC2. Users report that they cannot access resources on DC2.
John reports that he can no longer establish a Remote Desktop connection to DC2.
On a client computer named Certkiller 1 in the branch office, you run the ping dc2 command and receive a reply. You do not have physical access to DC2.
You want to restore access to resources on DC2 for all users. You need to make all configuration changes remotely.
Which two actions should you perform on Certkiller 1? (Each correct answer presents part of the solution. Choose two)

A. Use the Services console to connect to DC2 and stop the IPSec Services service.
B. Use IP Security Monitor to connect to DC2.
C. Run the net stop "ipsec services" command.
D. Install an IPSec certificate in the local machine store.
E. Assign the Client (Respond only) IPSec policy.

Answer: A, E.

Explanation: IPSec has predefined security policies that can be implemented via the IP Security Policy Management console. A security policy can be described as a set of rules and filters that provide a level of security. In this scenario, the Secure Server (Require Security) policy was assigned to DC2. This means that all IP communication to or from DC2 must use IPSec. The result being that all DNS, web requests and all else which uses an IP connection must either be secured with IPSec or is simply blocked. To solve this issue, first use the Services console to connect to DC2 and stop the IPSec Services service. Next, assign the Client (Respond only) IPSec policy. This policy specifies that a Windows 2000, XP, or a Windows Server 2003 IPSec client will negotiate IPSec security with a peer that supports it - it will not try to initiate security. It accepts IPSec when the remote end requires it.
Incorrect Answers:
B: IP Security Monitor is to assist you with the standard monitoring of IPSec.
C: Running the net stop "ipsec services" command does not ensure that you will be able to connect to the remote desktop.
D: IPSec certificate installation in the local machine store is not going to help you to accomplish your task of enabling access to resources 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, p. 871
Zacker, Craig, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network, Microsoft Press, Redmond, 2003, Chapter 12, pp. 628 - 629

QUESTION 556
You are the network administrator for Certkiller .com. All servers run Windows Server 2003. All

client computers run Windows XP Professional.

Software Update Services (SUS) is installed on a computer named Certkiller 1. All client computers are configured to receive their software updates from Certkiller 1 by using a Group Policy object (GPO). Users report that when client computers receive updates through SUS, they are prompted to restart the computers. Users do not have the option to delay restating, and they report that restarting during business hours decreases their productivity.

You need to ensure that users have the option to delay restarting their computers after updates are received.

What should you do?

A. Enable the Remove access to use all Windows Update features GPO setting.
B. Disable the Remove access to use all Windows Update features GPO setting.
C. Assign users the Shut down the system user right in the local security policy.
D. Assign users the Act as part of the operating system user right in the local security policy.

Answer: C

Explanation: The folders in Local Policies are Audit Policy, User Rights and Security Options. User Rights in this context refer to system access rather than resource access. They determine which rights a user has on a computer. Assigning users the Shut down the system user right in the local security policy would allow the users to shut down local Windows Server 2003 computers. This would enable users to delay restarting their computers after updates are received.

Incorrect Answers:
A: Enabling the Remove access to use all Windows Update features will not grant users the right to shut down or delay shut down when their systems are updated.
B: Neither will disabling the Remove access to use all Windows Update features.
D: The Act as part of the operating system user right will be applied from the correct location, but it will be the wrong right 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, Chapter 11, pp. 654, 796

QUESTION 557
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains 20 Windows Server 2003 computers and 4,000 Windows XP Professional computers.

The written Certkiller security policy states that all servers must always have the most current security updates. The policy also states that all security updates must be tested in a lab before they are installed on production servers.

You need to find out whether domain servers have all available security updates and service packs.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Install Microsoft Baseline Security Analyzer (MBSA) on a server.
Configure MBSA to check for Windows vulnerabilities and to scan the range of IP addresses for all

servers.
B. Install Microsoft Baseline Security Analyzer (MBSA) on a server.
From a command prompt on the server, run the mbsacli.exe command.
C. On each server, connect to the Windows Update Web site.
Scan for and install security updates for Windows Server 2003 computers.
D. Configure the Automatic Updates client on all servers to automatically download and install security updates.

Answer: A, B

Explanation: Microsoft Baseline Security Analyzer (MBSA) is the utility that can be used to ensure that you have the most current security updates. You can use the MBSA to verify whether domain servers have all available security updates and service packs. The options for a scan include Check For Windows Vulnerabilities, Check For Weak Passwords, Check For IIS Vulnerabilities, Check For SQL Vulnerabilities and Check For Security Updates. Once the scan is completed, a report is accessible for each machine that was scanned.
Incorrect Answers:
C: Scanning and installing all security updates in this fashion will make the rule of only installing approved and tested updates a farce especially if it is done directly from the Microsoft Windows Web site.
D: Automatically downloading updates will install all types of updates and not just approved and tested updates that were made available. Besides this option does not mention from where the updates are to be downloaded automatically.
Reference:
Zacker, Craig, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network, Microsoft Press, Redmond, 2003, Chapter 13, p. 659

QUESTION 558
You are the network administrator for Certkiller .com. All servers run Windows Server 2003.
Two Web servers named Certkiller 1 and Certkiller 2 host Certkiller 's public Web site. Both servers share the same Web content.
The Web files on Certkiller 1 are modified inadvertently. After reviewing the NTFS file system security on Certkiller 1 and Certkiller 2, you decide that the NTFS file system security on Certkiller 1 should be modified to match the NTFS file system security on Certkiller 2.
You want to modify the NTFS file system permissions on Certkiller 1 to be the same as those on Certkiller 2. You also want to be able to reproduce these NTFS file system permissions to new Web servers in the future by using the minimum amount of administrative effort.
What should you do?

A. Export the security settings from Certkiller 1 to a security template.
Import the security template to Certkiller 2.
B. Import the Rootsec.inf security template to Certkiller 2.
C. Create a new security template and manually define the file system security.
Import the security template to Certkiller 1.
D. Run the ldifde command to modify the computer object.

Answer: A

Explanation: A security template contains configuration parameters for various operating system settings for different server types. To apply the NTFS file system permissions to Certkiller 2 and new Web servers, exporting the security settings from Certkiller 1 to a security template is the most feasible solution. You can then utilize the Security Configuration and Analysis MMC snap-in to apply the particular security template to local machines.

Incorrect Answers:

B: The rootsec.inf security template is used to restore permissions on the root file system. You would need the other .inf files as well for this scenario.

C: Creating a new security template is not the same as making use of the Certkiller 1 security settings and importing it to the Certkiller 2 security template.

D: The ldifde (LDIF Directory Exchange) command can be used to create, modify, and delete directory objects on Windows Server 2000, Windows Server 2003 and Windows XP Professional. However, in this scenario it is not applicable.

Reference:

Dan Holme and Thomas Orin, MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, 2003, pp 3-16, 3-20, 4-13, 13-6.

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, Chapter 11, pp. 651-659, 791-793

QUESTION 559

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

You configure the security settings for all servers by using a security template named Corpsec.inf.

After a recent security breach on a member server named Certkiller 2, you notice that the security settings are no longer configured as expected.

You want to analyze all the security settings on Certkiller 2 that do not match the security settings in the Corpsec.inf template.

What should you do?

A. Import Corpsec.inf into the security settings on Certkiller 2 by using the Local Security Policy console.

B. Import Corpsec.inf into a new security database by using the Security Configuration and Analysis console.

C. Run the dsquery.exe computer command.

D. Import Corpsec.inf into the security settings of the Default Domain Policy Group Policy object (GPO).

Answer: B

Explanation: Windows Server 2003 includes the Security Configuration and Analysis tool MMC snap-in. You can use it to analyze the local security settings of a computer. The Security Configuration and Analysis tool is able to compare your actual security configuration to the security template Corpsec.inf, configured with your required settings. In the Security Configuration and Analysis tool, you indicate a security database that will be used for the security analysis. You import the security template (Corpsec.inf) that can be used as

a basis for the manner in which you want your security configured. You then perform the security analysis, and evaluate your configuration against the security template specified previously.

Incorrect Answers:

A: The Corpsec.inf template should be imported into the security database and not the security settings. The database is being used for the security analysis.

C: Running the dsquery.exe computer command finds computers in the directory and is thus not applicable in this case.

D: The template should be imported into a new database and not into the security settings of the GPO.

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. 269

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. 651-657

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, Chapter 11, p. 657

QUESTION 560

You are the network administrator for Certkiller .com. The network contains Windows Server 2003 domain controllers, Windows Server 2003 member servers, and Windows XP Professional computers. The network security administrator creates a new Group Policy object (GPO) to configure security settings for computers in the accounting department.

You need to ensure that this GPO takes affect as soon as possible on five member servers in the accounting department.

What should you do?

A. On each member server, run the secedit command.
B. On each member server, run the gpupdate command.
C. On each domain controller, run the gpresult command.
D. On each domain controller, run the dcgprofix command.

Answer: B

Explanation: By default, group policies are applied each 90 minutes to computers. Typing gpupdate at the command prompt would ensure that the new GPO takes affect as soon as possible. This would force an update of the new security policy.

Incorrect Answers:

A: The secedit command provides a command line interface to analyze, modify, and apply security templates. However, this has been replaced by the gpupdate command.

C: The gpresult command displays the Resultant Set of Policy (RSoP) information for a target user and computer.

D: The dcgprofix command is not used to make GPOs take effect immediately after being modified.

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, p. 795
Jill Spealman, Kurt Hudson, and Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Chapter 10, p. 610
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, Rockland, 2003, p. 270

QUESTION 561
You are the administrator of an Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
A server named Certkiller 1 contains confidential data that is only available to users in the human resources (HR) department.
You want all computers in the HR department to connect to Certkiller 1 by using an IPSec policy. You assign the Server (Request Security) IPsec policy for Certkiller 1. Using Network Monitor, you notice that some computers in the HR department connect to Certkiller 1 without using the IPSec policy.
You need to configure Certkiller 1 to ensure that all computers connect to it by using the IPSec policy. What should you do?

A. Assign the Secure Server (Require Security) IPSec policy.
B. Assign the Client (Respond Only) IPSec policy.
C. Unassign the Server (Request Security) IPSec policy.
D. Restart the IPSec Services service.

Answer: A

Explanation: The Secure Server (Require Security) policy specifies that all IP traffic must use IPSec. The Secure Server (Require Security) default policy is ideal for Certkiller 1 that needs high security. When this option is selected, the server requires all communications to be secure. If a client is not IPSec-aware, the session will not be allowed.
Incorrect Answers:
B: Assigning the Client (Respond Only) IPSec policy on Certkiller 1 will not ensure that all computers that connect need to employ IPSec policy. This setting 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.
C: Unassigning the Server (Request Security) IPSec policy will defeat the purpose of having all computers that connect using the IPSec policy. This 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.
D: Restarting IPSec Services service will not ensure that all connecting computers are IPSec aware.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapters 4 & 5
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. 867-868

Zacker, Craig, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network, Microsoft Press, Redmond, 2003, p. 629

QUESTION 562

You are a 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	Internal IP	External IP	Server role	Applications and services Installed
Name	Address	Address		
Certkiller 1	192.168.2.1	N/A	Web server	Network Monitor, IIS 6.0
Certkiller 2	192.168.2.2	131.107.0.1	ISA Server Computer	Network Monitor, ISA Server 2000

You need to use Network Monitor to find out which client computers are infected by the virus. What should you do?
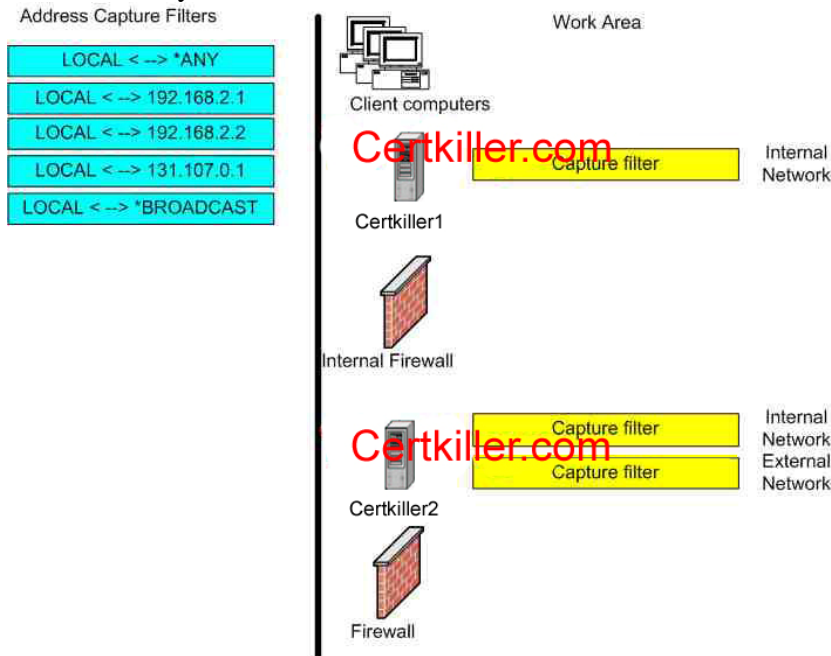
Answer:
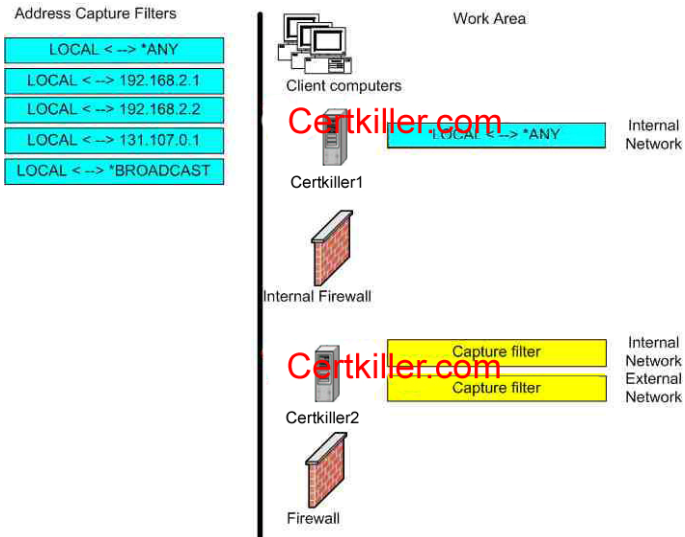
Explanation: Capture filters allow you to isolate data transmitted to and from your machine on the network. The arrow should be both directions (LOCAL <-> * ANY) in this instance so that traffic in both directions can be monitored to isolate the client computers that are infected by the virus. Capture filters will enable you to specify the type of information that is captured.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 6

QUESTION 563
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com.
The domain contains an organizational unit (OU) named Webservers. The Webservers OU contains the computer accounts of 12 Windows Server 2003 computers that function as intranet Web servers. A Group Policy object (GPO) named WebserverPolicy is linked to the Webservers OU. The GPO is used to configure various settings on the computers in the OU. A global group named WebserverAdmins is a member of the Administrators local group on each intranet Web server.
You plan to install a security scanning application on each intranet Web server. The documentation for the application states that it uses a service account, which must be able to modify the HKEY_LOCAL_MACHINE\SYSTEM key in the registry of every computer on which the application is installed.
You create the service account in the domain. Certkiller 's written security policy states that service accounts must be assigned only the minimum rights and permissions that they require to function.
You need to configure the intranet Web servers so that they comply with the installation requirements of the security scanning application. You also need to comply with Certkiller 's security policy. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Add the service account to the WebserverAdmins global group.
B. Configure the required permissions as registry security settings in the WebserversPolicy GPO.
C. Run the regedit.exe command to add the required permissions to the registry of each intranet Web server.

D. Run the explorer.exe command to modify NTFS permissions on the
Systemroot\System32\Config\System file.
Assign the service account the Allow - Change permission.
E. Configure file system security settings in the WebserversPolicy GPO to modify NTFS permissions
on the Systemroot\System32\Config\System file.
Assign the service account the Allow - Change permission.

Answer: B

Explanation: Security templates contain security settings for all security areas. You can apply templates to
individual computers or deploy them to groups of computers by using Group Policy. When you apply a
template to existing security settings, the settings in the template are merged into the computers security
settings. You can configure and analyze security settings for computers by using the Security Settings Group
Policy extension or Security Configuration and Analysis. You can change many things with security
templates; one of which is registry settings. You use registry settings to configure security on registry keys.
This solution uses the minimum amount of administrative effort. To accomplish this task with the minimum
administrative effort, you can make use of the Registry Editor Regedit.exe to add the required permissions
to the registry of each intranet Web server in the following subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface
Incorrect Answers:
A: By adding the service account to the WebserverAdmins global group you will not be able to comply
with the company's security policy.
C: Adding the required permissions to the registry of each intranet webserver is not the answer in this
scenario.
D: Modifying the NTFS permissions on the Systemroot\System32\Config\System file by running the
explorer.exe to assign the Allow-Change permission is not what is needed when security policy states
that service accounts must be assigned only the minimum rights and permissions that they require to
function with the minimum amount of administrative effort.
E: Configuring file system security settings to suit the company security policy as described in this option
will require more administrative effort than is necessary.
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. 1: 17.

QUESTION 564
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain named Certkiller .com. The domain contains 10 Windows Server 2003 computers and
1,000 Windows XP Professional computers. All client computers are in the Clients organizational unit
(OU). You create and link a Group Policy object (GPO) named ClientConfig to the Clients OU.
The written company security policy states that all Windows XP Professional computers must have
identical security settings for user rights assignment and security options.
You need to deploy these settings to all Windows XP Professional computers in the domain. You need
to accomplish this task with the minimum amount of administrative effort.
What should you do?

A. Run Microsoft Baseline Security Analyzer (MBSA) on a server and scan all computers in the domain.
B. Use the Local Security Policy console on each Windows XP Professional computer to apply the identical security settings.
C. Create a logon script that runs the Gpupdate /target:computer command on all Windows XP Professional computers in the domain.
D. Create a custom security template that contains the settings.
Import the security template into the Clientconfig GPO.

Answer: D

Explanation: A Group Policy Object (GPO) is a collection of policies stored in two locations: a Group Policy container (GPC) and a Group Policy template (GPT). The GPC is an Active Directory object that stores version information, status information, and other policy information (for example, application objects).
A security template is a collection of configured security settings. Windows Server 2003 provides predefined security templates that contain the recommended security settings for different situations. You can use predefined security templates to create security policies that are customized to meet different organizational requirements. You customize the templates with the Security Templates snap-in. After you customize the predefined security templates, you can use them to configure security on an individual computer or thousands of computers.
You can configure individual computers with the Security Configuration and Analysis snap-in or the secedit command-line tool or by importing the template into Local Security Policy. You can configure multiple computers by importing a template into Security Settings, which is an extension of Group Policy. You can also use a security template as a baseline for analyzing a system for potential security holes or policy violations by using the Security Configuration and Analysis snap-in. By default, the predefined security templates are stored in systemroot/Security/Templates. Thus to create a custom security template that contains the settings and to minimize the administrative effort and time this task can take, all you need to do is to modify the appropriate GPO. Import the security template into the Clientconfig GPO.
Incorrect Answers:
A: Scanning all computers in the domain by running Microsoft Baseline Security Analyzer (MBSA) on a server is not the way to see whether all Windows XP Professional computers must have identical security settings for user rights assignment and security options.
B: Applying identical security settings by making use of the Local Security Policy console on each Windows XP Professional computer involves too much administrative effort than is necessary to comply with the company policy.
C: Writing a logon script to run the Gpupdate /target:computer command on all Windows XP Professional computers in the domain will only accomplish the task on a per user basis whereas you could have just imported the appropriately modified GPO.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 4

QUESTION 565
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 domain controllers, Windows Server 2003 member servers, and Windows XP Professional computers.

The security administrator creates a new security policy, which states that auditing must be enabled for all user logon attempts. The security policy also states that a security event must be generated every time a computer is successfully shut down.
You need to configure auditing for the domain to comply with the new security policy. You do not want to generate any other type of security event.
What should you do?

Audit Policy Settings

Success

Failure

Success, Failure

Policies

Scripts (Startup/Shutdown)
Security Settings
  Account Policies
  Local Policies
    Audit Policy
    User Rights Assignment
    Security Options
  Event Log
  Restricted Groups
  System Services
  Registry
  File System
  Wireless Network (IEEE 802.11
  Public Key Policies
  Software Restriction Policies

Audit account management — Place here
Audit directory service access — Place here
Audit Logon events — Place here
Audit object access — Place here
Audit policy change — Place here
Audit privilege use — Place here
Audit process tracking — Place here

Certkiller.com

Answer:

Audit Policy Settings

Success

Failure

Success, Failure

Policies

Scripts (Startup/Shutdown)
Security Settings
  Account Policies
  Local Policies
    Audit Policy
    User Rights Assignment
    Security Options
  Event Log
  Restricted Groups
  System Services
  Registry
  File System
  Wireless Network (IEEE 802.11
  Public Key Policies
  Software Restriction Policies

Audit account management — Place here
Audit directory service access — Place here
Audit Logon events — Success, Failure
Audit object access — Place here
Audit policy change — Place here
Audit privilege use — Success
Audit process tracking — Place here

Certkiller.com

Explanation:
Audit logon events: Determines whether to audit each instance of a user logging on, logging off, or making a network connection to this computer.
Audit privileged use: Determines whether to audit each instance of a user exercising a user right
Incorrect answers:
Audit object access: Determines whether to audit the event of a user accessing an object, such as a file, folder, registry key, or printer, which has its own system access control list (SACL) has specified.
Audit policy change: Determines whether to audit every incidence of a change to user rights assignment policies, audit policies, or trust policies.
Audit process Tracking: Determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.
Audit system events: Determines whether to audit when a user restarts or shuts down the computer; or an event which has occurred that affects either system security or the security log.
Audit directory service access: Determines whether to audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified.
Audit account management: Determines whether to audit each event of account management on a computer. Examples of account management events include:
• A user account or group is created, changed, or deleted.

• A user account is renamed, disabled, or enabled.
• A password is set or changed.
Audit account logon events: Determines whether to audit each instance of a user logging on or logging off of another computer where this computer was used to validate the account (mostly domain controllers).
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. 871

QUESTION 566
You are the network administrator for Certkiller .com. The company consists of a main office and five branch offices. Network servers are installed in each office. All servers run Windows Server 2003.
The technical support staff is located in the main office. Users in the branch offices do not have the Log on locally right on local servers.
Servers in the branch offices collect auditing information.
You need to ability to review the auditing information located on each branch office server while you are working at the main office. You also need to save the auditing information on each branch office server in the local hard disk.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. From the Security Configuration and Analysis snap-in, save the appropriate .inf file on the local hard disk.
B. Solicit Remote Assistance from each branch office server.
C. From Computer Management, open Event Viewer.
Save the appropriate .evt file on the local hard disk.
D. Run Secedit.exe, specifying the appropriate parameters.
E. Establish a Remote Desktop client session with each branch office server.

Answer: C, E

Explanation: You can connect to the branch office servers by using a Remote Desktop connection. You can then use Event Viewer to save the log files to the local hard disk.
Incorrect Answers:
A: Auditing information is not stored in .inf files. E.g. rootsec.inf security template is used to restore permissions on the root file system; securews.inf security template is used to supply increased security over a standard installation for workstations. The setup security.inf security template provide configuration equivalent to a default installation, etc.
B: You do not need remote assistance. You can use a Remote Desktop client session.
D: Secedit is not used to save auditing information. It is used to enforce a group policy.
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. 791-793

QUESTION 567
You are the network administrator for Certkiller . 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 Default Domain Policy has been modified by importing a security template file, which contain several security settings.
A server named Certkiller 1 cannot run a program that us functioning on other similarly configured servers. You need to find out whether additional security settings have been added to the local security policy on Certkiller 1.
To troubleshoot, you want to use a tool to compare the current security settings on Certkiller 1 against the security template file in order to automatically identify any settings that might have been added to the local security policy.
Which tool should you run on Certkiller 1?

A. Microsoft Baseline Security Analyzer (MBSA)
B. Security Configuration and Analysis console
C. gpresult.exe
D. Resultant Set of Policy console in planning mode

Answer: B

Explanation: You can use the Security Configuration and Analysis console to analyse a system by comparing the local security settings to a template. When you analyse a system, any differences in configuration between the local computer and the defined template will be displayed.
Security Configuration and Analysis tool is used to compare the current security configuration with a security configuration that is stored in a database. You can create a database that contains a preferred level of security and then run an analysis that compares the current configuration to the settings in the database.
Security Configuration and Analysis includes the following features:
• Security Templates
• Security Configuration and Analysis
• Secedit command-line command
To analyze the security configuration of your computer, you must perform the following two steps:
• Create the security database by using a security template
• Compare the computer security analysis to the database settings.
Incorrect Answers:
A: The MBSA is used to check for missing security updates as well as other security vulnerabilities. It will not however compare the security settings with a defined template.
C: GPresult.exe is used to display the resultant set of policies when multiple group policies are applied to an object. However, it is not applicable to this scenario.
D: This is similar to answer C. It will display what the resultant set of policies would be if multiple group policies were applied to an object, without actually applying the group policies.
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. 797, 868

QUESTION 568
You are the network security 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.
The human resources department stores confidential data on a server named Certkiller B. The written
company security policy states that TCP/IP traffic sent to and from Certkiller B must be encrypted.
You need to encrypt all TCP/IP traffic that is sent between Certkiller B and the client computers in the
human resources department.
What should you do?

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

Answer: D

Explanation: IPSEC for High security - Computers that contain highly sensitive data are at risk for data
theft, accidental or malicious disruption of the system (especially in remote dial-up scenarios), or any public
network communications.
Secure Server (Require Security) is a default policy, requires IPSec protection for all traffic being sent or
received (except initial inbound communication) with stronger security methods. Unsecured communication
with a non-IPSec-aware computer is not allowed.
Assigning the Client IPSec policy to all client computers in the human resources department will enable the
clients to communicate with Certkiller B using IPSec.
Incorrect Answers:
A: Providing certificates does not automatically provide encryption. You would thus not be able to
accomplish your task.
B: Providing certificates does not automatically provide encryption. It is a different process.
C: EFS encrypts and protects data at rest, the requirement is protecting data in transit.
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. 586

QUESTION 569
You are the administrator of an Active Directory domain named Certkiller .com. All servers run
Windows Server 2003. All client computers run Windows XP Professional.
An unauthorized file sharing application named Fileshare.exe is being used on your network. The
default installation directory for Fileshare.exe is C:\Program Files\File Share\.
You need to prevent all users from using the unauthorized file sharing application, even if they
rename the application.
You create a new software restriction policy in the Default Domain Policy Group Policy object (GPO).

You now need to configure the software restriction policy.
What should you do?

A. Create a new path rule for Fileshare.exe. Set the security level to Disallowed for the new rule.
B. Create a new hash rule for Fileshare.exe. Set the security level to Disallowed for the new rule.
C. Create a new path rule for C:\Program Files\File Share\. Set the security level to Disallowed for the new rule.
D. Set the default security level to Disallowed for the software restriction policy.

Answer: B

Explanation: When you create a hash rule, you identify a specific file to which you want the rule to apply, and the system generates a hash on the file, including attributes such as date and time of creation and file size. After the policy is in place, the system performs a hash on each file accessed, and if the hash matches the hash in the rule, the rule is applied. Since several rules can be applied to the same program, there is an established order of precedence that is applied. A rule based on a higher precedence will override a conflicting rule applied with a lower precedence. Take for example the following order:
1. Hash rule
2. Certificate rule
3. Path rule
4. Internet zone rule
Based on this order, if a program is unrestricted based on a hash rule but disallowed based on a path rule, the program will run, as the hash rule has precedence over the path rule. For path rules, there is an additional order of precedence based on the path specified. If there are conflicting path rules, the more restrictive path rule will apply.
Incorrect answers:
A: When you create a path rule, you identify a file or set of files based on their location on disk. The path can identify the path to a folder, a specific file, or a set of files based on a wildcard. When the system processes a file request when path rules are in place, it will compare the file requested to the path rules, and process the rule if there is a match. This is not what is needed.
C: Creating a path rule is wrong; furthermore the rule should be for the Fileshare.exe and not C:\Program Files\File Share\.
D: This is irrelevant.
Reference:
Michael Cross and Jeffery
A. Martin, MCSE Exam 70-294: Planning, Implementing, and Maintaining a
Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, Syngress
Publishing, Rockland, 2003, p. 617

QUESTION 570
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain Certkiller .com. The domain contains 35 Windows Server 2003 computers; 3,000
Windows XP Professional computers; 2,200 Windows 2000 Professional computers.
The written company security policy states that all computers in the domain must be examined, with
the following goals:
• To find out whether all available security updates are present.

• To find out whether shared folders are present.
• To record the file system type on each hard disk.
You need to provide this security assessment of every computer and verify that the requirements of the written security policy are met.
What should you do?

A. Open the Default Domain Policy and enable the Configure Automatic Updates policy.
B. Open the Default Domain Policy and enable the Audit object access policy, the Audit account management policy, and the Audit system events policy.
C. On a server, install and run mbsacli.exe with the appropriate configuration switches.
D. On a server, install and run HFNetChk.exe with the appropriate configuration switches.

Answer: C

Explanation: The Microsoft Baseline Security Analyser can perform all the required assessments.
Mbsacli.exe includes HFNetChk.exe which is used to scan for missing security updates.
In general, the MBSA scans for security issues in the Windows operating systems (Windows NT 4, Windows 2000, Windows XP), such as Guest account status, file system type, available file shares, and members of the Administrators group, etc. Descriptions of each OS check are shown in the security reports with instructions on fixing any issues found.
Incorrect Answers:
A: This would not check for missing updates, shared folders or file system type.
B: This would not check for missing updates, shared folders or file system type.
D: This would check for missing updates but not for shared folders or file system type.
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, pp. 788-790
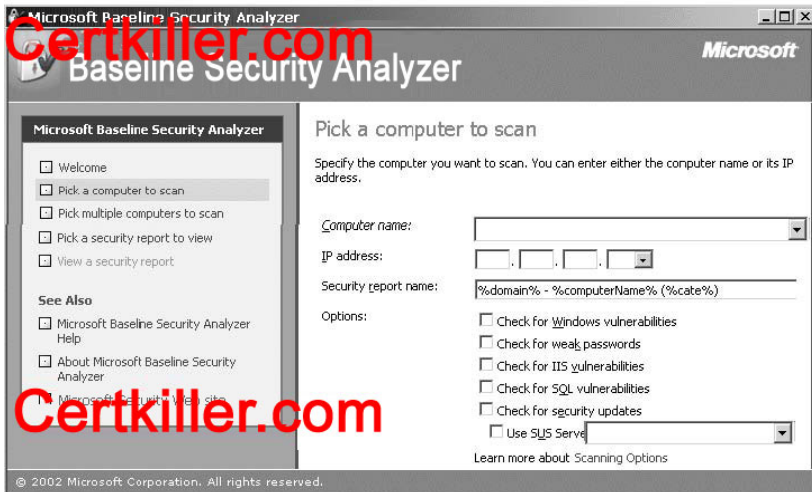
QUESTION 571
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
The written Certkiller .com security policy states that unnecessary services must be disabled and that servers must have the most recent, company-approved security updates. You install and configure Software Update Services (SUS) on a server named Certkiller 7. Certkiller 6 is used only as a file and printer server. Certkiller 7 has two local user accounts; and the administrator account has been renamed.
You need to find out whether Certkiller 7 is running unnecessary services and whether it has all available approved security updates. To reduce the amount of network bandwidth and time requirements, you need to scan for only the required information.
What should you do?
To answer configure the appropriate option or options.

Answer:

QUESTION 572
You install Windows Server 2003 on a computer named Certkiller 2. Certkiller 2 will host a missioncritical application. The system engineer asks you to monitor Certkiller 2 to ensure reliability and availability.
You assign a computer maintenance engineer named Kim to assist you in maintaining Certkiller 2.
Kim will have the following responsibilities on Certkiller 2:
• Use Event Viewer to monitor all events logs except the security logs.
• Use Performance Logs and Alerts to create new performance logs.
You need to assign Kim only the minimum rights on Certkiller 2 that are required to perform these tasks. Kim must be able to perform the tasks locally or from another computer. To simplify administration, you must use the minimum number of groups required.
To which local built-in security group or groups should you assign Kim? (Choose all that apply)

A. Administrators
B. Performance Log Users
C. Performance Monitor Users
D. Power Users
E. Remote Desktop Users

Answer: B

Explanation: Performance Logs and Alerts provide logging and alert capabilities for both local and remote computers. You use logging for detailed analysis and recordkeeping. Retaining and analyzing log data that is collected over time can be helpful for capacity and upgrade planning. To perform this procedure, you must be a member of the Administrators group, or you must have been delegated the appropriate authority. If the computer is connected to a domain, members of the Domain Admins group might be able to perform this procedure. Performance Log Users members can manage performance counters, logs and alerts on the server locally and from remote clients without being a member of the Administrators group. Thus making Kim a member of the Performance log users will grant her enough permissions to complete her tasks without granting her membership to too many groups.

Incorrect Answers:

A: Administrators have the ability to provide both logging and alert capabilities for both local and remote computers. Kim will not be needing membership to this group as well. Being a member of the Performance Log Users is sufficient.

C: Performance Monitor users can monitor performance counters on the server locally and from remote clients without being a member of the Administrators or Performance Log Users groups.

D: Power Users membership will be too restrictive to allow Kim to complete her tasks.

E: Remote Desktop Users membership will not enable Kim to complete her tasks.

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. 783

QUESTION 573

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. Three thousand client computers run Windows 2000 Professional, and 1,500 client computers run Windows XP Professional.

A new employee named Dr King is hired to assist you in installing Windows XP Professional on 150 new client computers.

You need to ensure that Dr King has only the minimum permissions required to add new computer accounts to the domain and to own the accounts that he creates. Dr King must not be able to delete computer accounts.

What should you do?

A. Add Dr King's user account to the Server Operators group.

B. Add Dr King's user account to the Account Operators group.

C. Use the Delegation of Control Wizard to permit Dr King's user account to create new computer objects in the Computers container.

D. Create a Group Policy object (GPO) and link it to the domain.

Configure the GPO to permit Dr King's user account to add client computers to the domain.

Answer: C

Explanation: Active Directory enables you to efficiently manage objects by delegating administrative control of the objects. You can use the Delegation of Control Wizard and customized consoles in Microsoft Management Console (MMC) to grant specific users the permissions to perform various administrative and management tasks.

You use the Delegation of Control Wizard to select the user or group to which you want to delegate control. You also use the wizard to grant users permissions to control organizational units and objects and to access and modify objects.

The Delegation tab enables you to use the computer for delegation.

There are three choices for delegation:

• Do not trust this computer for delegation - This is the default for Windows Server 2003 machines.

• Trust this computer for delegation to any service (Kerberos only) - This option makes all services under the Local System account trusted for delegation. In other words, any installed service has the capability to access any network resource by impersonating a user.

• Trust this computer for delegation to specified services only - This feature was not available in previous versions of Windows. It enables an administrator to choose the services that are delegated by selecting a specific service or computer account. This is commonly referred to as constrained delegation.

Delegation of control can be done through the Delegation of Control Wizard or via Group Policy settings.

Incorrect answers:

A: The Server operators group has the following abilities: shut down the server from the console, restore files and directories from a backup devise, can change system time and date, and log on to the server console interactively, though the question only asks for the minimum permissions to add new computer accounts.

B: The account operators group has the following abilities: shut down the server from the console and log on to the server console interactively, though the question only asks for the minimum permissions to add new computer accounts

D: Creating a GPO and linking it to the domain will be obsolete in this case.

References:

Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 355, 441, 830.

QUESTION 574
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.

Confidential files are stored on a member server named CK1 . The computer object for CK1 resides in an organizational unit (OU) named Confidential. A Group Policy object (GPO) named GPO1 is linked to the Confidential OU.

To audit access to the confidential files, you enable auditing on all private folders on CK1 .

Several days later, you review the audit logs. You discover that auditing is not successful.

You need to ensure that auditing occurs successfully.

What should you do?

A. Start the System Event Notification Service (SENS) on CK1 .
B. Start the Error Reporting service on CK1 .
C. Modify the Default Domain Controllers GPO by selecting Success and Failure as the Audit Object Access setting.
D. Modify GPO1 by selecting Success and Failure as the Audit Object Access setting.

Answer: D

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

tab in that object's Properties dialog box.

We want to audit a server that resides in the Confidential OU. We do not want to audit domain controllers. Since GPO1 is linked to the confidential OU, it has to be modified as the Audit Object Access setting will be applicable to the confidential files.

Incorrect answers:

A: System Event Notification Service - Tracks system events such as Windows logon, network, and power events. It notifies COM+ Event System subscribers of these events.

B: Error Reporting Service - Allows error reporting for services and applications running in non-standard environments.

C: Modifying the Default Domain Controllers GPO by selecting Success and Failure as the Audit Object Access setting will not solve your problem as you need to monitor and modify the access setting to the confidential files. Also, we do not want to edit domain controllers.

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, 364

QUESTION 575

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

The network security administrator revises the written company security policy. The security policy now states that all computers must have the ability to audit any attempts to change the registry.

To comply with the company security policy, you need to enable auditing for the domain. You do not want to generate any other type of event that is not related to the changes in the security policy.
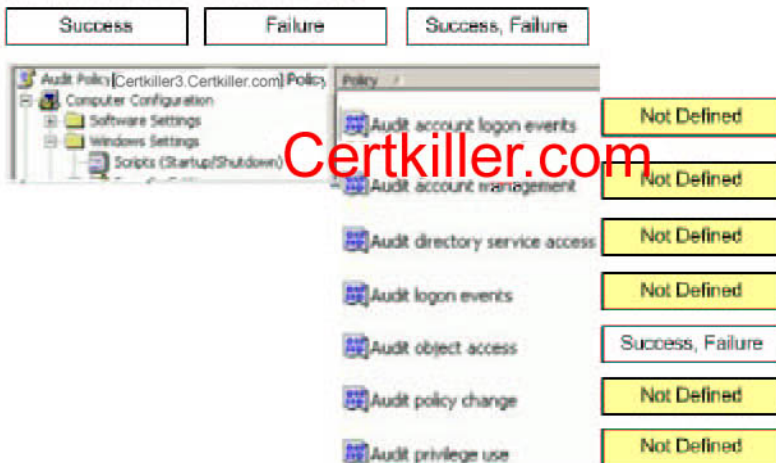
How should you configure auditing?

To answer, drag the appropriate Audit Policy setting or settings to the correct policy or polices.

Answer:

Audit Policy Settings, Select from these

Success	Failure	Success, Failure

Audit Policy [Certkiller3.Certkiller.com] Policy | Policy /
- Computer Configuration
  - Software Settings
  - Windows Settings
    - Scripts (Startup/Shutdown)

Certkiller.com

Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Success, Failure
Audit policy change	Not Defined
Audit privilege use	Not Defined

Drag and drop Success and Failure to Audit Object Access

Explanation: Audit object access - This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified.
Assign permissions to files, folders, and registry keys
Appropriate object manager and Properties page
Access control is the model for implementing authorization. Once a user account has received authentication and can access an object, the type of access granted is determined by either the user rights that are assigned to the user or the permissions that are attached to the object. For objects within a domain, the object manager for that object type enforces access control. For example, the registry enforces access control on registry keys.
Every object controlled by an object manager has an owner, a set of permissions that apply to specific users or groups, and auditing information. By setting the permissions on an object, the owner of the object controls which users and groups on the network are allowed to access the object. The permission settings also define what type of access is allowed (such as read/write permission for a file). The auditing information defines which users or groups are audited when attempting to access that object.
After setting the audit refresh the policy and enabling the setting for the everyone group on the regedit.exe you will be able to see any attempt to access.
References:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 754, 752

QUESTION 576
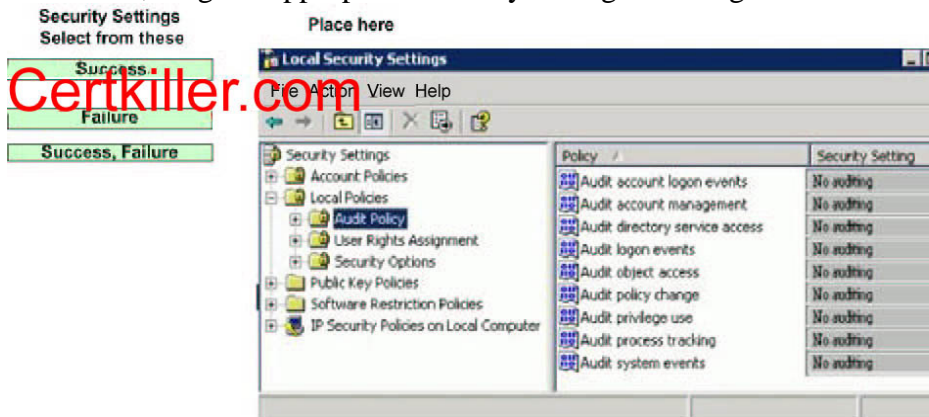You are the network administrator for Certkiller .
A server named Certkiller SrvC functions as a local file server. Certkiller SrvC contains several extremely confidential files.
The company's security department wants all attempts to access the confidential files on Certkiller SrvC to be recorded in a log.
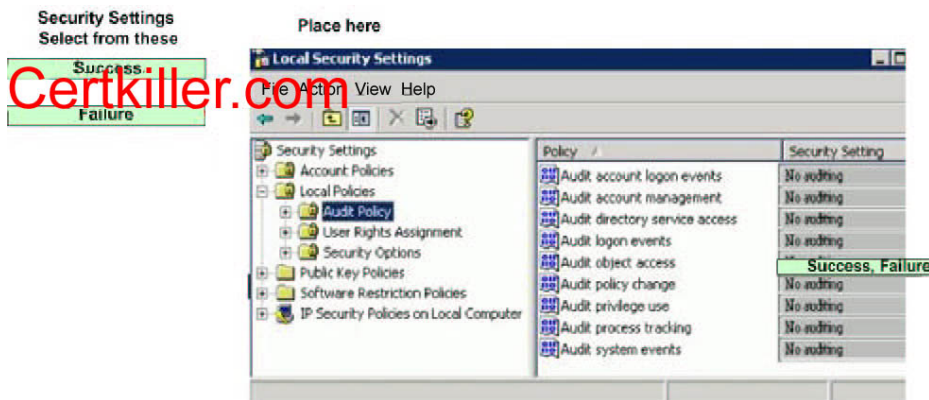You need to configure the local security policy on Certkiller SrvC to give you the ability to comply with the security department's requirements. No other auditing should be configured.
What should you do?

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

Answer:

Explanation: You should audit Success and Failure to log all attempts to access the files on Certkiller SrvC. The Audit object access policy setting determines whether the event of a user accessing an object such as a file, folder, registry key and printer; which has its own system access control list (SACL) specified, should be audited. You can configure whether to audit successes, audit failures, or not to audit the event type. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.
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, pp. 871-875

QUESTION 577
You are the network administrator for Certkiller . The network consists of a single Active Directory domain Certkiller .com. The domain contains Windows Server 2003 domain controllers and Windows XP Professional computers.
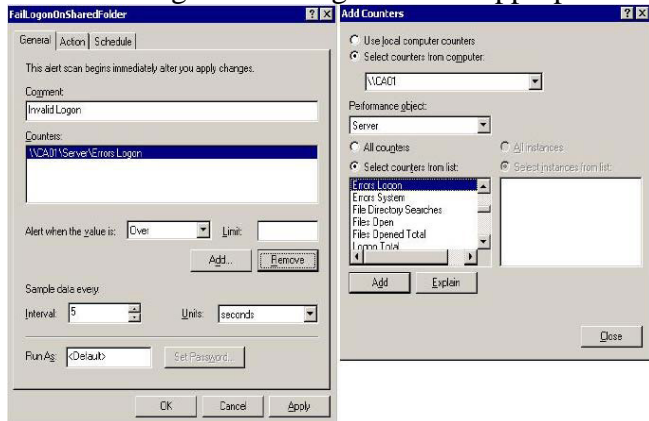A server named Certkiller Srv7 hosts a shared folder.
You want to use System Monitor to configure monitoring of the server performance object to alert you when invalid logon attempts are made to the shared folder. You want to monitor only events that are associated with invalid logons.

How should you configure the alert?
To answer, drag one or more appropriate instances of the server performance object to the alter interface.
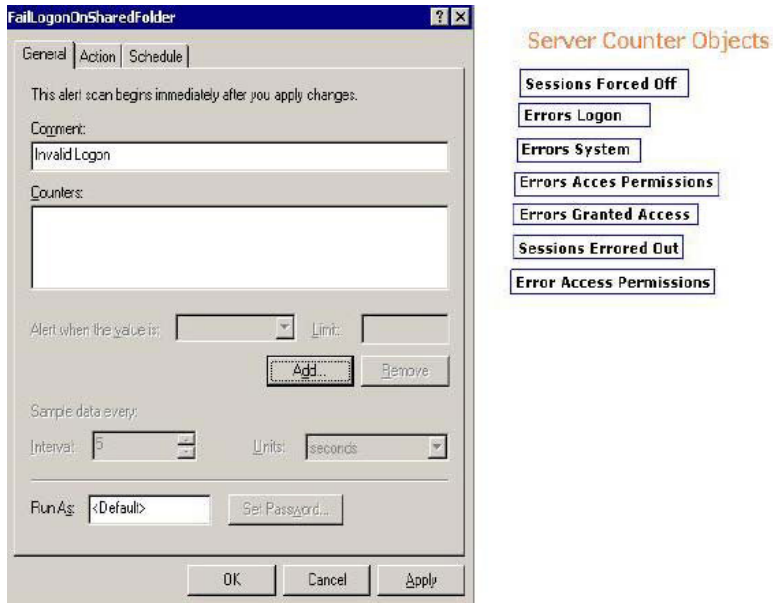
Answer: Drag "Errors Logon" to the appropriate location.

Explanation:
Server Object and Counter Errors Logon

Explanation: A user's credentials have to be validated when a UNC name is utilized to connect to a remote network resource. The UNC connection uses Server Messaging Blocks (SMBs) to work through the Multiple UNC Provider (MUP). A SMB, called SESSION SETUP and X, is used for the connection. At this point, the user's credentials are passed to the network resource. Validation occurs locally on the computer when the resource is a domain controller that maintains the user account.
A secure channel mechanism is utilized for user validation when the resource uses pass-through authentication.
The network resource requests a validation of the user from its domain controller. The domain controller returns an error to the network resource when the user's credentials are invalid and increments its usri3_bad_pw_count for the particular user. The network resource returns a message that has the NT status

code 0xC000006D, STATUS_LOGON_FAILURE, to the client workstation.
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. 634
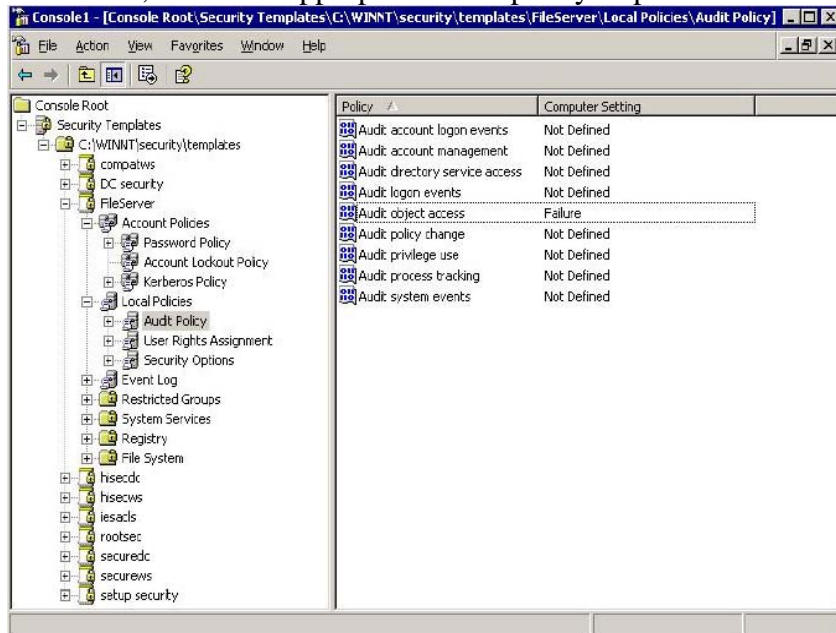

QUESTION 578

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

The written company security policy states that the audit policy on all file servers in the domain must have the ability to audit failure events for user access to files and folders. You create a custom security template named fileserver.

You need to configure the fileserver security template to enforce the written security policy of Certkiller for all file servers.
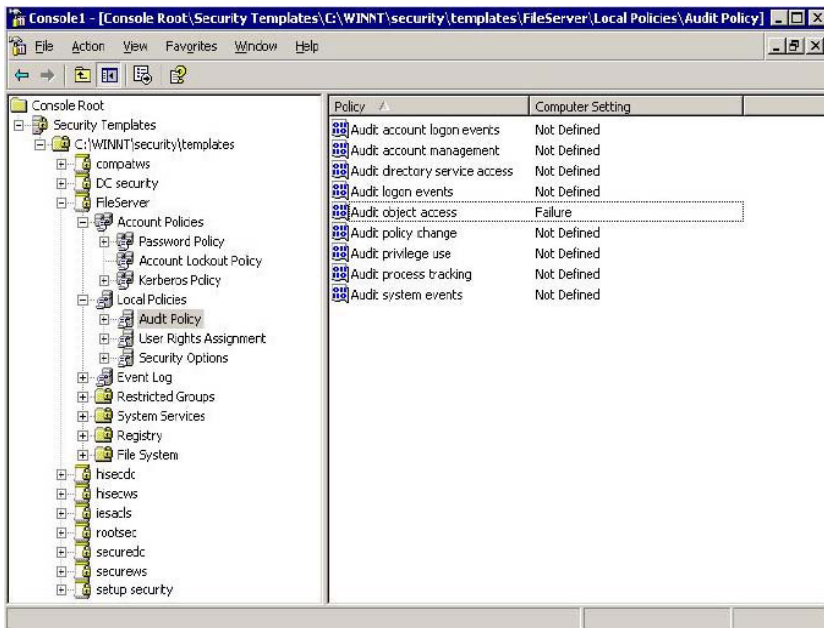
Which policy or polices should you modify?

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

Answer: Audit object access.

Take care in the exam not all the policies are in not defined state

Explanation: The Audit object access policy setting determines whether the event of a user accessing an object such as a file, folder, registry key and printer; which has its own system access control list (SACL) specified, should be audited.

You can set a SACL on a file system object by using the Security tab in the object's Properties dialog box. You can configure whether to audit successes, audit failures, or not to audit the event type. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.

To disable auditing, select the "Define these policy settings" check box in the Properties dialog box for this particular policy setting, and clear the Success and Failure check boxes.

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. 798

QUESTION 579

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows Server 2003 member servers, Windows Server 2003 domain controllers, and Windows XP Professional computers. The relevant portion of the Active Directory structure is in the work area below.

The written company security policy allows users to use Encryption File System (EFS) on only portable computers. The network security administrator creates a separate domain account as the data recover agent (DRA). The Default Domain Policy contains the Internet Explorer security settings that are required on all computers in the domain.

Users are currently able to use EFS on any computer that will support EFS.

You need to configure Group Policy to ensure compliance with the company security policy. You want to link the minimum number of GPOs to accomplish this goal. All other domain GPOs must remain.
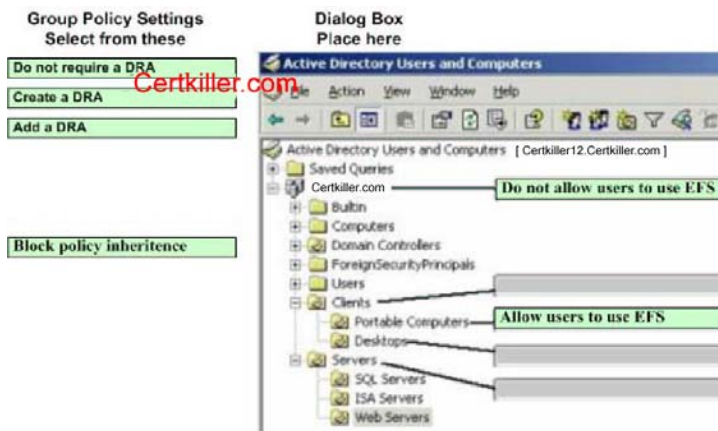
How should you configure Group Policy to ensure that users can use EFS on only portable

computers?

To answer, drag the appropriate Group Policy setting or settings to the correct organizational unit (OU) or OUs.
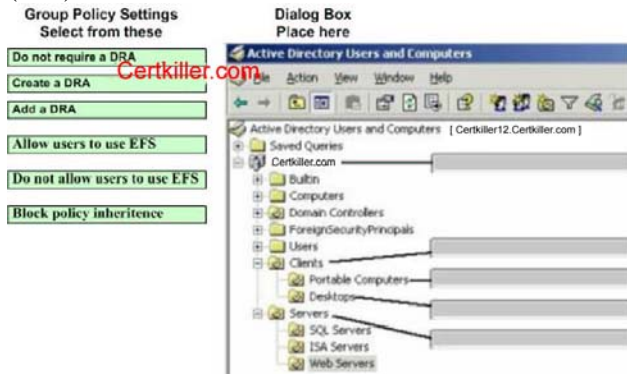
Answer:

Explanation:

The question does not ask to add a DRA option for the domain. The question states, "The network security administrator creates a separate domain account as the data recover agent (DRA)" so it has been created already and will permit to us to recover encrypted Data.

Set do not permit EFS to domain level and permit to the portable OU level.

By default:

GPO is referred to as "scoping the GPO". Scoping a GPO is based on three factors:

• The site(s), domain(s), or organization unit(s) where the GPO is linked.

• The security filtering on the GPO.

• The WMI filter on the GPO.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas

W. Shinder, Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 586

QUESTION 580

You are the regional network administrator for the Boston branch office of Certkiller 's network. The

company network consists of a single Active Directory domain Certkiller .com. All computers in the Boston office run Windows XP Professional.

The domain contains an organizational unit (OU) named BostonClientsOU, which contains all the computer objects for the Boston office. A Group Policy object (GPO) named BClientsGPO is linked to BostonClientsOU. You have been granted the right to modify the GPO.

BClientsGPO contains a software restriction policy that prevents the execution of any file that has a .vbs file extension. All other applications are allowed to run.

You want to use a script file named maintenance.vbs, which you will schedule to run every night on the computers in the Boston office. The maintenance.vbs file is located in the Scripts shared folder on a server named Certkiller SrvC. The contents of maintenance.vbs will frequently change based on the maintenance tasks you want to perform.

You need to modify the software restriction policy to prevent unauthorized .vbs scripts from running on the computers in the Boston office, while allowing maintenance.vbs to run. You want to ensure that no other applications are affected by your solution. You want to implement a solution that you can configure once, without requiring additional administration in the future, when maintenance.vbs changes.

What should you do?

A. Obtain a digital certificate.
Create a new certificate rule.
Set the security level of the rule to Unrestricted.
Digitally sign maintenance.vbs.
B. Create a new path rule.
Set the security level on the rule to Unrestricted.
Set the path to \\ Certkiller SrvC\Scripts*.vbs.
C. Create a new path rule.
Set the security level on the rule to Unrestricted.
Set the path to \\ Certkiller SrvC\Scripts\maintenance.vbs.
D. Create a new hash rule.
Set the security level on the rule to Unrestricted.
Create a file hash of maintenance.vbs.

Answer: C

Explanation: The file will change so we can only use a path rule. The purpose of a rule is to identify one or more software applications, and specify whether or not they are allowed to run. Creating rules largely consists of identifying software that is an exception to the default rule. Each rule can include descriptive text to help communicate why the rule was created.

A software restriction policy supports the following four ways to identify software:
Hash-A cryptographic fingerprint of the file.
Certificate-A software publisher certificate used to digitally sign a file.
Path-The local or universal naming convention (UNC) path of where the file is stored.
Zone-Internet Zone
A hash rule is a cryptographic fingerprint that uniquely identifies a file regardless of where it is accessed or what it is named. An administrator may not want users to run a particular version of a program. This may be the case if the program has security or privacy bugs, or compromises system stability. With a hash rule,

software can be renamed or moved into another location on a disk, but it will still match the hash rule because the rule is based on a cryptographic calculation involving file contents.

Files that are digitally signed will use the hash value contained in the signature, which may be SHA-1 or MD5. Files that are not digitally signed will use an MD5 hash.

A certificate rule specifies a code-signing, software publisher certificate. For example, a company can require that all scripts and ActiveX controls be signed with a particular set of publisher certificates. Certificates used in a certificate rule can be issued from a commercial certificate authority (CA) such as VeriSign, a Windows 2000/Windows Server 2003 PKI, or a self-signed certificate.

A certificate rule is a strong way to identify software because it uses signed hashes contained in the signature of the signed file to match files regardless of name or location. If you wish to make exceptions to a certificate rule, you can use a hash rule to identify the exceptions.

A path rule can specify a folder or fully qualified path to a program. When a path rule specifies a folder, it matches any program contained in that folder and any programs contained in subfolders. Both local and UNC paths are supported. A rule can identify software from the Internet Explorer zone from which it is downloaded.

Incorrect answers:

A: We can't use a certificate because the file will change.

B: *.vbs will allow any vbs script to run.

D: The hash is calculated using the filename, filesize etc. The file will change so the size will change and therefore the hash will need to be changed.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas

W. Shinder, Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 617

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/maintain/rstrplcy.asp

---

QUESTION 581

You are the network administrator for the Tokyo office of Certkiller . The company network consists of a single Active Directory domain Certkiller .com. The network in your office contains 20 Windows XP Professional computers.

The domain contains an organizational unit (OU) named TokyoOU, which contains all the computer objects for your office. You have been granted the right to create and link Group Policy objects (GPOs) on the TokyoOU.

You need to prevent the computers in your office from executing unauthorized scripts that are written in the Microsoft Visual Basic, Scripting Edition (VBScript) language. However, you want to be able to use VBScript files as startup scripts on all computers in your office. You need to implement a solution that will not affect any other applications.

You plan to implement software restriction policies, by using a GPO on TokyoOU. You will set the default security level to Unrestricted.

Which two actions should you perform to configure software restriction polices? (Each correct answer presents part of the solution. Choose two)

A. Create a new certificate rule.

Set the security level on the rule to Unrestricted.
Digitally sign all the .vbs files that you want to use.
B. Create a new certificate rule.
Set the security level on the rule to Restricted.
Digitally sign all the .vbs files that you want to use.
C. Create a new path rule.
Set the security level on the rule to Unrestricted.
Set the path to *.vbs.
D. Create a new path rule.
Set the security level on the rule to Restricted.
Set the path to *.vbs.
E. Create a new Internet zone rule.
Set the security level on the rule to Unrestricted.
Set the Internet zone to Local computer.
F. Create a new Internet zone rule.
Set the security level on the rule to Restricted.
Set the Internet zone to Local computer.

Answer: A, D

Explanation: The purpose of a rule is to identify one or more software applications, and specify whether or not they are allowed to run. Creating rules largely consists of identifying software that is an exception to the default rule. Each rule can include descriptive text to help communicate why the rule was created.
A software restriction policy supports the following four ways to identify software: Hash-A cryptographic fingerprint of the file. Certificate-A software publisher certificate used to digitally sign a file. Path-The local or universal naming convention (UNC) path of where the file is stored. Zone-Internet Zone
A hash rule is a cryptographic fingerprint that uniquely identifies a file regardless of where it is accessed or what it is named. An administrator may not want users to run a particular version of a program. This may be the case if the program has security or privacy bugs, or compromises system stability. With a hash rule, software can be renamed or moved into another location on a disk, but it will still match the hash rule because the rule is based on a cryptographic calculation involving file contents. A hash rule consists of three pieces of data, separated by colons.
A certificate rule specifies a code-signing, software publisher certificate. For example, a company can require that all scripts and ActiveX controls be signed with a particular set of publisher certificates. Certificates used in a certificate rule can be issued from a commercial certificate authority (CA) such as VeriSign, a Windows 2000/Windows Server 2003 PKI, or a self-signed certificate.
A certificate rule is a strong way to identify software because it uses signed hashes contained in the signature of the signed file to match files regardless of name or location. If you wish to make exceptions to a certificate rule, you can use a hash rule to identify the exceptions.
A path rule can specify a folder or fully qualified path to a program. When a path rule specifies a folder, it matches any program contained in that folder and any programs contained in subfolders. Both local and UNC paths are supported.
Incorrect
Answer:
B: This will allow all vbs script to run except the ones you want to run.
C: This will allow all vbs scripts to run.

E: Zone rules don't apply in this scenario.
F: Zone rules don't apply in this scenario.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas
W. Shinder, Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, p. 617

QUESTION 582
You are the network administrator for Certkiller .com. The network consists of a single Active
Directory domain named Certkiller .com. All network servers run Windows Server 2003.
The domain contains a member server named Certkiller 1, which is located in an organizational unit
(OU) named Servers. Certkiller 1 is managed by an application administrator named King. His domain
user account is a member of the local Administrators group on the server. Members of this group are
the only users who have the Log on locally user right on Certkiller 1.
The written company security policy states that only authorized individuals can access Certkiller 1.
However, you discover that help desk technicians use the Remote Assistance feature to share their
server logon session with unauthorized individuals.
You need to reconfigure Certkiller 1 so the Remote Assistance feature cannot be enabled or used by the
help desk technicians. However, King should have the ability to enable and use this feature.
What should you do?

A. In the System Properties dialog box on Certkiller 1, disable the Turn on Remote Assistance and
allow invitations to be sent from this computer option.
B. In the System Properties dialog box on Certkiller 1, disable the Allow users to connect remotely to
this computer option.
C. Edit the Group Policy object (GPO) for the Servers OU by disabling the Offer Remote Assistance
setting.
D. Edit the Group Policy object (GPO) for the Servers OU by disabling the Solicited Remote
Assistance setting.

Answer: A

Explanation: Remote Desktop Connection is installed by default on all Windows Server 2003 family
operating systems, while Remote Desktop for Administration is disabled by default in Windows Server 2003
family operating systems.
To enabling users to connect remotely to the server Remote Desktop for Administration you must have the
appropriate permissions. By default, members of the Administrator group can connect remotely to the
server. However, the Remote Desktop Users group is not populated by default. You must decide which users
and groups should have permission to log on remotely, and then add them manually to the group.
Incorrect Answers:
B: You need to disable Remote Assistance, and not Remote Desktop.
C: King needs to be able to enable Remote Assistance. A group policy applied to the server would prevent
King from enabling Remote Assistance.
D: King needs to be able to enable Remote Assistance. A group policy applied to the server would prevent

King from enabling Remote Assistance.
Reference:
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 5

QUESTION 583
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. All client computers run Windows XP Professional.
You are responsible for managing Group Policy objects (GPOs) in the domain. A desktop support team administers client computers. The desktop support team's user accounts are all members of a global group named Support. The Support global group belongs to the Administrators local group on all client computers. On all client computers, the Administrators local group also contains the domain user account of the user who is assigned to use that computer, so that the user can install software.
The security administrator creates a GPO named RegTools and links the GPO to the root of the domain. He configures a software restriction policy in the GPO that uses hash rules to prevent users from running registry editing tools. The policy applies to all user accounts in the domain. The desktop support team reports that when they attempt to run registry editing tools, they receive the following error message: "Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator". You need to ensure that only the desktop support team can run registry editing tools.
What should you do?

A. Configure the enforcement options of the software restriction policy so that the policy applies to all users except local administrators.
B. Make all users members of the Power Users group instead of the Administrators group on their computers.
C. Use file system security settings in the Default Domain Policy to modify the NTFS permissions for the registry editing tools' executable files.
Assign only the Support group the Allow - Read and Execute permission for the files.
D. Use a startup script policy to ensure that the registry editing tools are moved to a folder named RegTools.
Assign only the Support group the Allow - Read and Execute permission for the RegTools folder.
E. Edit the permission of the RegTools GPO by assigning the Support group the Deny - Apply group policy permission.
F. Change the software restriction in the RegTools GPO to use a zone rule.

Answer: E

Explanation: Edit the permission of the RegTools GPO by assigning the Support group the Deny - Apply group policy permission. The GPO would not apply to members of this group irrespective of the permissions they have in other security groups
Incorrect Answers:
A: This will not work in this case. Not all the users in the support group are necessarily local administrators.
B: Making all users power users will not work. Usually the most restrictive properties take precedence.
C: The Allow - Read and Execute permission for files, albeit a Default domain policy, is not an NTFS permissions issue.

D: You need to edit the GPO and assign the appropriate permission. There is no need to move any folders.
F: Modifying the RegTools GPO software restriction to make use of a zone rule will not help in this scenario.
Reference:
Jill Spealman, Kurt Hudson, and Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Chapter 10, pp. 601 - 607
Diana Huggins, Windows Server 2003 Network Infrastructure Exam Cram 2 (Exam 70-291), Chapter 3

QUESTION 584
You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains a Windows Server 2003 file server named Certkiller 1.
During a routine security audit, you examine the security log on Certkiller 1 in Event Viewer. You discover that the security log contains thousands of events that indicate failed logon attempts from a variety of computers for the built-in Administrator account on Certkiller 1. The local Administrator account is never used. You suspect that an unauthorized user is attempting to access Certkiller 1 by using the built-in Administrator account.
You need to protect Certkiller 1 from attacks that attempt to use the built-in Administrator accounts, while ensuring that users can continue to use it as a file server.
What should you do on Certkiller 1?

A. Enable the Do not allow anonymous enumeration of SAM accounts policy in the Default Domain security settings.
B. Disable the local Administrator account.
C. Modify the built-in Administrator account by enabling the Account in sensitive and cannot be delegated option.
D. In the local security policy, assign the built-in Administrator account the Deny log on locally user right.

Answer: B

Explanation: Since the local Administrator account is never used and you suspect it is being used by unauthorized users, it should be disabled because it allows unauthorized users access to Certkiller 1 thus leaving Certkiller 1 vulnerable.
Incorrect Answers:
A: You need to disable the local Administrator account since it is being used for unauthorized access. You still have to ensure that users can continue to use the file server thus this option will not do.
C: This option will not work as what needs to be done is to take away the right to access Certkiller 1 and this means disabling the local Administrator account.
D: The Built-in Administrator account cannot be assigned the Deny log on locally user right because only Domain Admins and the local Administrator account remain members of the local Administrators group who can assign these rights.
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. 783

QUESTION 585
You are the network administrator for Certkiller .com. The network consists of single Active directory domain Certkiller .com.
The domain contains a Window server 2003 domain controller named Certkiller 2. The securews.inf security policy has been applied to the domain. Server6 hosts a network application that installs a new service named NetAppService. NetAppService is configurable in the Services console. The network application requires a service account. The network application runs constantly.
You create and configure a service account named SrvAcct for the network application. The software functions properly using the new account and service.
You discover an ongoing brute force attack against the SrvAcct account. The intruder appears to be attempting a distributed attack from several Window XP Professional domain member computers on the LAN. The account has not been compromised and you are able to stop the attack. You restart Certkiller 2 and attempt to run the network application, but the application does not respond.
What should you do to run the application so that it runs constantly?

A. Reset the SrvAcct password,
B. Configure the default Domain Controllers policy to assign the SrvAcct account the right to log on locally.
C. Unlock the SrvAcct account.
D. Restart the NetAppService service.

Answer: C

Explanation: Disabling the Interactive logon: Require Domain Controller authentication to unlock workstation will weaken the security configuration, but it will allow the application to run smoothly.
Incorrect Answers:
A: Resetting the password for that specific account will not work in this scenario. You want to be able to run the network application after the attack has been stopped and thus locked the account which first has to be unlocked to enable the application to run smoothly.
B: Assigning the log on locally permission to the SrvAcct account is not sufficient; you still need to unlock the account.
D: Restarting the backup application is not sufficient as the account has to be unlocked for the application to respond.
Reference:
Deborah Littlejohn Shinder and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress Publishing Inc., Rockland, 2003, pp. 317-318.

QUESTION 586
You are the network administrator for Certkiller .
A server named Certkiller SrvC functions as a local file server. Certkiller SrvC contains several extremely confidential files.
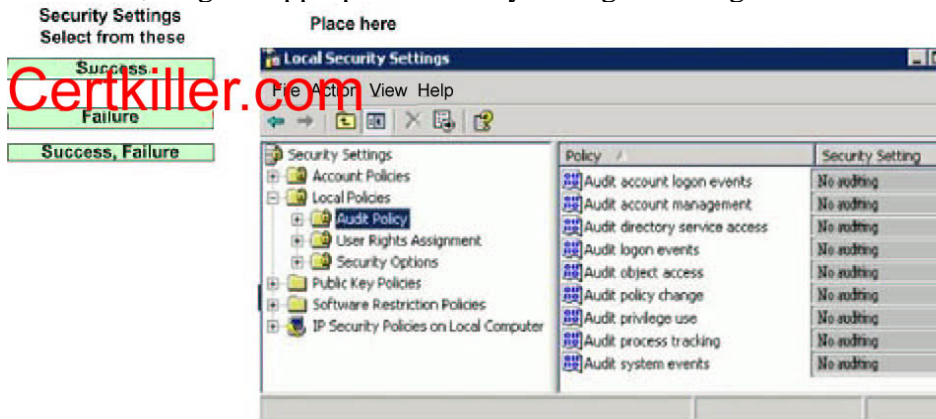The company's security department wants all attempts to access the confidential files on
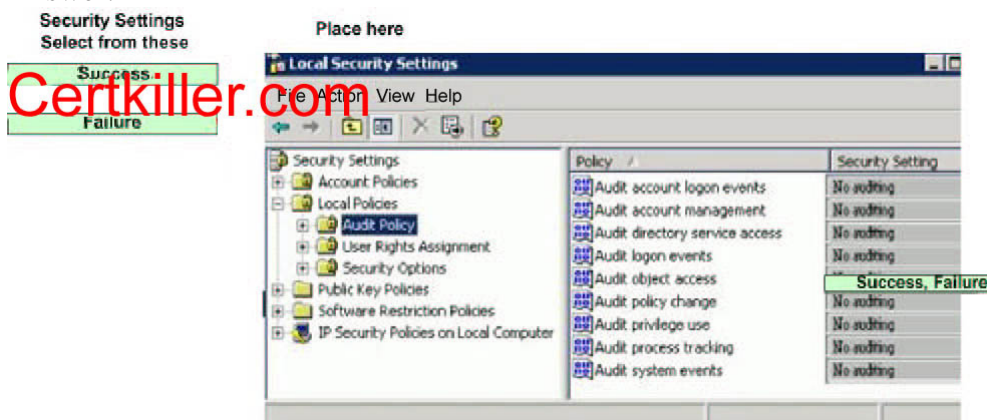
Certkiller SrvC to be recorded in a log.
You need to configure the local security policy on Certkiller SrvC to give you the ability to comply with the security department's requirements. No other auditing should be configured.
What should you do?
To answer, drag the appropriate security setting or settings to the correct policy or polices.

Answer:

Explanation: You should audit Success and Failure to log all attempts to access the files on Certkiller SrvC. The Audit object access policy setting determines whether the event of a user accessing an object such as a file, folder, registry key and printer; which has its own system access control list (SACL) specified, should be audited. You can configure whether to audit successes, audit failures, or not to audit the event type. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.
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, pp. 871-875
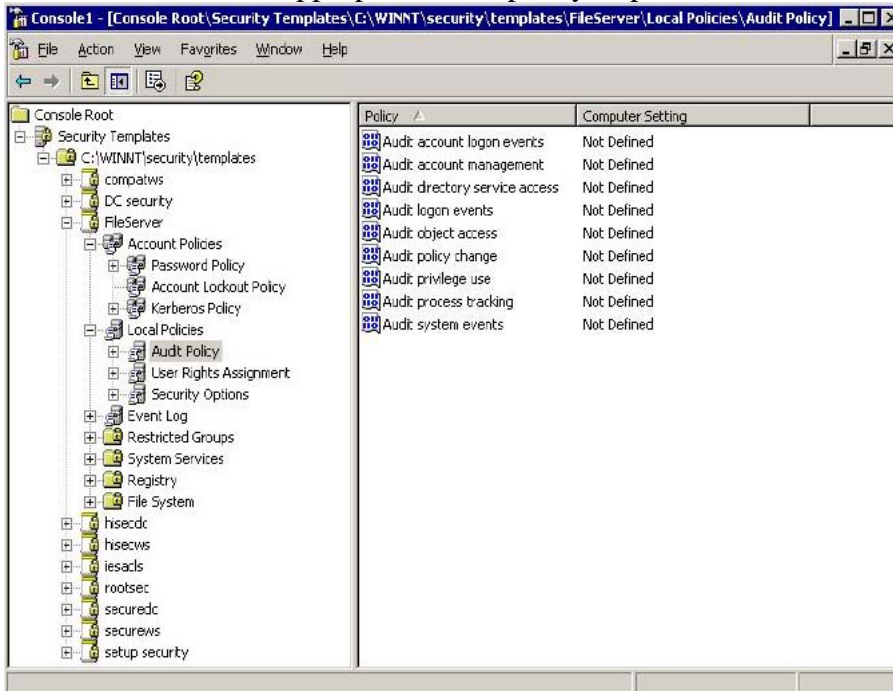

QUESTION 587
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain Certkiller .com. The domain contains Windows Server 2003 computers and Windows XP Professional computers.

The written company security policy states that the audit policy on all file servers in the domain must have the ability to audit failure events for user access to files and folders. You create a custom security template named fileserver.
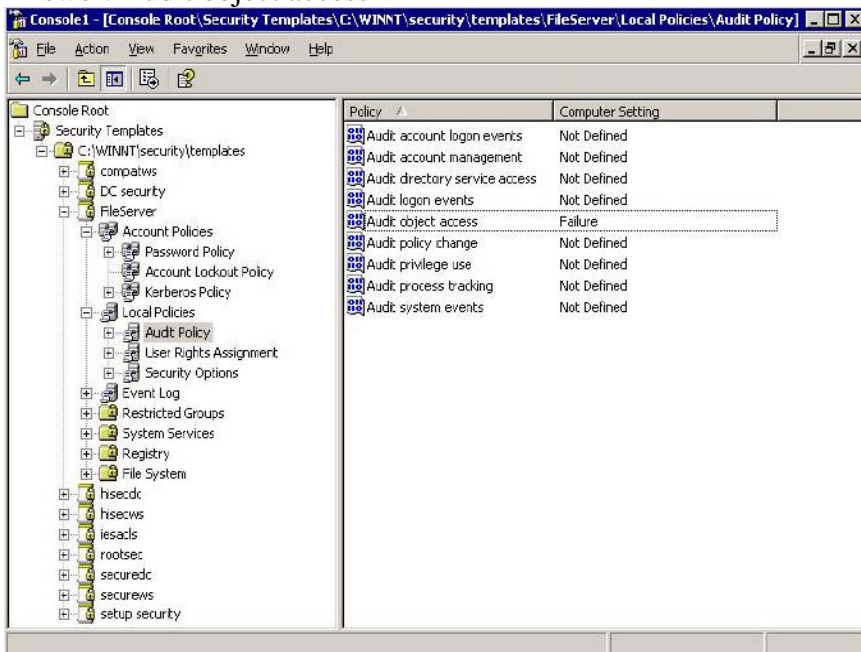You need to configure the fileserver security template to enforce the written security policy of Certkiller for all file servers.
Which policy or polices should you modify?
To answer, select the appropriate audit policy or polices in the list of audit polices.

Answer: Audit object access

Explanation: The Audit object access policy setting determines whether the event of a user accessing an object such as a file, folder, registry key and printer; which has its own system access control list (SACL) specified, should be audited.
You can set a SACL on a file system object by using the Security tab in the object's Properties dialog box. You can configure whether to audit successes, audit failures, or not to audit the event type. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.
To disable auditing, select the "Define these policy settings" check box in the Properties dialog box for this particular policy setting, and clear the Success and Failure check boxes.
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. 798

QUESTION 588
You install Windows Server 2003 on a computer named Certkiller 2. Certkiller 2 will host a missioncritical application. The system engineer asks you to monitor Certkiller 2 to ensure reliability and availability.
You assign a computer maintenance engineer named Kim to assist you in maintaining Certkiller 2. Kim will have the following responsibilities on Certkiller 2:
• Use Event Viewer to monitor all events logs except the security logs.
• Use Performance Logs and Alerts to create new performance logs.
You need to assign Kim only the minimum rights on Certkiller 2 that are required to perform these tasks. Kim must be able to perform the tasks locally or from another computer. To simplify administration, you must use the minimum number of groups required.
To which local built-in security group or groups should you assign Kim? (Choose all that apply)

A. Administrators
B. Performance Log Users
C. Performance Monitor Users
D. Power Users
E. Remote Desktop Users

Answer: B

Explanation: Performance Logs and Alerts provide logging and alert capabilities for both local and remote computers. You use logging for detailed analysis and recordkeeping. Retaining and analyzing log data that is collected over time can be helpful for capacity and upgrade planning. To perform this procedure, you must be a member of the Administrators group, or you must have been delegated the appropriate authority. If the computer is connected to a domain, members of the Domain Admins group might be able to perform this procedure. Performance Log Users members can manage performance counters, logs and alerts on the server locally and from remote clients without being a member of the Administrators group. Thus making Kim a member of the Performance log users will grant her enough permissions to complete her tasks without granting her membership to too many groups.
Incorrect Answers:

A: Administrators have the ability to provide both logging and alert capabilities for both local and remote computers. Kim will not be needing membership to this group as well. Being a member of the Performance Log Users is sufficient.

C: Performance Monitor users can monitor performance counters on the server locally and from remote clients without being a member of the Administrators or Performance Log Users groups.

D: Power Users membership will be too restrictive to allow Kim to complete her tasks.

E: Remote Desktop Users membership will not enable Kim to complete her tasks.

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. 783


QUESTION 589

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 domain controllers and Windows XP Professional computers.

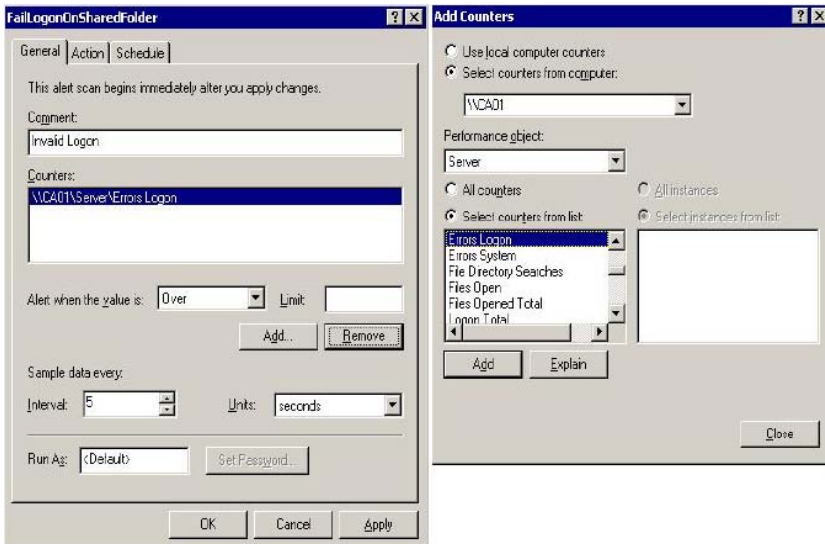A server named Certkiller Srv7 hosts a shared folder.

You want to use System Monitor to configure monitoring of the server performance object to alert you when invalid logon attempts are made to the shared folder. You want to monitor only events that are associated with invalid logons.

How should you configure the alert?

To answer, drag one or more appropriate instances of the server performance object to the alter interface.
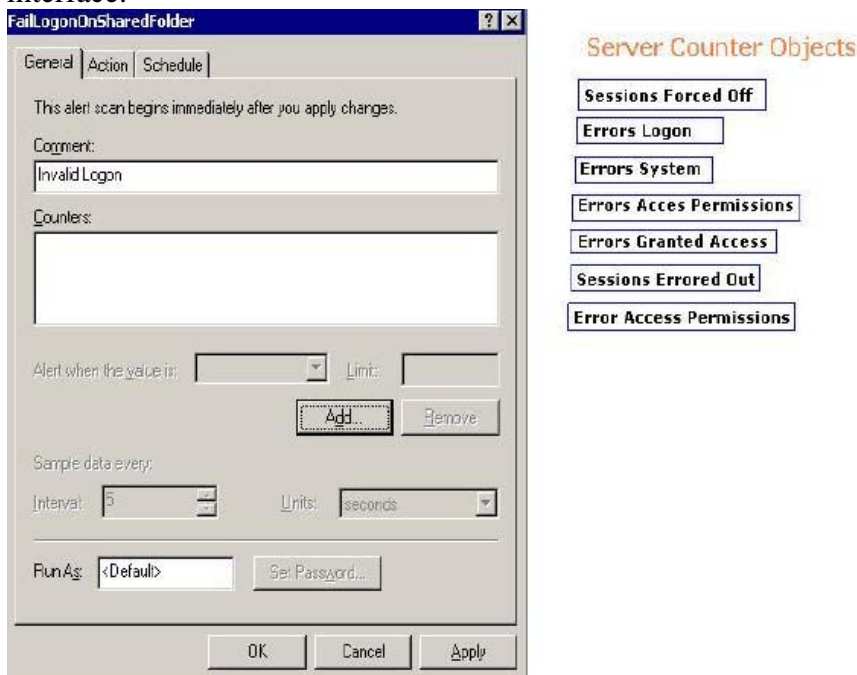
Answer: Drag Errors Logon to the appropriate location.

Server Object and Counter Errors Logon

Explanation: A user's credentials have to be validated when a UNC name is utilized to connect to a remote network resource. The UNC connection uses Server Messaging Blocks (SMBs) to work through the Multiple UNC Provider (MUP). A SMB, called SESSION SETUP and X, is used for the connection. At this point, the user's credentials are passed to the network resource. Validation occurs locally on the computer when the resource is a domain controller that maintains the user account.

A secure channel mechanism is utilized for user validation when the resource uses pass-through authentication.

The network resource requests a validation of the user from its domain controller. The domain controller returns an error to the network resource when the user's credentials are invalid and increments its usri3_bad_pw_count for the particular user. The network resource returns a message that has the NT status code 0xC000006D, STATUS_LOGON_FAILURE, to the client workstation.

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. 634

QUESTION 590

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 three email servers. These e-mail servers send messages to each other by using SMTP.

Certkiller 's written security policy states that all Simple Mail Transfer Protocol (SMTP) traffic must be encrypted by using an IPSec policy. You create an organizational unit (OU) named Mail Servers and place all the e-mail servers in the OU. You create an IPSec policy that requires security for all SMTP connections to the e-mail servers.

You need to verify that all SMTP traffic sent between the e-mail servers is encrypted.

What should you do?

A. Use IP Security Monitor to find out which IPSec policies are being applied to the e-mail servers.

B. Use Network Monitor to capture network packets sent between the e-mail servers.

C. Use Group Policy Editor to find out which IPSec policies are being applied to the Mail Servers OU.

D. Run the gpresult command on each mail server to find out which Group Policy objects (GPOs) are being applied to the e-mail servers.

Answer: B

Explanation: You can use Network Monitor to design and create a capture filter to capture network packets sent between the e-mail servers. Using a capture filter would assist in isolating SMTP traffic sent between the e-mail servers.
Incorrect Answers:
A: To assist you with the standard monitoring of IPSec, you have the IPSec Security monitor. Finding out which IPSec policies are being applied to the e-mail servers will not necessarily verify which traffic is encrypted. The question pertinently asks for all SMTP traffic sent between e-mail servers is encrypted, not which policies are applied.
C: Group Policy Editor is not used to monitor which IPSec policies are applied. Also finding out which policies are applied where is not what the question asks.
D: This option will require that you are also aware of which Group Policies entails which objects. This will not necessarily help you in verifying which SMTP traffic is encrypted. The question wants verification that all SMTP traffic be encrypted.
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, Chapter 3, pp. 142, 586, 868

QUESTION 591
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.
Two of the servers on the network contain highly confidential documents. Certkiller 's written security policy states that all network connections with these servers must be encrypted by using an IPSec policy.
You place the two servers in an organizational unit (OU) named SecureServers. You configure a Group Policy object (GPO) that requires encryption for all connections. You assign the GPO to the SecureServers OU.
You need to verify that users are connecting to the two servers by using encrypted connections.
What should you do?

A. Run the net view command.
B. Run the gpresult command.
C. Use the IP Security Monitor console.
D. Use the IPSec Policy Management console.

Answer: C

Explanation: Administrators can use the IP Security Monitor tool to confirm whether IP Security (IPSec) communications are successfully secured. The tool can display the number of packets that have been sent over the Authentication Header (AH) or Encapsulating Security Payload (ESP) security protocols, and how

many security associations and keys have been generated since the computer was last started. The IP Security Monitor is implemented as a Microsoft Management Console (MMC) snap-in on the Windows Server 2003 and Windows XP Professional operating systems. It includes enhancements that allow you to view details about an active IPSec policy, in addition to Quick Mode and Main Mode statistics, and active IPSec SAs. IP Security Monitor also enables you to search for specific Main Mode or Quick Mode filters.
Incorrect Answers:
A: Running the net view command will not aid you in verifying users connecting to the two servers make use of encrypted connections.
B: The gpresult command displays the Resultant Set of Policy (RSoP) information for a target user and computer.
D: If you want to verify whether users connecting to the two servers make use of encrypted connections then you should use the IP Security Monitor console and not the IPSec Policy Management console.
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, p. 15: 20
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.795

QUESTION 592
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains three Windows Server 2003 domain controllers, 20 Windows Server 2003 member servers, and 750 Windows XP Professional computers. The domain is configured to use only Kerberos authentication for all server connections.
A user reports that she receives an "Access denied" error message when she attempts to connect to one of the member servers. You want to test the functionality of Kerberos authentication on the user's client computer.
Which command should you run from the command prompt on the user's computer?

A. netsh
B. netdiag
C. ktpass
D. ksetup

Answer: B

Explanation: Netdiag is a command-line diagnostic tool that you can use to test network connectivity. It performs a series of tests to determine the state and functionality of a network client. You can use the results of these tests, and network status information provided by Netdiag to assist you in isolating network and connectivity problems on your Windows 2000-based workstation or server computer. The netdiag command is used to run a diagnostics test against your server to see if anything is not working correctly.
Incorrect Answers:
A: With the Netsh.exe tool, you can direct the context commands you enter to the appropriate helper, and the helper then carries out the command. A helper is a Dynamic Link Library (.dll) file that extends the

functionality of the Netsh.exe tool by providing configuration, monitoring, and support for one or more services, utilities, or protocols. The helper may also be used to extend other helpers.

C: If you want to configure your UNIX hosts to use a Windows 2000-based server as a Kerberos Key Distribution Center (KDC), you must generate a Kerberos keytab file. You can use the Ktpass utility, which is included with the Microsoft Windows 2000 Resource Kit, to create a keytab file for your UNIX host.

D: KSetup is a command-line tool that configures Windows 2000 clients to use an MIT Kerberos server instead of using a Windows 2000 domain for user authentication.

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. 871-874

QUESTION 593
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. All computers are members of the domain.

All users in the Certkiller Sales Staff (TSS) use only their designated computers. The TSS users frequently access confidential data stored on servers in the domain.

To ensure that confidential data is not compromised during data transmissions, you want to secure all communication between the TSS computers and all domain servers. You must ensure that all other users will continue to have access to the domains servers.

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

A. Assign the Server (Request Security) IPSec policy on all servers.
B. Assign the Secure (Require Security) IPSec policy on all servers.
C. Assign the Client (Respond Only) IPSec policy on all servers.
D. Create and assign a new IPSec policy on all servers. Activate the Default Response rule.
E. Assign the Client (Respond Only) IPSec policy on all TSS computers.
F. Enable Internet Connection Firwall (ICF) on all TSS computers.

Answer: A, E

Explanation: The Client (Respond Only) policy specifies that a Windows 2000, XP, or Server 2003 IPSec client will negotiate IPSec security with any peer that supports it but that it won't attempt to initiate security. Let's say you apply this policy to a Server 2003 computer. When it initiates outbound network connections, it won't attempt to use IPSec. When someone opens a connection to it, though, it will accept IPSec if the remote end asks for it.

The Server (Request Security) policy is a mix of the Client (Respond Only) and the Secure Server (Require Security) policy. In this case, the machine will always attempt to use IPSec by requesting it when it connects to a remote machine and by allowing it when an incoming connection requests it. This policy provides the best general balance between security and interoperability.

To ensure that there is no compromise on confidential data during transmissions between the TSS computers and all the domain servers without disrupting acesss you need to assign the Server (Request Security) IPSec policy on all the servers. In addition you also need to assign the Client (Respond Only) IPSec policy on all

the TSS computers.
Incorrect answers:
B: The Secure Server (Require Security) policy specifies that all IP communication to or from the policy target must use IPSec. In this case, all DNS, WINS, and web requests and everything else that uses an IP connection either has to be secured with IPSec or will be blocked. This may not be what you want unless you plan to implement IPSec on your entire network. This is not what is required on the servers.
C: This is the incorrect IPSec policy to assign to the servers in this case.
D: There is no need to create and assign a new IPSec policy on all the servers. It is not going to ensure the confidentiality of transmitted data oin this case as there are the TSS computers also to take into account.
F: Internet Connection Firewall on all TSS computers is not going to ensure the confidentiality of transmitted data between TSS clients and the servers.
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. 177

QUESTION 594
Exhibit:

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 includes a file server named Certkiller 8, which contains highly confidential data. The company's written security policy states that all connections to Certkiller 8 must be encrypted by using IPSec.
Another network administrator creates an OU named Secure Servers. He then creates a GPO named Secure Servers. He configures an IPSec policy as part of the Secure Servers GPO.
During a routine security check, the security office reports that client computers can still make nonsecure connections to Certkiller 8. You open IP Security Monitor on Certkiller 8, as shown in the exhibit.
You need to identify why client computers still can make nonsecure connections to Certkiller 8.
What is the most likely cause of the problem?

A. Certkiller 8 is located in the wrong Active Directory container.
B. The IPSec policy is configured incorrectly.
C. The Secure Servers GPO is not linked to the appropriate OU.
D. The IPSec Services service is not running on Certkiller 8.

Answer: B

Explanation: The security office reports that client computers can still make nonsecure connections to Certkiller 8 is due the IPSec policy not being configured properly. The other options' suggestions does not explain why unsecure connections can still be made.
Incorrect answers:
A: It is not a matter of Certkiller 8 being in the wrong Active Directory container that has a bearing on the IPSec policy in this case.
C: The GPO is linked to the correct OU.
D: This is not true. The exhibit shows that there is IPSec policies applied to Certkiller 8 and is active.
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. 201-204

QUESTION 595
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 five servers that contain highly confidential information. You place the five servers in an OU named SecureServers. You create a GPO named IPSecGPO. The GPO configures an IPSec policy that requires secure connections for all connections to servers in the SecureServers OU.
You need to verify that the IPSecGPO GPO is being applied to each of the servers in the SecureServers OU.
What should you do?

A. Use the IPSec Policy Management console.
B. Use the Microsoft Baseline Security Analyser (MBSA).
C. Run the gpresult command on each of the servers.
D. In the Group Policy Management Console (GPMC), configure a Resultant Set of Policy (RSoP) modelling report for the SecureServers OU.

Answer: C

Explanation: The gpresult command displays the Resultant Set of Policy (RSoP) information for a target user and computer.
Incorrect answers:
A: The IPSec Policy Management tool is used to ensure that the IPSec policies are assigned to both computers and that they are compatible with each other.you need to verify that the appropriate GPO is applied to each of the servers in the SecureServers OU.
B: The MBSA is used to to ensure that you have the most current security updates. This is not what is required. This does not tell you what you ahave applied to the servers.
D: IPSec support for Resultant Set of Policy (RSoP) provides the ability to see exactly how the various policies within the domain will apply to a specific user or computer. IPSec provides an extension to the RSoP console that you can use to view detailed settings for the IPSec policy that is being applied. However, you should run the gpresult command to be able to see the RSoP reports and not configure an

RSoP modelling report.
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, p. 15: 20
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. 173, 207, 795

QUESTION 596
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The domain contains two domain controllers that are configured as DNS servers. Forward and reverse DNS lookup zones are configured on both DNS servers.
You install the Windows Server 2003 administrative tools on your client computer. You use IP Security Monitor to view network information. You notice that many servers on the network are identified only by IP address within the IP Security Monitor interface.
You need to ensure that servers on the network are listed by server names rather than IP addresses. What should you do?

A. Configure your client computer to use the domain controllers for DNS lookups.
B. Enable DNS name resolution in IP Security Monitor.
C. Force a registration of DNS information on all servers on the network.
D. Configure all servers on the network to support NetBIOS over TCP/IP.

Answer: C

Explanation: Every computer in a Windows Server 2003 network can be assigned a primary DNS suffix to be used in name resolution and name registration. The primary DNS suffix is specified on the Computer Name tab of the properties dialog box in My Computer. The primary DNS suffix is also known as the primary domain name and the domain name. To force a registration of DNS information on all servers on the network, is a way to ensure that servers on the network are listed by server names and not IP addresses.
Incorrect answers:
A: When lookups and responses are made using DNS, resource records are represented in binary form in packets. In the DNS console, resource records are represented graphically so that they can be viewed and modified easily. However, at the source-in the zone database files-resource records are represented as text entries. In fact, by creating resource records in the DNS console, you are automatically adding text entries to the corresponding zone's database file. Thus using the domain controllers for DNS lookups will not ensure that servers are listed by server names.
B: Name resolution is not a function of IP Security Monitor.
D: 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. However, this is not what is required in this case.

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. 4:5-8, 32

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

QUESTION 597

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

A server named Certkiller 1 is configured with IIS. Certkiller 1 hosts a Web site for the engineering department.

The engineering Web site is configured to support communications by using HTTPS. You use Network Monitor on Certkiller 1 and discover that users are connecting to the engineering Web site by using both HTTP and HTTPS.

You must ensure that all access to the engineering Web site on Certkiller 1 is gained by using HTTPS. What should you do on Certkiller 1?

A. Install a new server certificate.
B. Change the TCP port on the engineering Web site to port 8080.
C. Configure the engineering Web site to use only Integrated Windows authentication.
D. Use the IIS Certificate wizard to renew the current certificate for the engineering Web site.
E. Configure the engineering Web site to require a secure channel.

Answer: E

Explanation: HTTPS makes use of TCP port 443. Any time you visit a Web site that uses an https:// prefix instead of http://, you're seeing Secure Sockets Layer (SSL) encryption in action. Web page encryption is implemented using the Secure Sockets Layer (SSL) protocol. This is useful when you need to ensure that all access to the engineering Web site is gained by means of HTTPS.

Incorrect answers:

A: Installing a new server certificate will not ensure all access occur through HTTPS.

B: Changing the port of the Web site to 8080 will not work as HTTPS makes use of port 443.

C: The Integrated Windows Authentication option employs a cryptographic exchange between the web server and the user's Internet Explorer web browser to confirm the user's identity. Making use of only Integrated Windows authentication is not ensuring that all access is through HTTPS.

D: Renewing the current certificate with the IIS Certificate wizard will not ensure that all access will be through HTTPS.

Reference:

Lisa Donald, Suzan Sage London and James Chellis, MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide, Sybex Inc. Alameda, 2003, p. 328

QUESTION 598

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. Client computers run

Windows XP Professional, Windows 2000 Professional, and Windows NT Workstation 4.0.
The network contains a file server named Certkiller 1. Certkiller 1 hosts a shared folder that contains
confidential financial data. This data is accessible only by users in the finance department.
Certkiller 's written security policy states that all network traffic from Certkiller 1 to client computers in
the finance department must be encrypted by using an IPSec policy. To satisfy this requirement, you
configure an IPSec policy for Certkiller 1. The Quick Mode filters applied by the policy are shown in
the exhibit.

You monitor the connections on Certkiller 1. You notice that all users in the finance department are
connecting to Certkiller 1 by using the IPSec policy with the exception of one user. This user can
connect to the server without using a secure connection.
You need to identify why the user cannot connect to Certkiller 1 by using an IPSec connection.
What is the most likely cause of the problem?

A. The client computer does not support the IPSec policy.
B. The client computer has an IP address that is not on the appropriate subnet.
C. The client computer is using an incorrect port number to connect to Certkiller 1.
D. The client computer is not configured to respond as an IPSec client.

Answer: C

Explanation: You can think of IPSec policies as a collection of packet filters that enforce security policy on
IP traffic. Each filter describes some network protocol action. You configured an IPSec policy for
Certkiller 1. This IPSec policy contains a set or rules including selected filter lists (protocols and ports to
which you want the filter to apply), filter actions, authentication methods, connection types, and tunnel
settings. When a client computer uses an incorrect port number to connect to Certkiller 1, it would prevent the
user from connecting to Certkiller 1 by via an IPSec connection.
Incorrect Answers:
A: The issue of whether the client computer is configured to support IPSec policy is not the issue. The
problem stems from the client computer making use of the wrong port number when attempting to
connect to Certkiller 1.
B: The IP address is no the cause of the problem. Thus this option is irrelevant.
D: The problem originated due to an incorrect port number being used as not due to a configuration
problem regarding IPSec client.
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,

2004, pp. 673-674
Zacker, Craig, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft
Windows Server 2003 Network, Microsoft Press, Redmond, 2003, Chapter 12, p. 630

QUESTION 599
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 domain controllers and
Windows XP Professional computers. All client computers are portable computers.
The company hires a consultant to deploy a wireless network infrastructure. The name of the wireless
network is WLAN_FRTHCF. To ensure the highest level of security on the wireless network, you
create and link a Group Policy object (GPO) to enable Protected EAP (PEAP) 802.1x authentication
on all wireless client computers. You name the GPO WLAN_PEAP. All Wireless access Points are
configured to use the same RADIUS server. Certificate services are not deployed in Certkiller .com.
After the WLAN_PEAP GPO is applied to client computers, users report that their wireless
connection functions properly, but it disconnects when they carry their wireless portable computers
from one area to another in their office building.
You need to ensure that client computers are not disconnected.
What should you do?
To answer, configure the appropriate option or options in the dialog box.

Answer:
Select the Enable Fast Reconnect check box. The checkbox is at the bottom of the dialog box and as a
result cannot be seen in the exhibit.

Explanation: To ensure that client computers are not disconnected one should enable Fast Reconnect because it has the capability to reconnect to a wireless access point using cached session keys facilitating quick roaming between wireless access points, TLS-generated dynamic keying material, and server authentication that prevents deployment of unauthorized wireless access points.
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. 697

QUESTION 600
The Certkiller network design requires secure network connections across all IP public communication media.
On a daily basis, you must verify that secure network connections are functioning properly
What should you do?

A. From a command prompt, run the netdiag command.
B. Use the IP Security Monitor snap-in.
C. Create an IPSec Security Group Policy object (GPO).
D. From a command prompt, run the ipsec6 command.

Answer: B

Explanation: To assist you with the standard monitoring of IPSec, you have the IPSec Security monitor. You should use the IP Security Monitor included in Windows Server 2003 and implemented as an MMC snap-in, to monitor IPSec information on local computers and remote machines. You can examine information on IPSec policies, generic and specific filters, security associations and statistics.
Incorrect Answers:
A: Running the netdiag command from a command prompt will run a diagnostics test against your server to see if anything is not working correctly. This does not mean that it will check up on whether secure network connections are operational. Although netdiag.exe can still be used to obtain information about networking, Windows Server 2003 no longer uses the netdiag /test:ipsec option; it has been removed and replaced with the netsh commands for IPSec.
C: This option suggests a group policy object which will not work in this particular scenario.
D: Running the ipsec6 command from a command prompt will not work.
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 11, Syngress Publishing Inc., Rockland, 2003, pp. 682, 868, 871