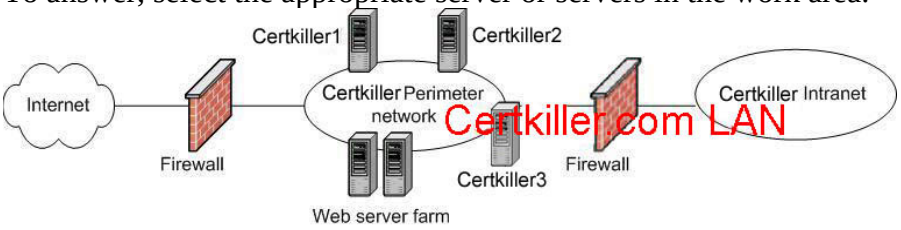
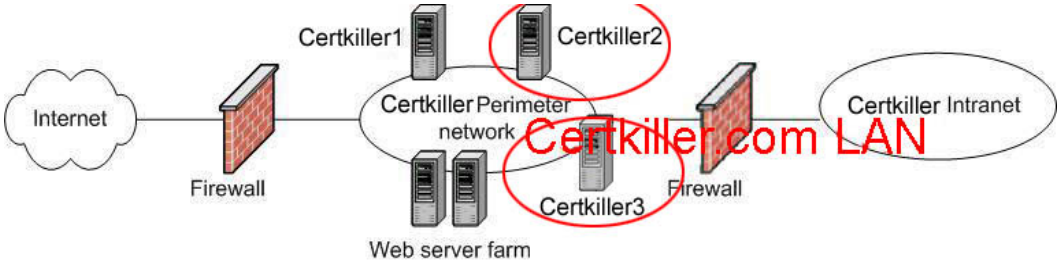
QUESTION 1
You are a network administrator for Certkiller . The network consists of an intranet and a perimeter network, as shown in the work area. The perimeter network contains:
• One Windows Server 2003, Web Edition computer named Certkiller 1.
• One Windows Server 2003, Standard Edition computer named Certkiller 2.
• One Windows Server 2003, Enterprise Edition computer named Certkiller 3.
• One Web server farm that consists of two Windows Server 2003, Web Edition computers.
All servers on the perimeter network are members of the same workgroup.
The design team plans to create a new Active Directory domain that uses the existing servers on the perimeter network. The new domain will support Web applications on the perimeter network. The design team states that the perimeter network domain must be fault tolerant.
You need to select which server or servers on the perimeter network need to be configured as domain controllers.
Which server or servers should you promote?
To answer, select the appropriate server or servers in the work area.



Answer:



Explanation: We know web editions can't be domain controllers, and we want fault tolerance, which means two Domain Controllers.
The answer is promote the two servers that aren't running Web Edition to dc's (Certkiller 2 and Certkiller 3).
Reference: MS training kit 70-290 chapter one lesson 1;"the server belongs to a domain but cannot be a domain controller"

QUESTION 2
You are a network administrator for Certkiller . The network consists of a single Active Directory domain and contains Windows Server 2003 computers.
You install a new service on a server named Certkiller 3. The new service requires that you restart Certkiller 3. When you attempt to restart Certkiller 3, the logon screen does not appear. You turn off and then turn on the power for Certkiller 3. The logon screen does not appear. You attempt to recover the failed server by using the Last Known Good Configuration startup option. It is unsuccessful. You attempt to recover Certkiller 3 by using the Safe Mode Startup options. All Safe Mode options are unsuccessful.

You restore Certkiller 3. Certkiller 3 restarts successfully. You discover that Certkiller 3 failed because the new service is not compatible with a security path.
You want to configure all servers so that you can recover from this type of failure by using the minimum amount of time and by minimizing data loss. You need to ensure that in the future, other services that fail do not result in the same type of failure.
What should you do?

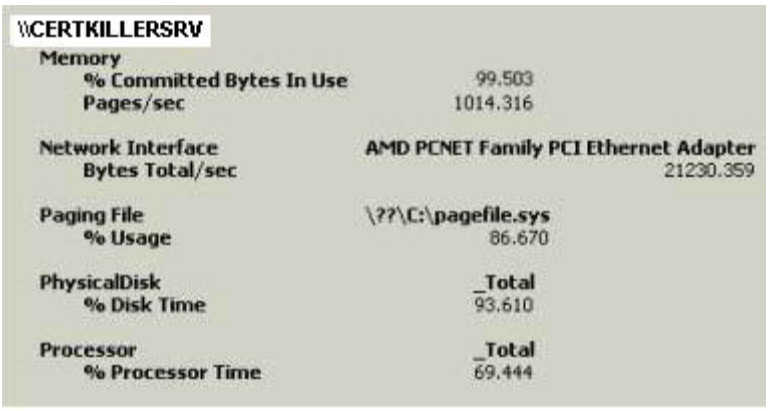
A. Use Add or Remove Programs.
B. Install and use the Recovery Console.
C. Use Automated System Recovery (ASR).
D. Use Device Driver Roll Back.

Answer: B

Explanation:
1.We know that this service causes the failure.
2. We want minimum of time and minimum of data loss.
3. We want a solution for all servers.
4.. We want to make sure other services that fail do not result in the same type of failure.
Server HELP
Recovery Console overview
Repair overview
Safe Mode
A method of starting Windows using basic files and drivers only, without networking. Safe Mode is available by pressing the F8 key when prompted during startup. This allows you to start your computer when a problem prevents it from starting normally and other startup options do not work, consider using the Recovery Console. This method is recommended only if you are an advanced user who can use basic commands to identify and locate problem drivers and files. In addition, you will need the password for the built-in administrator account
administrator account
On a local computer, the first account that is created when you install an operating system on a new workstation, stand-alone server, or member server. By default, this account has the highest level of administrative access to the local computer, and it is a member of the Administrators group.
In an Active Directory domain, the first account that is created when you set up a new domain by using the Active Directory Installation Wizard.
By default, this account has the highest level of administrative access in a domain, and it is a member of the Administrators, Domain Admins, Domain Users, Enterprise Admins, Group Policy Creator Owners, and Schema Admins groups.
to use the Recovery Console.
Using the Recovery Console, you can enable and disable services
A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level. When services are provided over a network, they can be published in Active Directory, facilitating service-centric administration and usage. Some examples of services are the Security Accounts Manager service, File Replication service, and Routing and Remote Access service., format drives, read and write data on a local drive (including drives formatted to use NTFS)
NTFS
An advanced file system that provides performance, security, reliability, and advanced features that are not

found in any version of file allocation table (FAT). For example, NTFS guarantees volume consistency by using standard transaction logging and recovery techniques. If a system fails, NTFS uses its log file and checkpoint information to restore the consistency of the file system. NTFS also provides advanced features, such as file and folder permissions, encryption, disk quotas, and compression.), and perform many other administrative tasks.
The Recovery Console is particularly useful if you need to repair your system by copying a file from a floppy disk or CD-ROM to your hard drive, or if you need to reconfigure a service that is preventing your computer from starting properly.
Operating system does not start (the logon screen does not appear).
Feature: Last Known Good Configuration startup option
When to use it: When you suspect that a change you made to your computer before restarting might be causing the failure.
What it does: Restores the registry settings and drivers that were in effect the last time the computer started successfully.
For more information, see To start the computer using the last known good configuration.
Feature: Recovery Console
When to use it: If using the Last Known Good Configuration startup option is unsuccessful and you cannot start the computer in Safe Mode
Safe Mode
A method of starting Windows using basic files and drivers only, without networking. Safe Mode is available by pressing the F8 key when prompted during startup. This allows you to start your computer when a problem prevents it from starting normally.
This method is recommended only if you are an advanced user who can use basic commands to identify and locate problem drivers and files. To use the Recovery Console, restart the computer with the installation CD for the operating system in the CD drive. When prompted during text-mode setup, press R to start the Recovery Console.
What it does: From the Recovery Console, you can access the drives on your computer. You can then make any of the following changes so that you can start your computer:
• Enable or disable device drivers or services.
• Copy files from the installation CD for the operating system, or copy files from other removable media. For example, you can copy an essential file that had been deleted.
• Create a new boot sector and new master boot record (MBR)
master boot record (MBR)
The first sector on a hard disk, which begins the process of starting the computer. The MBR contains the partition table for the disk and a small amount of executable code called the master boot code.
You might need to do this if there are problems starting from the existing boot sector.

QUESTION 3
You are a network administrator for Certkiller . The network contains a Windows Server 2003 application server named Certkiller Srv. Certkiller Srv has one processor. Certkiller Srv has been running for several weeks.
You add a new application to Certkiller Srv. Users now report intermittent poor performance on Certkiller Srv. You configure System Monitor and track the performance of Certkiller Srv for two hours. You obtain the performance metrics that are summarized in the exhibit.



The values of the performance metrics are consistent over time.
You need to identify the bottleneck on Certkiller Srv and upgrade the necessary component. You need to minimize hardware upgrades.
What should you do?

A. Install a faster CPU in Certkiller Srv.
B. Add more RAM to Certkiller Srv.
C. Add additional disks and spread the disk I/O over the new disks.
D. Increase the size of the paging file.

Answer: B

Explanation:
Reference, Windows help:
Determining acceptable values for counters
In general, deciding whether or not performance is acceptable is a judgment that varies significantly with variations in user environments. The values you establish as the baselines for your organization are the best basis for comparison. Nevertheless, the following table containing threshold values for specific counters can help you determine whether values reported by your computer indicate a problem. If System Monitor consistently reports these values, it is likely that hindrances exist on your system and you should take tune or upgrade the affected resource.

Resource	Object\Counter	Suggested threshold	Comments
Disk	Physical Disk\% Free Space Logical Disk\% Free Space	15%	
Disk	Physical Disk\\% Disk Time Logical Disk\% Disk Time	90%	
Disk	Physical Disk\Disk Reads/sec, Physical Disk\Disk Writes/sec	Depends on manufacturer's specifications	Check the specified transfer rate for your disks to verify that this rate does not exceed the specifications. In general, Ultra Wide SCSI disks can handle 50 to 70 I/O operations per second.
Disk	Physical Disk\Current Disk Queue Length	Number of spindles plus 2	This is an instantaneous counter; observe its value over several intervals. For an average over time, use Physical Disk\Avg. Disk Queue Length.
Memory	Memory\Available Bytes	Less than 4 MB	Research memory usage and add memory if needed.
Memory	Memory\Pages/sec	20	Research paging activity.
Paging File	Paging File\% Usage	Above 70%	Review this value in conjunction with Available Bytes and Pages/sec to understand paging activity on your computer.
Processor	Processor\% Processor Time	85%	Find the process that is using a high percentage of processor time. Upgrade to a faster processor or install an additional processor.
Processor	Processor\Interrupts/sec	Depends on processor;	A dramatic increase in this counter value without a corresponding increase in system activity indicates a hardware problem. Identify the network adapter causing the interrupts. You might need to install an

		1000 interrupts per second is a good starting point	additional adapter or controller card.
Server	Server\Bytes Total/sec		If the sum of Bytes Total/sec for all servers is roughly equal to the maximum transfer rates of your network, you might need to segment the network.
Server	Server\Work Item Shortages	3	If the value reaches this threshold, consider adding the DWORD entries **InitWorkItems** (the number of work items allocated to a processor during start up) or **MaxWorkItems** (the maximum number of receive buffers that a server can allocate) to the registry (under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters). The entry **InitWorkItems** can range from 1 to 512 while **MaxWorkItems** can range from 1 to 65535. Start with any value for **InitWorkItems** and a value of 4096 for **MaxWorkItems** and keep doubling these values until the Server\Work Item Shortages threshold stays below 3. For information about modifying the registry, see Registry Editor Help. Caution • Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.
Server	Server\Pool Paged Peak	Amount of physical RAM	This value is an indicator of the maximum paging file size and the amount of physical memory.
Server	Server Work Queues\Queue Length	4	If the value reaches this threshold, there may be a processor hindrance. This is an instantaneous counter; observe its value over several intervals.
Multiple Processors	System\Processor Queue Length	2	This is an instantaneous counter; observe its value over several intervals.

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All computers on the network are members of the domain.
You administer a three-node Network Load Balancing cluster. Each cluster node runs Windows Server 2003 and has a single network adapter. The cluster has converged successfully.
You notice that the nodes in the cluster run at almost full capacity most of the time. You want to add a fourth node to the cluster. You enable and configure Network Load Balancing on the fourth node. However, the cluster does not converge to a four-node cluster. In the System log on the existing three nodes, you find the exact same TCP/IP error event. The event has the following description: "The system detected an address conflict for IP address 10.50.8.70 with the system having network hardware address 02:BF:0A:32:08:46."
In the System log on the new fourth node, you find a similar TCP/error event with the following description: "The system detected an address conflict for IP address 10.50.8.70 with the system having network hardware address 03:BF:0A:32:08:46." Only the hardware address is different in the two descriptions.
You verify that IP address 10.50.8.70 is configured as the cluster IP address on all four nodes.
You want to configure a four-node Network Load Balancing cluster.
What should you do?

A. Configure the fourth node to use multicast mode.
B. Remove 10.50.8.70 from the Network Connections Properties of the fourth node.
C. On the fourth node, run the nlb.exe resume command.
D. On the fourth node, run the wlbs.exe reload command.

Answer: A

Explanation: This normally happens when you don't enable the network load balancing service in TCP/IP of the server when adding two IP's (one for the server and one for the load balancing IP).
When you want to manage a NLB cluster with one network adapter you use multicast option.
My idea is since reload/suspend and remove the IP are all garbage answers could be that the other nodes are using multicast and this new node is using unicast that's why on a single network adapter configuration it will cause an IP conflict.
Reference: Syngress 070-293, Page 689

QUESTION 5
You are the network administrator for Certkiller . You need to provide Internet name resolution services for the company. You set up a Windows Server 2003 computer running the DNS Server service to provide this network service.
During testing, you notice the following intermittent problems:
• Name resolution queries sometimes take longer than one minute to resolve.
• Some valid name resolution queries receive the following error message in the Nslookup command
You suspect that there is a problem with name resolution.
You need to review the individual queries that the server handles. You want to configure monitoring on the DNS server to troubleshoot the problem.
What should you do?

A. In the DNS server properties, on the Debug Logging tab, select the Log packets for debugging option.
B. In the DNS server properties, on the Event Logging tab, select the Errors and warnings option.
C. In the System Monitor, monitor the Recursive Query Failure counter in the DNS object.
D. In the DNS server properties, on the Monitoring tab, select the monitoring options.

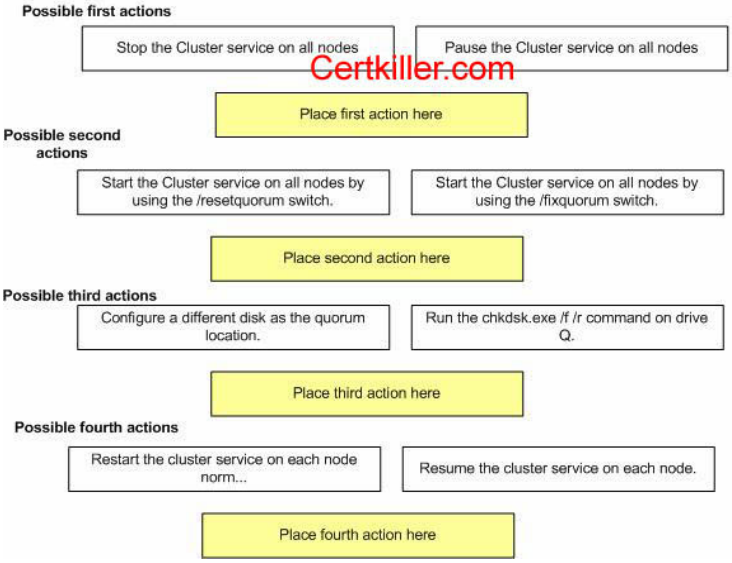
Answer: A

Explanation: If you need to analyze and monitor the DNS server performance in greater detail, you can use the optional debug tool.
You can choose to log
packets based on the following:
_ƒnTheir direction, either outbound or inbound
_ƒnThe transport protocol, either TCP or UDP
_ƒnTheir contents: queries/transfers, updates, or notifications
_ƒnTheir type, either requests or responses
_ƒnTheir IP address
Finally, you can choose to include detailed information.
Note: That's the only thing that's going to let you see details about packets.
Reference: Syngress 070-293, page 414
Troubleshooting DNS servers
Using server debug logging options
The following DNS debug logging options are available:
• Direction of packets
Send Packets sent by the DNS server are logged in the DNS server log file.

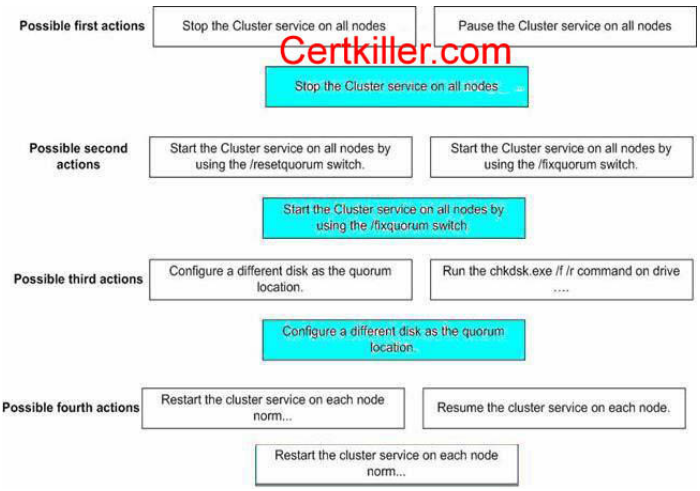
Receive Packets received by the DNS server are logged in the log file.
• Content of packets
Standard queries Specifies that packets containing standard queries (per RFC 1034) are logged in the DNS server log file.
Updates Specifies that packets containing dynamic updates (per RFC 2136) are logged in the DNS server log file.
Notifies Specifies that packets containing notifications (per RFC 1996) are logged in the DNS server log file.
• Transport protocol
UDP Specifies that packets sent and received over UDP are logged in the DNS server log file.
TCP Specifies that packets sent and received over TCP are logged in the DNS server log file.
• Type of packet
Request Specifies that request packets are logged in the DNS server log file (a request packet is characterized by a QR bit set to 0 in the DNS message header).
Response Specifies that response packets are logged in the DNS server log file (a response packet is characterized by a QR bit set to 1 in the DNS message header).
• Enable filtering based on IP address Provides additional filtering of packets logged in the DNS server log file. This option allows logging of packets sent from specific IP addresses to a DNS server, or from a DNS server to specific IP addresses.
• File name Lets you specify the name and location of the DNS server log file.
For example:
• dns.log specifies that the DNS server log file should be saved as dns.log in the systemroot

---

QUESTION 6
You are a network administrator for Certkiller .com. The network contains four Windows Server 2003 computers configured as a four-node server cluster.
The cluster uses drive Q for the quorum resource. You receive a critical warning that both drives of the mirrored volume that are dedicated to the quorum disk have failed.
You want to bring the cluster and all nodes back into operation as soon as possible.
Which four actions should you take to achieve this goal?
To answer, drag the action that you should perform first to the First Action box. Continue dragging actions to the corresponding numbered boxes until you list all four required actions in the correct order.



Answer:



Explanation:
To recover from a corrupted quorum log or quorum disk
1. If the Cluster service is running, open Computer Management.
2. In the console tree, double-click Services and Applications, and then click Services.
3. In the details pane, click Cluster Service.
4. On the Action menu, click Stop.
5. Repeat steps 1, 2, 3, and 4 for all nodes.
6. If you have a backup of the quorum log, restore the log by following the instructions in "Backing up and restoring server clusters" in Related Topics.
7. If you do not have a backup, select any given node. Make sure that Cluster Service is highlighted in the details pane, and then on the Action menu, click Properties.
Under Service status, in Start parameters, specify /fixquorum, and then click Start.
8. Switch from the problematic quorum disk to another quorum resource.
For more information, see "To use a different disk for the quorum resource" in Related Topics.
9. In Cluster Administrator, bring the new quorum resource disk online.
For information on how to do this, see "To bring a resource online" in Related Topics.
10. Run Chkdsk, using the switches /f and /r, on the quorum resource disk to determine whether the disk is corrupted.
For more information on running Chkdsk, see "Chkdsk" in Related Topics.
If no corruption is detected on the disk, it is likely that the log was corrupted. Proceed to step 12.
11. If corruption is detected, check the System Log in Event Viewer for possible hardware errors.
Resolve any hardware errors before continuing.
12. Stop the Cluster service after Chkdsk is complete, following the instructions in steps 1 - 4.
13. Make sure that Cluster Service is highlighted in the details pane. On the Action menu, click Properties.
Under Service status, in Start parameters, specify /resetquorumlog, and then click Start.
This restores the quorum log from the node's local database.
Important
• The Cluster service must be started by clicking Start on the service control panel. You cannot click OK or Apply to commit these changes as this does not preserve the /resetquorumlog

parameter.
14. Restart the Cluster service on all other nodes.

QUESTION 7
You are a network administrator for Certkiller . Certkiller has a main office and two branch offices. The branch offices are connected to the main office by T1 lines. The network consists of three Active Directory sites, one for each office. All client computers run either Windows 2000 Professional or Windows XP Professional. Each office has a small data center that contains domain controllers, WINS, DNS, and DHCP servers, all running Windows Server 2003.
Users in all offices connect to a file server in the main office to retrieve critical files. The network team reports that the WAN connections are severely congested during peak business hours. Users report poor file server performance during peak business hours. The design team is concerned that the file server is a single point of failure. The design team requests a plan to alleviate the WAN congestion during business hours and to provide high availability for the file server.
You need to provide a solution that improved file server performance during peak hours and that provides high availability for file services. You need to minimize bandwidth utilization.
What should you do?

A. Purchase two high-end servers and a shared fiber-attached disk array.
Implement a file server cluster in the main office by using both new servers and the shared fiber attached disk array.
B. Implement Offline Files on the client computers in the branch offices by using Synchronization Manager.
Schedule synchronization to occur during off-peak hours.
C. Implement a stand-alone Distributed File System (DFS) root in the main office.
Implement copies of shared folders for the branch offices.
Schedule replication of shared folders to occur during off-peak hours by using scheduled tasks.
D. Implement a domain Distributed File System (DFS) root in the main office.
Implement DFS replicas for the branch offices.
Schedule replication to occur during off-peak hours.

Answer: D

Explanation: A DFS root is effectively a folder containing links to shared files. A domain DFS root is stored in Active Directory. This means that the users don't need to know which physical server is hosting the shared files; they just open a folder in Active Directory and view a list of shared folders.
A DFS replica is another server hosting the same shared files. We can configure replication between the file servers to replicate the shared files out of business hours. The users in each office will access the files from a DFS replica in the user's office, rather than accessing the files over a WAN link.
Incorrect Answers:
A: This won't minimize bandwidth utilization because the users in the branch offices will still access the files over the WAN.
B: This doesn't provide any redundancy for the server hosting the shared files.
C: You need DFS replicas to use the replicas of the shared folders.

QUESTION 8
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All computers on the network are members of the domain. The domain contains a Windows Server 2003 computer named Certkiller A.
You are planning a public key infrastructure (PKI) for the company. You want to deploy an enterprise certification authority (CA) on Certkiller A.
You create a new global security group named Cert Approvers. You install an enterprise CA and configure the CA to issue Key Recovery Agent certificates.
The company's written security policy states that issuance of a Key Recovery Agent certificate requires approval from a member of the Cert Approvers group. All other certificates must be issued automatically.
You need to ensure that members of the Cert Approvers group can approve pending enrolment requests for a Key Recovery Agent certificate.
What should you?

A. Assign the Cert Approvers group the Allow - Enroll permissions for the Key Recovery Agent.
B. Assign the Cert Approvers group the Allow - Issue and Manage Certificates permission for the CA.
C. For all certificate managers, add the Cert Approvers group to the list of managed subjects.
D. Add the Cert Approvers group to the existing Cert Publisher group in the domain.
E. Assign the Cert Approvers group the Allow - Full Control permission for the Certificate Templates container in the Active Directory configuration naming context.

Answer: B
Explanations:
1. In order to approve certificates you need certificate manager rights.
2. In order to get those rights you need Issue and Manage Certificates rights.
3. The option to enable auto enroll or wait for approval is made at the certificate template (in this case the key recovery template).
From the windows 2003 help.

A. will allow enroll only.
C. will allow all certificate managers.
D. cert publisher group is meant to include the CA servers only.
E. no need to give them full control on the certificate template when we have role separation in windows 2003 pki.

QUESTION 9
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All computers on the network are members of the domain.
You are planning a public key infrastructure (PKI) for the company. You want to ensure that users who log on to the domain receive a certificate that can be used to authenticate to Web sites.
You create a new certificate template named User Authentication. You configure a Group Policy object (GPO) that applies to all users. The GPO specifies that user certificates must be enrolled when the policy is applied. You install an enterprise certification authority (CA) on a computer that runs Windows Server 2003.
Users report that when they log on, they do not have certificates to authenticate to Web sites that require

certificate authentication.
You want to ensure that users receive certificates that can be used to authenticate to Web sites.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. On the User Authenticate certificate template, select the Reenroll All Certificate Holders command.
B. Assign the Domain Users group the Allow - Autoenroll permission for the User Authentication certificate template.
C. Configure the CA to enable the User Authentication certificate template.
D. Assign the Domain Users group the Allow - Issue and Manage Certificates permission for the CA.

Answer: B, C
Explanation:
Certificate enrollment methods and domain membership
The domain membership of computers for which you want to enroll certificates affects the certificate enrollment method that you can choose.
Certificates for domain member computers can be enrolled automatically (also known as auto-enrollment), while an administrator must enroll certificates for non-domain member computers using the Web or a floppy disk.
The certificate enrollment method for non-domain member computers is known as a trust bootstrap process, through which certificates are created and then manually requested or distributed securely by administrators, to build common trust.
Allowing for auto enrollment
You can use auto enrollment so that subjects automatically enroll for certificates, retrieve issued certificates, and
renew expiring certificates without subject interaction.
For certificate templates, the intended subjects must have Read, Enroll and Autoenroll permissions before the subjects can enroll.
To ensure that unintended subjects cannot request a certificate based on this template, you must identify those unintended subjects and explicitly configure the Deny permission for them. This acts as a safeguard, further ensuring that they cannot even present an unacceptable request to the certification authority. Note that Read permission does not allow enrollment or auto enrollment, it only allows the subject to view the certificate template.
Renewal of existing certificates requires only the Enroll permission for the requesting subject.
Certificates obtained in any way, including auto enrollment and manual requests, can be renewed automatically. These types of renewals do not require Autoenroll permission, even if they are renewed automatically.
Planning for auto enrollment deployment
Auto enrollment is a useful feature of certification services in Windows XP and Windows Server 2003, Standard
Edition. Auto enrollment allows the administrator to configure subjects to automatically enroll for certificates, retrieve issued certificates, and renew expiring certificates without requiring subject interaction. The subject does not need to be aware of any certificate operations, unless you configure the certificate template to interact with the subject.
To properly configure subject auto enrollment, the administrator must plan the appropriate certificate template or
templates to use. Several settings in the certificate template directly affect the behavior of subject auto enrollment.

• On the Request Handling tab of the selected certificate template, the selection of an auto enrollment user interaction setting will affect auto enrollment:

•

Setting	Affect on auto enrollment behavior
Enroll subject without requiring any user input	This setting will allow "silent" auto enrollment without requiring the user to take any action. This setting is preferred when clients require certificates but may not be aware that they are using them.
Prompt the user during enrollment	The user will receive a message and may need to take an action when enrollment is performed. This action may be necessary when the certificate is intended for a smart card, which would require the user to provide their personal identification (PIN).
Prompt the user during the enrollment and require user input when the private key is used	This setting prompts the user both during enrollment and whenever private key is used. This is the most interactive auto enrollment behavior, as it requires the user to confirm all use of the private key. It is also the setting that provides the highest level of user awareness regarding key usage. Caution • This setting is provided to the client during certificate enrollment. The client should follow the configuration setting, but the setting is not enforced by the certification

---

QUESTION 10

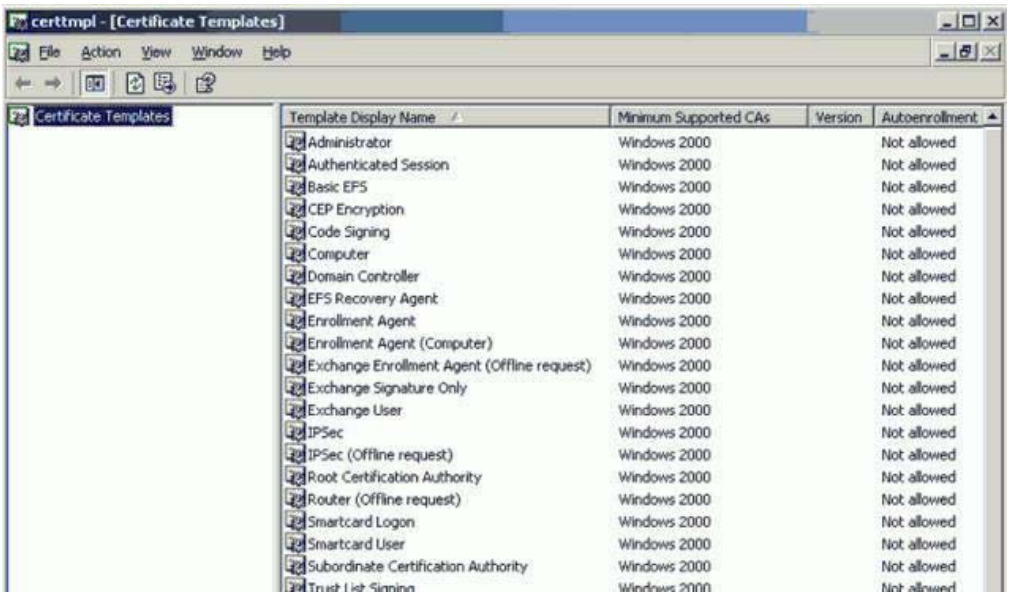
You are a network administrator for Certkiller . The network consists of a single Windows 2000 Active Directory forest that has four domains. All client computers run Windows XP Professional.

The company's written security policy states that all e-mail messages must be electronically signed when sent to other employees. You decide to deploy Certificate Services and automatically enroll users for email authentication certificates.

You install Windows Server 2003 on two member servers and install Certificate Services. You configure one Windows Server 2003 computer as a root certification authority (CA). You configure the other Windows Server 2003 server as an enterprise subordinate C

A. You open Certificate Templates on the

enterprise subordinate CA, but you are unable to configure certificates templates for auto enrollment. The Certificate Templates administration tool is shown in the exhibit.



You need to configure Active Directory to support auto enrollment of certificates.
What should you do?

A. Run the adprep /forestprep command on the schema operations master.
B. Place the enterprise subordinate CA's computer account in the Cert Publisher Domain Local group.
C. Run the adprep /domainprep command on a Windows 2000 Server domain controller that is in the same domain as the enterprise subordinate CA.
D. Install Active Directory on the Windows Server 2003 member server that is functioning as the enterprise subordinate CA.
Configure this server as an additional domain controller in the Windows 2000 Active Directory domain.

Answer: A

Explanation:
The auto enrollment feature has several infrastructure requirements. These include:
Windows Server 2003 schema and Group Policy updates
Windows 2000 or Windows Server 2003 domain controllers
Windows XP Client
Windows Server 2003, Enterprise Edition running as an Enterprise certificate authority (CA)
Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/maintain/certenrl.asp?frame=true
In this question, we have a Windows 2000 domain; therefore, we have Windows 2000 domain controllers. The Enterprise CA is running on a Windows Server 2003 member server which will work ok, but only if the forest schema is a Windows Server 2003 schema. We can update the forest schema with the adprep /forestprep command.
Incorrect Answers:
B: This will happen in the domain in which the CAs are installed.
C: The adprep /domainprep command prepares a Windows 2000 domain for an upgrade to a Windows Server 2003 domain. We are not upgrading the domain, so this isn't necessary.

D: The CA doesn't have to be installed on a domain controller. You can't install AD on a Windows 2003 server until you run the adprep commands.

QUESTION 11
You are a network administrator for Certkiller . The network contains a perimeter network. The perimeter network contains four Windows Server 2003, Web Edition computers that are configured as a Network Load Balancing cluster.
The cluster hosts an e-commerce Web site that must be available 24 hours per day. The cluster is located in a physically secure data center and uses an Internet-addressable virtual IP address. All servers in the cluster are configured with the Hisecws.inf template.
You need to implement protective measures against the cluster's most significant security vulnerability.
What should you do?

A. Use Encrypting File System (EFS) for all files that contain confidential data stored on the cluster.
B. Use packet filtering on all inbound traffic to the cluster.
C. Use Security Configuration and Analysis regularly to compare the security settings on all servers in the cluster with the baseline settings.
D. Use intrusion detection on the perimeter network.

Answer: B

Explanation: The most sensitive element in this case is the network card that uses an Internet-addressable virtual IP address. The question doesn't mention a firewall implementation or and intrusion detection system (Usually Hardware). Therefore, we should set up packet filtering.
REF: Deploying Network Services (Windows Server 2003 Reskit) Using a Perimeter Network
IP packet filtering
You can configure packet filtering, the earliest implementation of firewall technology, to accept or deny specific types of packets. Packet headers are examined for source and destination addresses, TCP and UDP port numbers, and other information. Packet filtering is a limited technology that works best in clear security environments where, for example, everything outside the perimeter network is not trusted and everything inside is. You cannot use IP packet filtering when IP packet payloads are encrypted because the port numbers are encrypted and therefore cannot be examined.
In recent years, various vendors have improved on the packet filtering method by adding intelligent decision-making
features to the packet-filtering core, thus creating a new form of packet filtering called stateful protocol inspection.

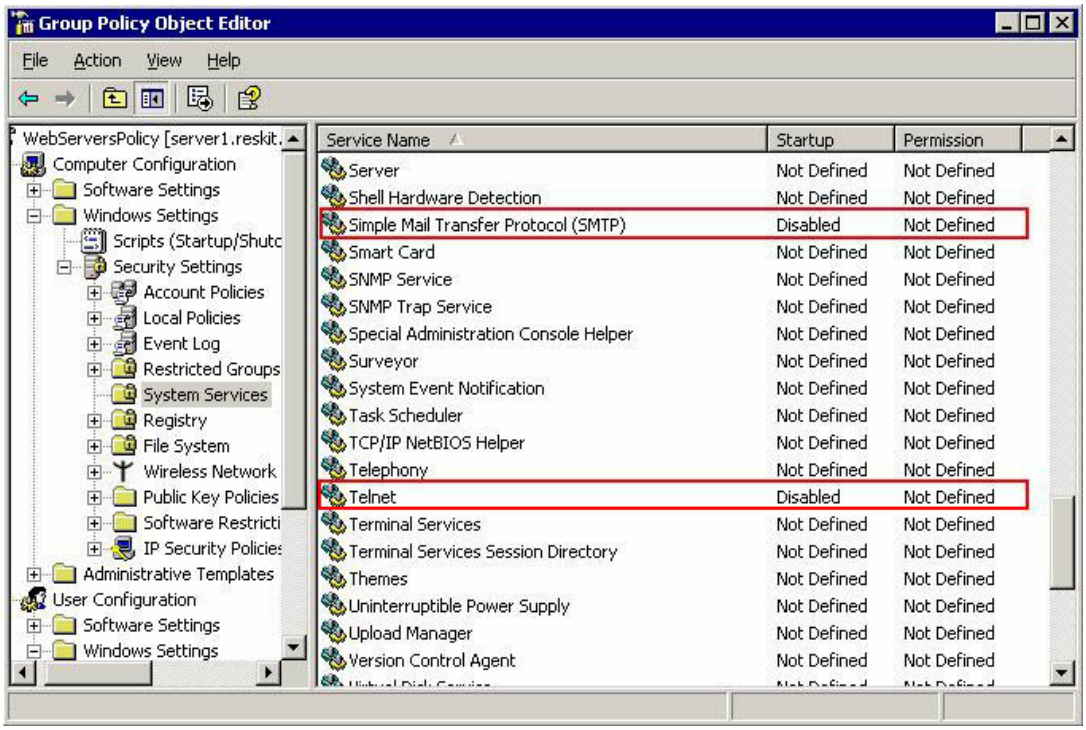
QUESTION 12
You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The network contains 80 Web servers that run Windows 2000 Server. The IIS Lockdown Wizard is run on all Web servers as they are deployed.
Certkiller is planning to upgrade its Web servers to Windows Server 2003. You move all Web servers into an organizational unit (OU) named Web Servers.
You are planning a baseline security configuration for the Web servers. The company's written security policy states that all unnecessary services must be disabled on servers. Testing shows that the server upgrade process leaves the following unnecessary services enabled:

• SMTP
• Telnet
Your plan for the baseline security configuration for Web servers must comply with the written security policy.
You need to ensure that unnecessary services are always disabled on the Web servers.
What should you do?

A. Create a Group Policy object (GPO) to apply a logon script that disables the unnecessary services.
Link the GPO to the Web Servers OU.
B. Create a Group Policy object (GPO) and import the Hisecws.inf security template.
Link the GPO to the Web Servers OU.
C. Create a Group Policy object (GPO) to set the startup type of the unnecessary services to Disabled.
Link the GPO to the Web Servers OU.
D. Create a Group Policy object (GPO) to apply a startup script to stop the unnecessary services.
Link the GPO to the Web Servers OU.

Answer: C

Explanation: The web servers have been moved to an OU. This makes it easy for us to configure the web servers using a group policy. We can simply assign a group policy to the Web Servers OU to disable the services.



Incorrect Answers:
A: The logon script would only run when someone logs on to the web servers. It's likely that the web servers will be running with no one logged in.
B: The Hisecws.inf security template is designed for workstations, not servers.
D: The startup script would only run when the servers are restarted. A group policy would be refreshed at regular intervals.

QUESTION 13
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. The domain contains Windows Server 2003 computers and Windows XP Professional computers. The domain consists of the containers shown in the exhibit.

All production server computer accounts are located in an organizational unit (OU) named Servers. All production client computer accounts are located in an OU named Desktops. There are Group Policy objects (GPOs) linked to the domain, to the Servers OU, and to the Desktop OU.
The company recently added new requirements to its written security policy. Some of the new requirements apply to all of the computers in the domain, some requirements apply to only servers, and some requirements apply to only client computers. You intend to implement the new requirements by making modifications to the existing GPOs.
You configure 10 new Windows XP Professional computers and 5 new Windows Server 2003 computers in order to test the deployment of settings that comply with the new security requirements by using GPOs. You use the Group Policy Management Console (GPMC) to duplicate the existing GPOs for use in testing.
You need to decide where to place the test computer accounts in the domain. You want to minimize the amount of administrative effort required to conduct the test while minimizing the impact of the test on production computers. You also want to avoid linking GPOs to multiple containers.
What should you do?

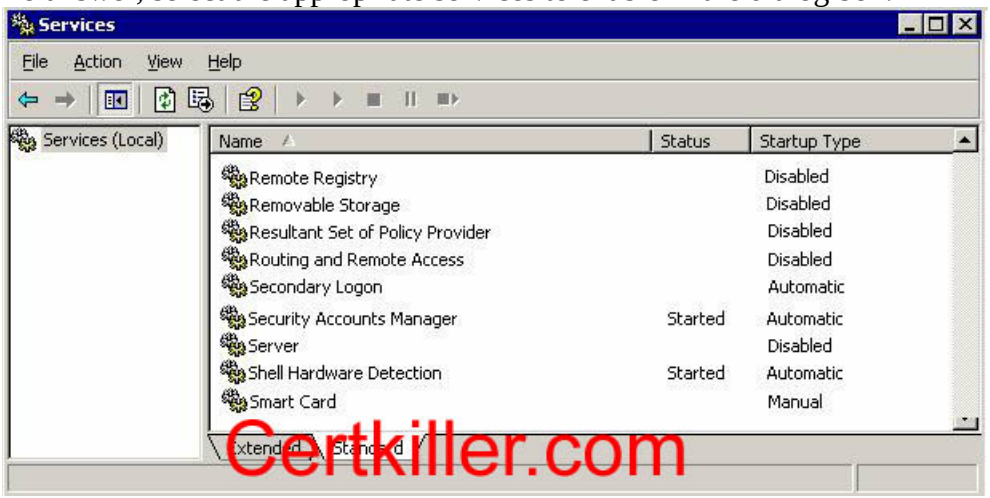
A. Place all test computer accounts in the Certkiller .com container.
B. Place all test computer accounts in the Computers container.
C. Place the test client computer accounts in the Desktops OU and the test server computer accounts in the Servers OU.
D. Create a child OU under the Desktops OU for the test client computer accounts.
Create a child OU under the Servers OU for the test server computer accounts.
E. Create a new OU named Test under the Certkiller .com container.
Create a child OU under the Test OU for the test client computer accounts.
Create a second child OU under the Test OU for the test server computer accounts.

Answer: E

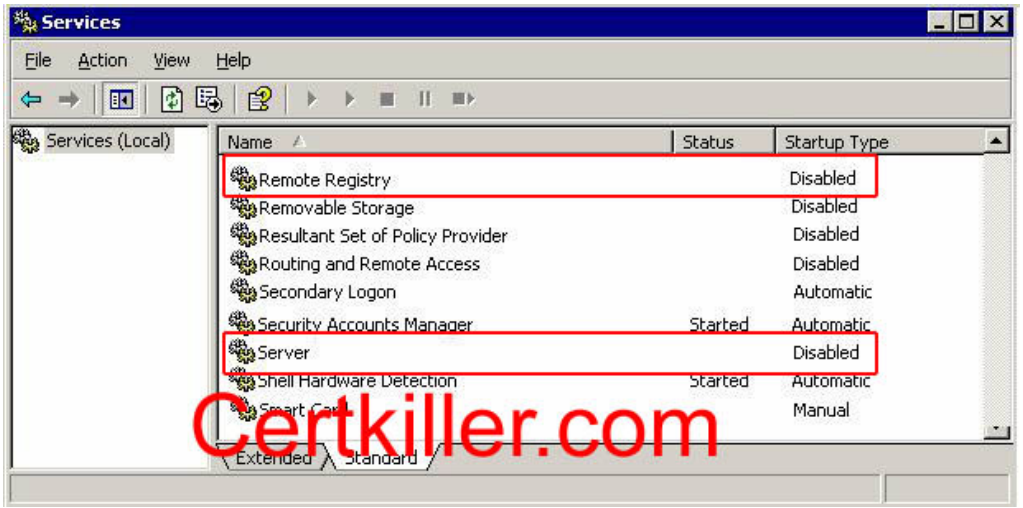
Explanation: To minimize the impact of the test on production computers, we can create a test OU with child OUs for the servers and the client computer accounts. Settings that should apply to the servers and client computers can be applied to the Test OU, and settings that should apply to the servers or the client computers can be applied to the appropriate child OUs.
Incorrect Answers:
A: You cannot place computer accounts directly under the domain container. They must be in an OU or in a

built in container such as the Computers container.
B: We need to separate the servers and the client computers into different OUs.
C: This solution would apply the new settings to existing production computers.
D: This could work but you would have more group policy links. For example, the GPO settings that need to apply to the servers and the client computers would need to be linked to both OUs. It would easier to link the GPO to a single parent OU.

QUESTION 14
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The network contains a Windows Server 2003 member server named Certkiller Srv
A. The network also contains a Windows XP Professional computer named Client1. You use Client1 as an administrative computer.
You plan to use Microsoft Baseline Security Analyzer (MBSA) on Client1 to analyze Certkiller SrvA. However, the recent application of a custom security template disabled several services on Certkiller SrvA.
You need to ensure that you can use MBSA to analyze Certkiller SrvA.
Which two services should you enable?
To answer, select the appropriate services to enable in the dialog box.



Answer:



Explanation: The Remote Registry and Server services should be enabled.
From the readme file for MBSA
The following are the requirements for a computer running the tool that is scanning remote machine(s):
Windows Server 2003, Windows 2000, or Windows XP
Internet Explorer 5.01 or greater
An XML parser (MSXML version 3.0 SP2 or later) is required in order for the tool to function correctly. Systems not running Internet Explorer 5.01 or greater will need to download and install an XML parser in order to run this tool. MSXML version 3.0 SP2 can be installed during tool setup. If you opt to not install the XML parser that is bundled with the tool, see the notes below on obtaining an XML parser separately.
The IIS Common Files are required on the computer on which the tool is installed if performing remote scans of IIS computers.
The following services must be enabled: Workstation service and Client for Microsoft Networks.
The following are the requirements for a computer to be scanned remotely by the tool:
Windows NT 4.0 SP4 and above, Windows 2000, Windows XP (local scans only on Windows XP computers that use simple file sharing), or Windows Server 2003
IIS 4.0, 5.0, 6.0 (required for IIS vulnerability checks)
SQL 7.0, 2000 (required for SQL vulnerability checks)
Microsoft Office 2000, XP (required for Office vulnerability checks)
The following services must be installed/enabled: Server service, Remote Registry service, File & Print Sharing

---

QUESTION 15
You are the network administrator for Certkiller . The network consists of a single Active Directory forest. The forest contains Windows Server 2003 servers and Windows XP Professional computers.
The forest consists of a forest root domain named Certkiller .com and two child domains named Asia. Certkiller .com and Europe. Certkiller .com. The Asia. Certkiller .com domain contains a member server named Certkiller 2. You configure Certkiller 2 to be an enterprise certification authority (CA), and you configure a user certificate template. You enable the Publish certificate in Active Directory setting in the certificate template. You instruct users in both the Asia. Certkiller .com and the Europe. Certkiller .com domains to enroll for user certificates.
You discover that the certificates for user accounts in the Asia. Certkiller .com domain are being published to Active Directory, but the certificates for user accounts in the Europe. Certkiller .com domain are not.
You want certificates issued by Certkiller 2 to Europe. Certkiller .com domain user accounts to be published in Active Directory.
What should you do?

A. Configure user certificate auto enrollment for all domain user accounts in the Certkiller .com domain.
B. Configure user certificate auto enrollment for all domain user accounts in the Europe. Certkiller .com domain.
C. Add Certkiller 2 to the Cert Publishers group in the Certkiller .com domain.
D. Add Certkiller 2 to the Cert Publishers group in the Europe. Certkiller .com domain.

Answer: D

Explanation: The problem here is that Certkiller SrvC doesn't have the necessary permission to publish certificates for users in child2. Certkiller .com. We can solve this problem by adding Certkiller SrvC to the Cert

Publisher group in the child2. Certkiller .com domain.
Reference: http://support.microsoft.com/default.aspx?scid=kb;en-us;219059

QUESTION 16
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The company has remote users in the sales department who work from home. The remote users' client computers run Windows XP Professional, and they are not members of the domain. The remote users' client computers have local Internet access through an ISP
Certkiller is deploying a Windows Server 2003 computer named Certkiller A that has Routing and Remote Access installed. Certkiller A will function as a VPN server, and the remote users will use it to connect to the company network. Confidential research data will be transmitted from the remote users' client computers. Security is critical to the company and Certkiller A must protect the remote users' data transmissions to the main office. The remote client computers will use L2TP/IPSec to connect to the VPN server.
You need to choose a secure authentication method.
What should you do?

A. Use the authentication method of the default IPSec policies.
B. Create a custom IPSec policy and use the Kerberos version 5 authentication protocol.
C. Create a custom IPSec policy and use certificate-based authentication.
D. Create a custom IPSec policy and use preshared authentication.
E. Use the authentication method of the Routing and Remote Access custom IPSec policy for L2TP connection.

Answer: C
Explanation
The security of a VPN is based on the tunneling and authentication protocols that you use and the level of encryption that you apply to VPN connections. For the highest level of security, use a remote access VPN based on L2TP/IPSec with certificate-based IPSec authentication and Triple-DES for encryption. If you decide to use a PPTP-based VPN solution to reduce costs and improve manageability and interoperability, use Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) as the authentication protocol.
Tunneling and authentication protocols, and the encryption levels applied to VPN connections, determine VPN security. L2TP/IPSec provides the highest level of security. For a VPN design, determine which VPN protocol best meets your requirements. Windows Server 2003 supports two VPN protocols: Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol with Internet Protocol security (L2TP/IPSec).
L2TP/IPSec
The more secure of the two VPN protocols, L2TP/IPSec uses PPP user authentication methods and IPSec encryption to encrypt IP traffic. This combination uses certificate-based computer identity authentication to create IPSec security associations in addition to PPP-based user authentication. L2TP/IPSec provides data integrity, data origin authentication, data confidentiality, and replay protection for each packet.
Support for L2TP/IPSec is provided with Windows Server 2003, as well as with Windows 2000 and Windows XP. To use L2TP/IPSec with the Microsoft(r) Windows(r) 98, Windows(r) Millennium Edition (Windows Me), or Windows NT(r) Workstation 4.0 operating system, download and install Microsoft L2TP/IPSec VPN Client (Mls2tp.exe).

Incorrect Answers:
A: The default IPSec policies don't require encryption.
B: We cannot use the Kerberos version 5 authentication protocol because the remote users are not members of the domain.
D: Pre-shared authentication uses a "password" that is known by the server and the client computers. This method is less secure than a certificate based method.
E: This answer sounds plausible, but the actual setting on RRAS "Allow Custom IPSec policy for L2TP connection" in the RRAS Server properties only allows a pre-shared key which is NOT secure compared to certificate-based IPSec policies.
Reference:
MS Windows Server 2003 Deployment Kit Deploying Network Services
Planning Security for a VPN
Selecting a VPN Protocol

QUESTION 17
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. The network contains 100 Windows XP Professional computers.
You configure a wireless network that requires IEEE 802.1x certificate-based authentication. Only 10 of the client computers are approved for wireless network access.
You need to enable the approved computers to access the wireless network while restricting access for all other computers.
What should you do?

A. Establish an enterprise certification authority (CA) for the domain.
Create a global group that contains the user accounts for the employees who will use the approved computers.
Create a certificate template for IEEE 802.1x authentication.
For the global group, configure auto enrollment for certificates based on the certificate template.
B. Establish an enterprise certification authority (CA) for the domain.
Create a global group that contains the approved computer accounts.
Create a certificate template for IEEE 802.1x authentication.
For the global group, configure the auto enrollment for certificates based on the certificate template.
C. Create a global group that contains the user accounts for the employees who will use the approved computers.
Configure the security permissions for the Default Domain Policy Group Policy object (GPO) so that only the new global group can apply to the GPO settings.
Establish an enterprise certification authority (CA) for the domain.
D. Create a global group that contains the approved computer accounts.
Configure the security permissions for the Default Domain Controllers Policy Group Policy object (GPO) so that only the new global group can apply the GPO settings.
Establish an enterprise certification authority (CA) for the domain.

Answer: B

Explanation: The question states that only 10 of the client computers are approved for wireless network access. Therefore we need to authenticate the computers to allow wireless access. Answer A is wrong because it suggests authenticating the users rather than the computers.
To plan for the configuration of Active Directory for your wireless clients, identify the user and computer accounts for wireless users, and add them to a group that will be used in conjunction with a remote access policy to manage wireless access. You must also determine how to set the remote access permission on the user and computer accounts
Provides options that allow you to specify how computer authentication works with user authentication.
If you select Computer only, authentication is always performed using the computer credentials. User authentication is never performed.
If you select With user re-authentication (recommended), when users are not logged on to the computer, authentication is performed using the computer credentials. After a user logs on to the computer, authentication is performed using the user credentials. When a user logs off of the computer, authentication is performed with the computer credentials.
If you select With user authentication, when users are not logged on to the computer, authentication is performed using the computer credentials. After a user logs on to the computer, authentication is maintained using the computer credentials. If a user travels to a new wireless access point, authentication is performed using the user credentials.
To create a policy we can do it at any level
To support a secure wireless solution, your existing network infrastructure must include the following components:
• Active Directory, to store account properties and validate password-based credentials.
• DHCP services, to provide automatic IP configuration to wireless clients.
• DNS services, to provide name resolution.
• RADIUS support, to provide centralized connection authentication, authorization, and accounting.
• A certificate infrastructure, also known as a PKI, to issue and validate the certificates required for Extensible Authentication Protocol-Transport Level Security (EAP-TLS) and Protected EAP (PEAP)-TLS authentication. TLS can use either smart cards or registry-based user certificates for authenticating the wireless client.
• For PEAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) authentication, computer certificates for the RADIUS servers and root CA certificates of the issuing CAs on the wireless clients (if needed).
Windows Server 2003 provides all of these components, with some variations in the levels of features supported and capabilities in different editions of the operating system (Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition).
IEEE 802.1X The 802.1X standard defines port-based network access control to provide authenticated network access for Ethernet networks. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard is designed for wired Ethernet networks, it applies to 802.11 WLANs as well.
Design Considerations for Wireless Network Policies
Consider the following issues that pertain to authentication methods and wireless network policies:
• Computer authentication is recommended. By default, authentication is set to Enabled.
• The access point must support the authentication method that you select. For example, the access point must support 802.1X. If you choose EAP-TLS, all computers must support it (for example, a RADIUS server must support EAP-TLS).

• Your servers and wireless clients must support the authentication method you plan to deploy. Whether you choose EAP-TLS or PEAP as the authentication method over 802.1X, both your RADIUS server and your wireless clients need to support it.
• It is recommended that you permit certificate auto enrollment for users and computer when you use EAP-TLS.
• The wireless network configuration settings that are defined in GPOs take precedence over user-defined settings. The only exception to this is the list of preferred networks, where the policy-defined list is merged with the user-defined list..
• If a domain policy for wireless configuration exists, the local user (whether the user is an administrator or non-administrator) cannot remove or disable the domain policy.
• When a Group Policy change occurs, the Wireless Configuration service breaks the current association if and only if the new policy takes precedence (for example, a visible network is now a more preferred network according to the policy's list of preferred networks). In all other cases, the association does not change.
• If a GPO that contains wireless network policies is deleted, the Wireless Configuration service clears its policy cache, initiates and processes a soft reset, and then reverts to the user-configured settings.

Creating Wireless Network Policies

You can define wireless network policies for your organization by using the Group Policy Object Editor snapin.

To access Wireless Network (IEEE 802.11) Policies

1. Open GPMC.
2. Right-click the GPO that you want to edit, and then click Edit.
3. In the Group Policy Object Editor console tree, click Computer Configuration, click Windows Settings, and then click Security Settings.
4. Right-click Wireless Network (IEEE 802.11) Policies on Active Directory, and then click Create Wireless Policies. The Wireless Policy Wizard starts.

Defining Wireless Configuration Options for Preferred Networks

By using the Properties page for your wireless configuration policy, you can define a list of preferred networks to use. You can use the General tab to specify how often to check for policy changes, which networks to access, whether to disable Zero Configuration, or automatically connect to non-preferred networks.

To define preferred wireless networks

1. Open GPMC.
2. In the console tree, expand the domain or OU that you want to manage, right-click the Group Policy object that you want to edit, and then click Edit.
3. In the Group Policy Object Editor console tree, click Computer Configuration, click Windows Settings, and then click Security Settings.
4. Click Wireless Network (IEEE 802.11) Policies, right-click the wireless network policy that you want to modify, and then click Properties.
5. Click the Preferred Networks tab, and then click Add.
6. Click the Network Properties tab, and then in the Name box, type a unique name.
7. In the Description box, type a description of the wireless network, such as the type of network and whether WEP and IEEE 802.1X authentication are enabled.
8. In the Wireless network key (WEP) box, specify whether a network key is used for encryption and authentication, and whether a network key is provided automatically. The options are:

o Data encryption (WEP enabled). Select this option to require that a network key be used for encryption.

o Network authentication (Shared mode). Select this option to require that a network key be

used for authentication. If this option is not selected, a network key is not required for authentication, and the network is operating in open system mode.
o The key is provided automatically. Select this option to specify whether a network key is automatically provided for clients (for example, whether a network key is provided for wireless network adapters).
9. To specify that the network is a computer-to-computer (ad hoc) network, click to select the This is a computer-to-computer (ad hoc) network; wireless access points are not used check box.
To define 802.1X authentication
1. Open GPMC.
2. In the console tree, expand the domain or OU that you want to manage, right-click the Group Policy object that you want to edit, and then click Edit.
3. In the Group Policy Object Editor console tree, click Computer Configuration, click Windows Settings, and then click Security Settings.
4. Click Wireless Network (IEEE 802.11) Policies, right-click the wireless network policy that you want to modify, and then click Properties.
5. On the Preferred Networks tab, under Networks, click the wireless network for which you want to define IEEE 802.1X authentication.
6. On the IEEE 802.1X tab, check the Enable network access control using IEEE 802.1X check box to enable IEEE 802.1X authentication for this wireless network. This is the default setting. To disable IEEE 802.1X authentication for this wireless network, clear the Enable network access control using IEEE 802.1X check box.
7. Specify whether to transmit EAPOL-start message packets and how to transmit them.
8. Specify EAPOL-Start message packet parameters.
9. In the EAP type box, click the EAP type that you want to use with this wireless network.
10. In the Certificate type box, select one of the following options:
o Smart card. Permits clients to use the certificate that resides on their smart card for authentication.
o Certificate on this computer. Permits clients to use the certificate that resides in the certificate store on their computer for authentication.
11. To verify that the server certificates that are presented to client computers are still valid, select the Validate server certificate check box.
12. To specify whether client computers must try authentication to the network, select one of the following check boxes:
o Authenticate as guest when user or computer information is unavailable. Specifies that the computer must attempt authentication to the network if user information or computer information is not available.
o Authenticate as computer when computer information is available. Specifies that the computer attempts authentication to the network if a user is not logged on. After you select this check box, specify how the computer attempts authentication.
References:
MS Windows Server 2003 Deployment
Deploying Network Services,
Overview of Deploying a Wireless LAN
WLAN Technology Background
Designing a Managed Environment
Creating Wireless Network Policies
Defining Wireless Configuration Options for Preferred Networks

QUESTION 18
You are the senior systems engineer for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Client computers in the sales department run Windows NT Workstation 4.0 with the Active Directory Client Extension software installed. All other client computers run Windows XP Professional. All servers are located in an organizational unit (OU) named Servers. All client computers are located in an OU named Desktops.
Four servers contain confidential company information that is used by users in either the finance department or the research department. Users in the sales department also store files and applications in these servers. The company's written security policy states that for auditing purposes, all network connections to these resources must require authentication at the protocol level. The written security policy also states that all network connections to these resources must be encrypted. The Certkiller budget does not allow for the purchase of any new hardware or software. The applications and data located on these servers may not be moved to any other server in the network.
You define and assign the appropriate permissions to ensure that only authorized users can access the resources on the servers.
You now need to ensure that all connections made to these servers by the users in the finance department and in the research department meet the security guidelines states by the written security policy. You also need to ensure that all users in the sales department can continue to access their resources.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Create a new Group Policy object (GPO) and link it to the Servers OU.
Enable the Secure Server (Require Security) IPSec policy in the GPO.
B. Create a new Group Policy object (GPO) and link to the Servers OU.
Enable the Server (Request Security) IPSec policy in the GPO.
C. Create a new Group Policy object (GPO) and link to the Desktops OU.
Enable the Client (Respond only) IPSec policy in the GPO.
D. Create a new Group Policy object (GPO).
Edit the GPO to enable the Registry Policy Processing option and the IP Security Policy Processing option.
Copy the GPO files to the Netlogon shared folder.
E. Use the System Policy Editor to open the System.adm file and enable the Registry Policy Processing option and the IP Security Policy Processing option.
Save the system policy as NTConfig.pol.

Answer: B, C

Explanation: We need to ensure that the connections made to the servers by the users in the finance department and in the research department meet the security guidelines states by the written security policy. The computers in these departments use Windows XP Professional. We can therefore enable IPSec communication between the servers and the clients in the finance and research departments. However, the sales users use Windows NT, which cannot use IPSec. Therefore, to ensure that the NT clients can still communicate with the servers, we should enable the Server (Request Security) IPSec policy on the servers and the Client (Respond only) IPSec policy for the client computers.

QUESTION 19
You are the systems engineer for Certkiller . The company has a main office in Las Palmas and two

branch offices, one in Barcelona and one in Madrid. The offices are connected to one another by dedicated T1 lines. Each office has its own local IT department and administrative staff.
The company 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 servers support firmware based console redirection by means of the serial port. The server hardware does not support any other method of console redirection and cannot be upgraded to do so.
The company is currently being reorganized. The IT department from each branch office is being relocated to a new central data center in the Las Palmas office. Several servers from each branch office are also being relocated to the Las Palmas data center. Each branch office will retain 10 servers. A new written security policy includes the following requirements:
• All servers must be remotely administered for all administrative tasks.
• All servers must be administered from the Las Palmas office.
• All remote administration connections must be authenticated and encrypted.
Your current network configuration already adheres to the new written security policy for day-to-day server administration tasks performed on the servers. You need to plan a configuration for out-of-band management tasks for each office that meets the new security requirements.
Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

A. Connect each server's serial port to a terminal concentrator.
Connect the terminal concentrator to the network.
B. Connect a second network adapter to each server.
Connect the second network adapter in each server to a separate network switch.
Connect the management port on the switch to a WAN port on the office router.
Enable IPSec on the router.
C. Enable Routing and Remote Access on a server in each branch office, and configure it as an L2TP/IPSec VPN server.
Configure a remote access policy to allow only authorized administrative staff to make a VPN connection.
D. On each server, enable the Telnet service with a startup parameter of Automatic.
Configure Telnet on each server to use only NTLM authentication.
Apply the Server (Request Security) IPSec policy to all servers.
E. On each server, enable Emergency Management Services console redirection and the Emergency Management Services Special Administration Console (SAC).

Answer: A, C, E

Explanation:
Special Administration Console Helper
You can use the Special Administration Console Helper system service to perform remote management tasks if the Windows Server 2003 family operating system stops functioning due to a Stop error message.
The main functions of Special Administration Console (!SAC)are to:
• Redirect Stop error message explanatory text
• Restart the system
• Obtain computer identification information
The !SAC is an auxiliary Emergency Management Services command - line environment that is hosted by Windows Server 2003 family operating systems. It also accepts input, and sends output through the out - of -

band port. SAC is a separate entity from both !SAC and Windows Server 2003 family command - line environments.
After a specific failure point is reached, Emergency Management Services components determine when the shift should be made from SAC to !SAC.!SAC becomes available automatically if SAC fails to load or is not functioning.
If the Special Administration Console Helper service is stopped, SAC services will no longer be available. If this service is disabled, any services that explicitly depend on this service will not start.

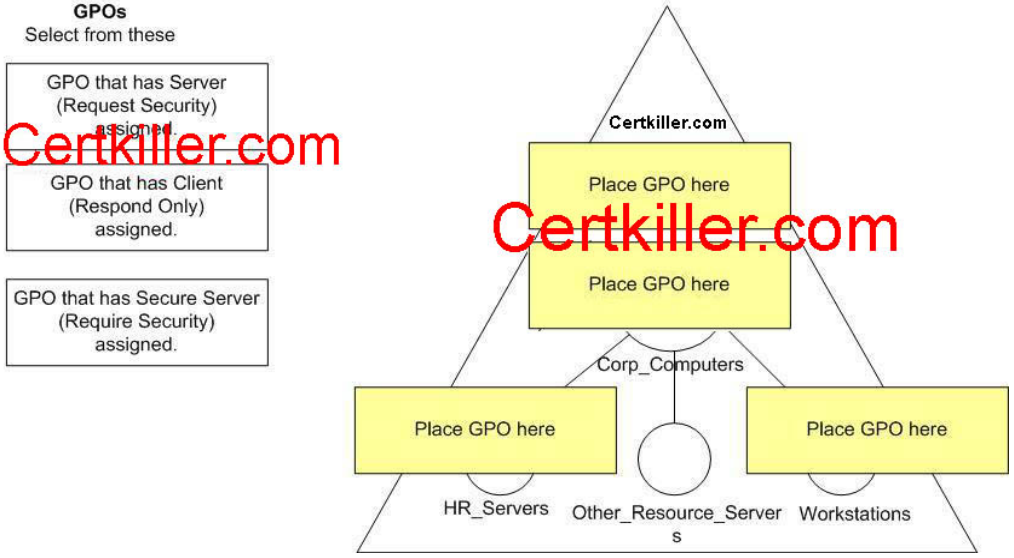
Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Sacsvr	Manual	Disabled	Disabled	Disabled

Terminal concentrators
A terminal concentrator is a hardware device that consolidates serial access to multiple servers into a single networked device. You can use this device to monitor a large number of servers simultaneously from one location.
Terminal concentrators include many serial ports
serial ports
An interface on the computer that allows asynchronous transmission of data characters one bit at a time. Also called a communication port or COM port.
connected to multiple servers using null modem cables
null modem cables
Special cabling that eliminates the modem's need for asynchronous communications between two computers over short distances. A null modem cable emulates modem communication.
Typically, you access terminal concentrators over the network through the Telnet
Telnet
A protocol that enables an Internet user to log on to and enter commands on a remote computer linked to the Internet, as if the user were using a text-based terminal directly attached to that computer. Telnet is part of the TCP/IP suite of protocols. The term telnet also refers to the software (client or server component) that implements this protocol.
protocol. Terminal concentrators provide an interface through which you can remotely view data on multiple servers that use serial ports as their out-of-band connection
out-of-band connection
A connection between two computers that relies on a nonstandard network connection, such as a serial port connection, and nonstandard remote administration tools, such as Special Administration Console (SAC). An out-of-band connection is usually used only when a remote computer cannot access a network or is not in a functional state because of hardware or software failure.
Terminal concentrators can improve your management of servers because they can establish in-band connections to the servers and then perform out-of-band management tasks. In addition, terminal concentrators make it easier to manage servers for the following reasons:
• You can use terminal concentrators to manage multiple servers without needing to be within a serial cable's distance to the computer.
• Several administrators can simultaneously view the output of different servers.
• Using an out-of-band connection, you can use terminal concentrators to monitor servers methodically. You can also manage multiple servers from one location.
Several companies manufacture terminal concentrators; their setup, features, and configuration details vary. When assessing the appropriateness of a particular terminal concentrator, consider the following:
• The number of serial ports available.

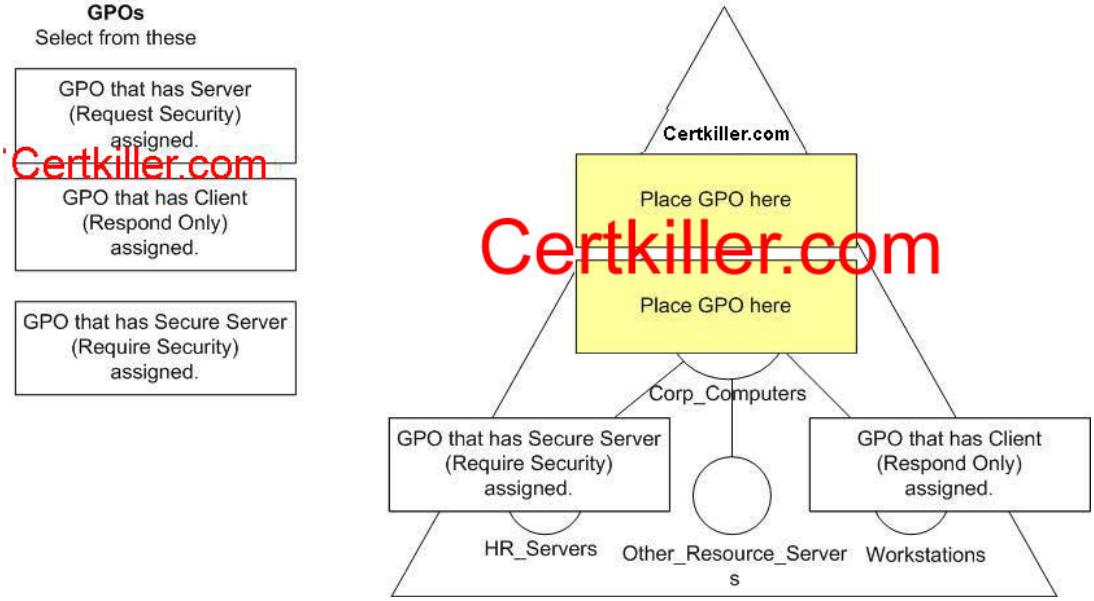
• Built-in Telnet security features, such as passwords.
• Remote-access capabilities.
• The number of Ethernet
Ethernet
The IEEE 802.3 standard that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the medium access control. Ethernet supports different mediums, such as coaxial cable, fiber-optic cable, and twisted-pair wiring, and different data rates, such as 10 megabits per second (Mbps).
ports available.
Telnet security features are not standard across terminal concentrators.
If your device does not include security features, consider using a secondary private management network accessible through a direct-dial remote access connection or a virtual private network (VPN)
Make sure that the terminal emulation software you use supports serial port and terminal definition settings that are compatible with Emergency Management Services, as well as with your service processor or system firmware. If possible, use terminal emulation software that supports the VT-UTF8 protocol because VT-UTF8 support for Unicode provides for multilingual versions of Windows. If English is the only language you need to support, the VT100+ terminal definition is sufficient. At minimum, you can use the VT100 definition, but this terminal definition requires that you manually enter escape sequences for function keys and so forth.
virtual private network (VPN)
The extension of a private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks. VPN connections can provide remote access and routed connections to private networks over the Internet.
connection. You can also use a router
router
Hardware that helps local area networks (LANs) and wide area networks (WANs) achieve interoperability and connectivity and that can link LANs that have different network topologies (such as Ethernet and Token Ring). Routers match packet headers to a LAN segment and choose the best path for the packet, optimizing network performance.
to secure network traffic going to the terminal concentrator.
References:
Server Help

QUESTION 20
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The domain contains four organizational units (OUs), as shown in the work area.
The HR_Servers OU contains 10 Windows Server 2003 computers that contain confidential human resources information. The Workstation OU contains all of the Windows XP Professional computers in the domain. All client computers need to communicate with the human resources servers.
The company's written security policy requires that all network communications with the servers that contain human resources data must be encrypted by using IPSec. Client computers must also be able to communicate with other computers that do not support IPSec.
You create three Group Policy objects (GPOs), one for each of the three default IPSec polices.
You need to link the GPOs to the appropriate Active Directory container or containers to satisfy the security and access requirements. You want to minimize the number of GPOs that are processed by any computer.

What should you do?
To answer, drag the appropriate GPO or GPOs to the correct Active Directory container or containers in the work area.



Answer:



Explanation: The servers in the HR_Servers OU require secure communications, so we must enable the Secure Server (Require Security) IPSec policy. The clients should have the Client (Respond Only) IPSec policy assigned. This means that when the clients communicate with an HR server, the server will demand the use of IPSec, and the client will be able to use IPSec. The clients will still be able to communicate with other computers without using IPSec.
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.
Understanding Default IPSec Policies

Windows Server 2003 includes three default IPSec policies that are provided as examples only. Do not use any part of the examples as templates to edit or change when creating your own IPSec policies. Instead, design new custom IPSec policies for operational use. The example policies will be overwritten during operating system upgrades and when IPSec policies are imported (when the import files contain other definitions of the same example policies). The three default IPSec policies are as follows:
• Client (Respond Only). This default policy contains one rule, the default response rule. The default response rule secures communication only upon request by another computer. This policy does not attempt to negotiate security for any other traffic.
• Server (Request Security). This default policy contains two rules: the default response rule and a second rule that allows initial incoming communication to be unsecured. The second rule then negotiates security for all outbound unicast IP traffic (security is not negotiated for multicast or broadcast traffic). The filter action for the second rule allows IKE to fall back to unsecured communication when required. This policy can be combined with the Client (Respond Only) policy when you want traffic secured by IPSec when possible, yet allow unsecured communication with computers that are not IPSec-enabled. If IKE receives a response from an IPSec-enabled client, but the IKE security negotiation fails, the communication is blocked. In this case, IKE cannot fall back to unsecured communication.
• Secure Server (Require Security). This default policy has two rules: the default response rule and a rule that allows the initial inbound communication request to be unsecured, but requires that all outbound communication be secured. The filter action for the second rule does not allow IKE to fall back to unsecured communication. If the IKE security negotiation fails, the outbound traffic is discarded and the communication is blocked. This policy requires that all connections be secured with IPSec. Any clients that are not IPSec-enabled cannot establish connections.
Reference
Server Help

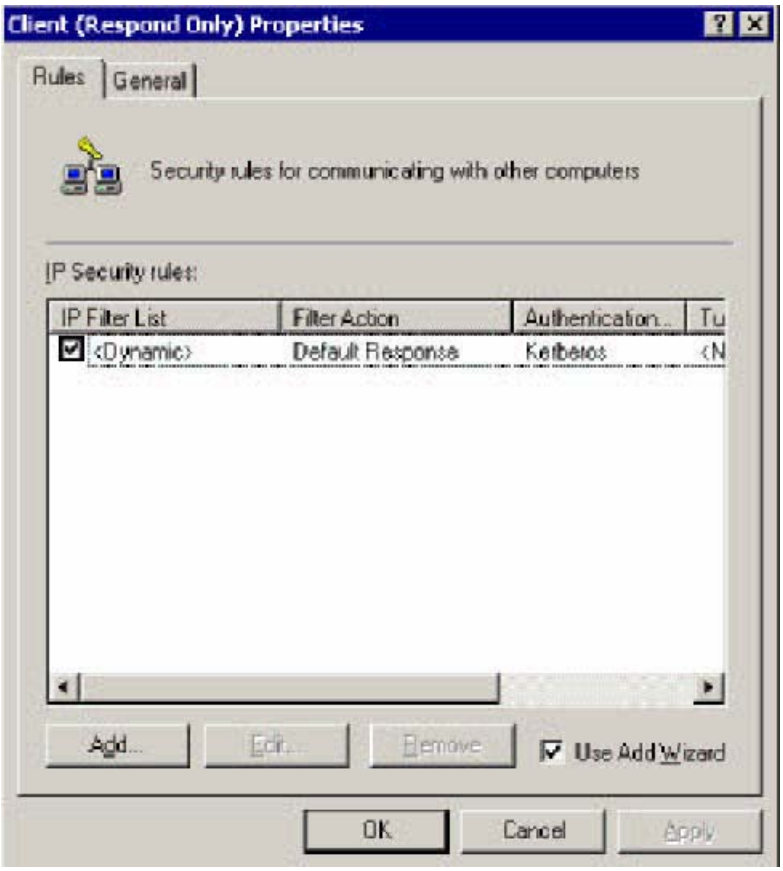
QUESTION 21
You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Client computers run Windows 2000 Professional, Windows XP Professional, or Windows NT Workstation 4.0.
Certkiller wants to increase the security of the communication on the network by using IPSec as much as possible. The company does not want to upgrade the Windows NT Workstation 4.0 client computers to another operating system. The servers use a custom IPSec policy named Domain Servers. The rules of the Domain Servers IPSec policy are shown in the exhibit.

You create a new Group Policy object (GPO) and link it to the domain. You configure the GPO to assign the predefined IPSec policy named Client (Respond Only). After these configuration changes, users of the Windows NT Workstation 4.0 computers report that they cannot connect to the servers in the domain. You want to ensure that Windows NT Workstation 4.0 client computers can connect to servers in the domain.
What should you do?

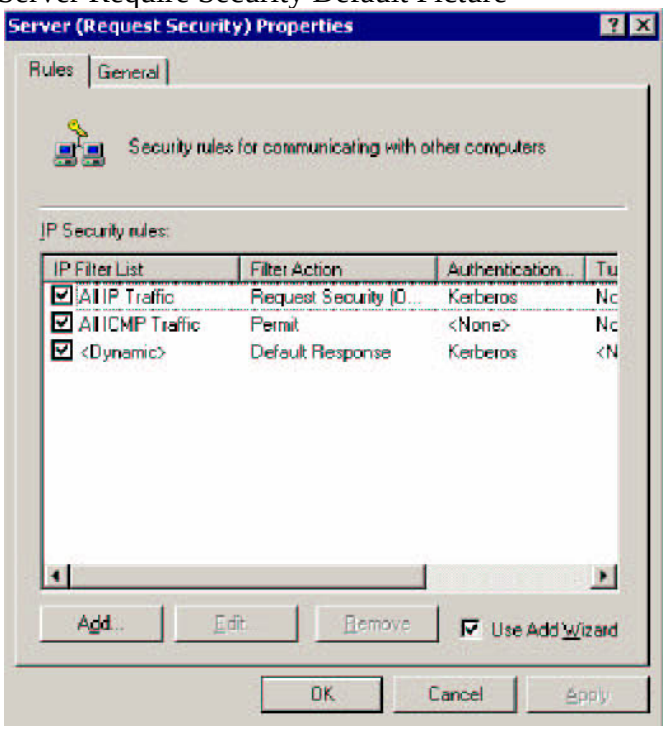
A. Change the All IP Traffic rule in the Domain Servers IPSec policy to use a preshared key for authentication.
B. Change the All IP Traffic rule in the Domain Servers IPSec policy to use the Request Security (Optional) filter action.
C. Activate the default response rule for the Domain Servers IPSec policy.
D. Install the Microsoft L2TP/IPSec VPN Client software on the Windows NT Workstation 4.0 computers.
E. Install the Active Directory Client Extensions software on the Windows NT Workstation 4.0 computers.

Answer: B

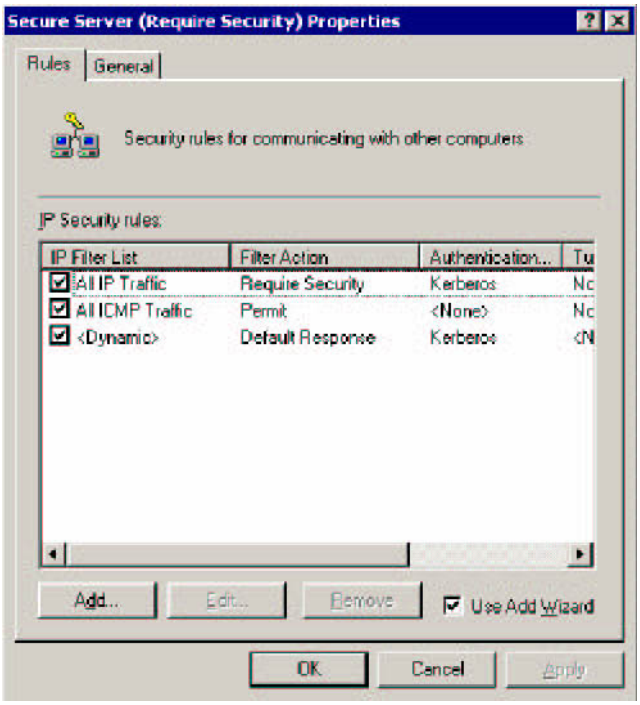
Explanation: The exhibit shows that the server has the "Require Security" IPSec policy. The Windows NT Workstation clients are unable to use IPSec, and so cannot communicate with the server. We can fix this by changing the IPSec policy to Request Security (Optional). This will configure the server to use IPSec whenever possible, but to allow unsecured communications if required.
Client Only Default Response Picture



Server Require Security Default Picture



Server Request Security Default Picture



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.

Understanding Default IPSec Policies

Windows Server 2003 includes three default IPSec policies that are provided as examples only. Do not use any part of the examples as templates to edit or change when creating your own IPSec policies. Instead, design new custom IPSec policies for operational use. The example policies will be overwritten during operating system upgrades and when IPSec policies are imported (when the import files contain other definitions of the same example policies). The three default IPSec policies are as follows:

• Client (Respond Only). This default policy contains one rule, the default response rule. The default response rule secures communication only upon request by another computer. This policy does not attempt to negotiate security for any other traffic.

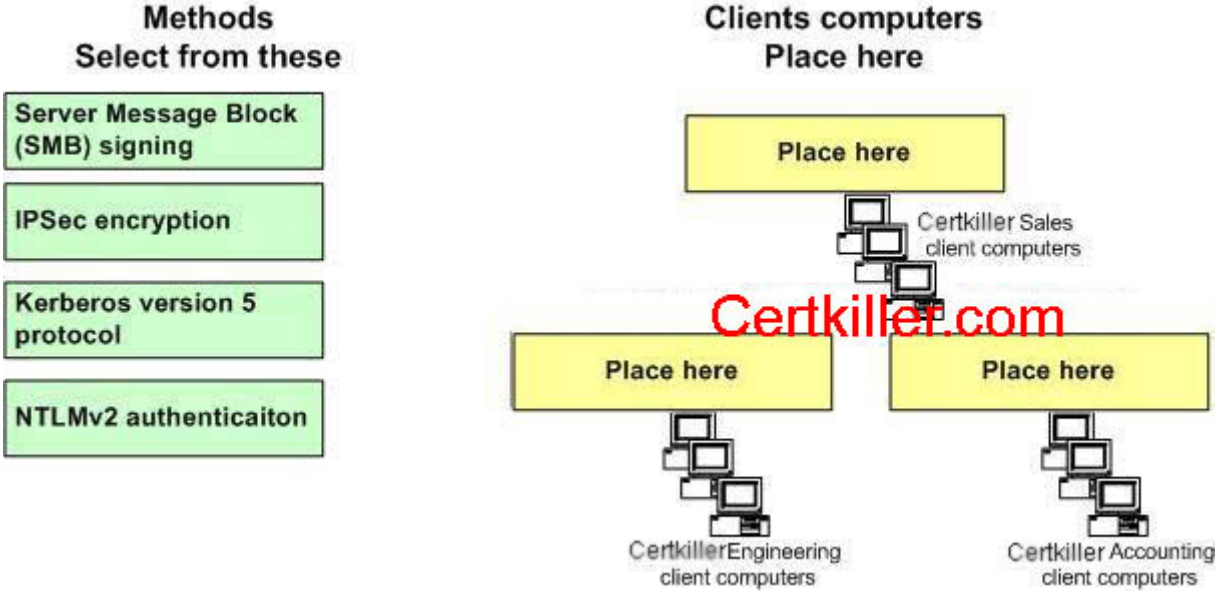
• Server (Request Security). This default policy contains two rules: the default response rule and a second rule that allows initial incoming communication to be unsecured. The second rule then negotiates security for all outbound unicast IP traffic (security is not negotiated for multicast or broadcast traffic). The filter action for the second rule allows IKE to fall back to unsecured communication when required. This policy can be combined with the Client (Respond Only) policy when you want traffic secured by IPSec when possible, yet allow unsecured communication with computers that are not IPSec-enabled. If IKE receives a response from an IPSec-enabled client, but the IKE security negotiation fails, the communication is blocked. In this case, IKE cannot fall back to unsecured communication.

• Secure Server (Require Security). This default policy has two rules: the default response rule and a rule that allows the initial inbound communication request to be unsecured, but requires that all outbound communication be secured. The filter action for the second rule does not allow IKE to fall back to unsecured communication. If the IKE security negotiation fails, the outbound traffic is discarded and the communication is blocked. This policy requires that all connections be secured with IPSec. Any clients that are not IPSec-enabled cannot establish connections.

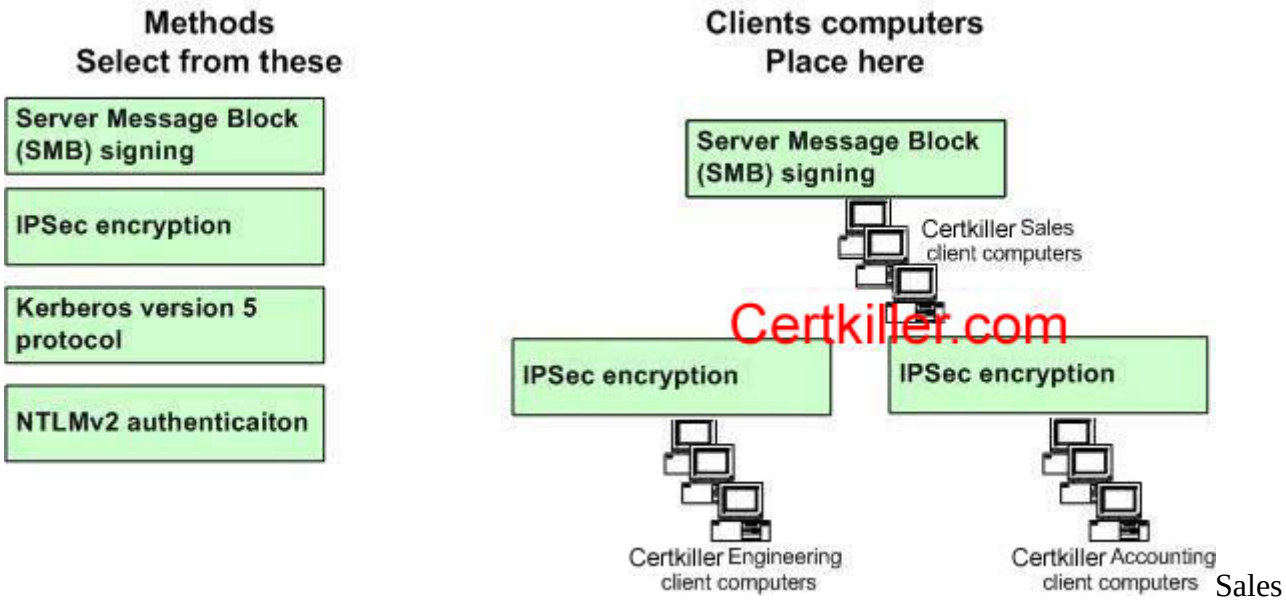
Reference

Server Help

QUESTION 22
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003. All application servers run Windows Server 2003.
Client computers in the accounting department run Windows XP Professional. Client computers in the engineering department run Windows 2000 Professional. Client computers in the sales department run either Windows NT Workstation 4.0 or Windows 98. All client computers access data files on the application servers.
You need to plan the method of securing the data transmissions for the client computers. You want to ensure that the data is not modified while it is transmitted between the application servers and the client computers. You also want to protect the confidentiality of the data, if possible.
What should you do?
To answer, drag the appropriate method or methods to the correct department's client computers.



Answer:



Sales

Explanation

We can use IPSEC on Windows 2000 and Windows XP but we cannot use IPSEC for Legacy clients except for VPNs.

Sales contains Windows NT 4.0 and Windows 98; in this case we use SMB signing.

With Windows 2000 and Windows XP both methods are supported in this case and for security reasons we will use IPSEC rules.

SMB signed is supported by Windows 2000 an XP by local policies or domain policies to be enforced

To be supported in legacy clients you must modify the registry in Windows 98 and Windows NT

SMB on Windows 98 KB article 230545

Windows 98 includes an updated version of the SMB authentication protocol. However, using SMB signing slows down performance when it is enabled. This setting should be used only when network security is a concern. The performance decrease usually averages between 10-15 percent. SMB signing requires that every packet is signed for and every packet must be verified.

SMB on Windows NT KB article 161372

Windows NT 4.0 Service Pack 3 provides an updated version of the Server Message Block (SMB) authentication protocol, also known as the Common Internet File System (CIFS) file sharing protocol

IPSEC

The Internet Protocol Security (IPsec) feature in Windows 2000, Windows XP and Windows Server 2003 was not designed as a full-featured host-based firewall. It was designed to provide basic permit and block filtering by using address, protocol and port information in network packets. IPsec was also designed as an administrative tool to enhance the security of communications in a way that is transparent to the programs. Because of this, it provides traffic filtering that is necessary to negotiate security for IPsec transport mode or IPsec tunnel mode, primarily for intranet environments where machine trust was available from the Kerberos service or for specific paths across the Internet where public key infrastructure (PKI) digital certificates can be used.

IPSEC is not supported on legacy clients just is supported for VPN

http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp

Microsoft L2TP/IPSec VPN Client is a free download that allows computers running Windows 98, Windows Millennium Edition (Me), or Windows NT(r) Workstation 4.0 to use Layer Two Tunneling Protocol (L2TP) connections with Internet Protocol security (IPSec).

Windows 98 (all versions) with Microsoft Internet Explorer 5.01 (or later) and the Dial-up Networking version 1.4 upgrade.
Windows Me with the Virtual Private Networking communications component and Microsoft Internet Explorer 5.5 (or later)
Windows NT Workstation 4.0 with Remote Access Service (RAS), the Point-to-Point Tunneling Protocol, Service Pack 6, and Microsoft Internet Explorer 5.01 (or later)

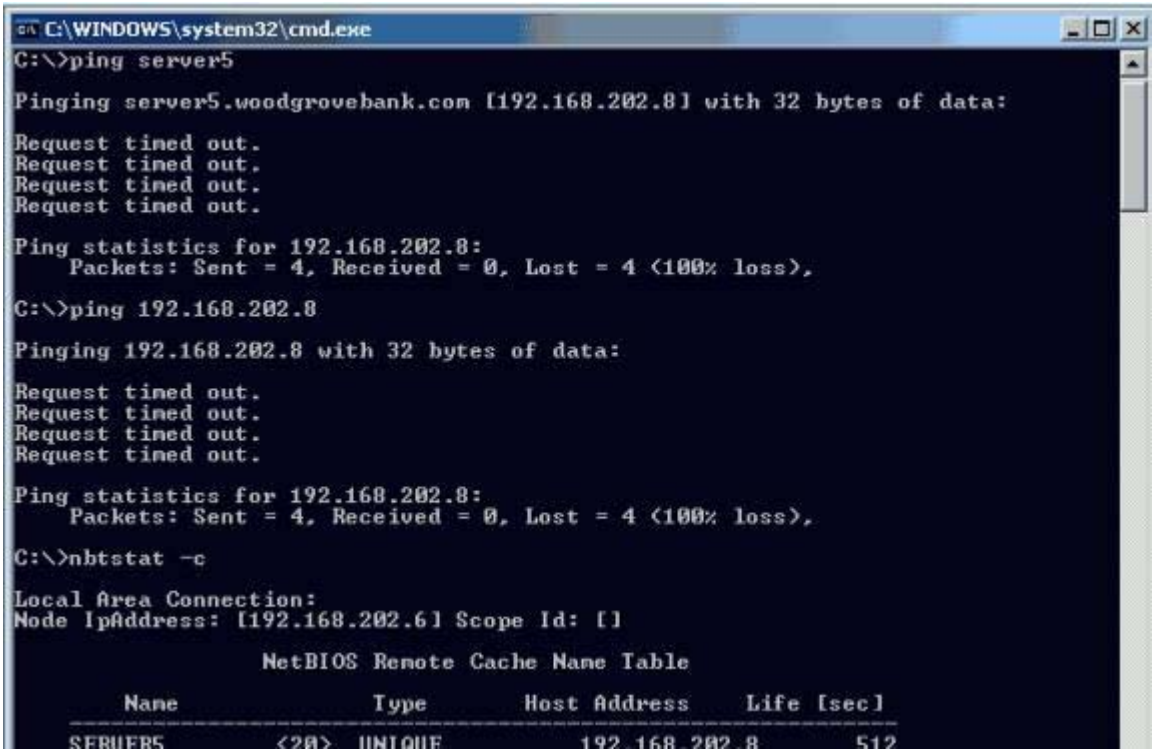
QUESTION 23
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The network contains 10 domain controllers and 50 servers in application server roles. All servers run Windows Server 2003.
The application servers are configured with custom security settings that are specific to their roles as application servers. Application servers are required to audit account logon events, object access events, and system events. Application servers are required to have passwords that meet complexity requirements, to enforce password history, and to enforce password aging. Application servers must also be protected against man-in-the-middle attacks during authentication.
You need to deploy and refresh the custom security settings on a routine basis. You also need to be able to verify the custom security settings during audits.
What should you do?

A. Create a custom security template and apply it by using Group Policy.
B. Create a custom IPSec policy and assign it by using Group Policy.
C. Create and apply a custom Administrative Template.
D. Create a custom application server image and deploy it by using RIS.

Answer: A

Explanation: The easiest way to deploy multiple security settings to a Windows 2003 computer is to create a security template with all the required settings and import the settings into a group policy. We can also use secedit to analyze the current security settings to verify that the required security settings are in place.
Incorrect Answers:
B: An IPSec policy will not configure the required auditing policy.
C: We need a security template, not an administrative template.
D: This will create multiple identical machines. We cannot use RIS images in this scenario.

QUESTION 24
You are a network administrator for Woodgrove Bank. All servers run Windows Server 2003. The company uses WINS and DNS for name resolution. The LMHosts and Hosts files are not used.
A user on a server named Server2 reports that when she attempts to map a network drive to a shared folder on a server named Server5 by name, she received the following error message: "System error 67 has occurred. The network name cannot be found". The user was previously able to map network drives by name to shared folders on Server5 from Server2.
You run the ping command on Server2 to troubleshoot the problem. The results of your troubleshooting are shown in the exhibit.



You need to allow the user on Server2 to connect to resources on Server5 both by name and by address. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. On Server2, purge and reload the remote NetBIOS cache name table.
B. Re-register Server5 with WINS.
C. On Server2, run the ipconfig command with the /flushdns option.
D. On Server5, run the ipconfig command with the /renew option.
E. On Server5, run the ipconfig command with the /registerdns option.

Answer: B, E

Explanation: The server doesn't answer to dns name or ip address which means either he is offline or he has changed his ip and is still registered with the old ip(192.168.202.8).
Ipconfig /registerdns will register in dns, and wins re-register will register the server with wins.

QUESTION 25
You are a network administrator for Certkiller . The network consists of multiple physical segments. The network contains two Windows Server 2003 computers named Certkiller SrvA and Certkiller SrvB, and several Windows 2000 Server computers. Certkiller SrvA is configured with a single DHCP scope for the 10.250.100.0/24 network with an IP address range of 10.250.100.10 to 10.250.100.100
Several users on the network report that they cannot connect to file and print servers, but they can connect to each other's client computers. All other users on the network are able to connect to all network resources. You run the ipconfig.exe /all command on one of the affected client computers and observe the information in the following table:
IP Address 10.250.100.150

Subnet Mask	255.255.255.0
Default Gateway	(blank)
DHCP Server	Certkiller Srv B
DNS Servers	(blank)
Primary WINS Sever	(blank)

You need to configure all affected client computers so that they can communicate with all other hosts on the network.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Disable the DHCP service on Certkiller Srv B.
B. Increase the IP address range for the 10.250.100.0/24 scope on Certkiller SrvA.
C. Add global DHCP scope options to Certkiller SrvA for default gateway, DNS servers, and WINS servers.
D. Delete all IP address reservation in the scope on Certkiller SrvA.
E. Run the ipconfig.exe /renew command on all affected client computers.
F. Run the ipconfig.exe /registerdns command on all affected client computers.

Answer: A, E

Explanation: We can see from the exhibit that the affected computer received it's IP configuration from Certkiller SrvB. We can also see that the IP configuration has no default gateway, WINS or DNS addresses. Obviously, Certkiller SrvB is misconfigured. Other client computers have no problems; it is likely that they get their IP configuration from Certkiller Srv
A. We can either correctly configure the DHCP service on
Certkiller SrvB or we can disable it and just use Certkiller SrvA as the DHCP server. The only option given is to
disable the DHCP service on Certkiller SrvB, so answer A is correct.
We need to run the ipconfig /renew command on all affected client computers so that they can update their IP configurations using Certkiller SrvA as their DHCP server.
Incorrect Answers:
B: The client computer received its IP configuration from Certkiller SrvB. Therefore, the problem is likely to be with Certkiller SrvB, not Certkiller SrvA.
C: Some client computers have no problems; it is likely that they get their IP configuration from
Certkiller Srv
A. Therefore, Certkiller SrvA is correctly configured.
D: The client computer received its IP configuration from Certkiller SrvB. Therefore, the problem is likely to be with Certkiller SrvB, not Certkiller SrvA.
F: The affected client computers have no DNS configuration; therefore this command will have no affect.

QUESTION 26
You are the network administrator for Certkiller . The company has a main office and two branch offices. The network in the main office contains 10 servers and 100 client computers. Each branch office contains 5 servers and 50 client computers. Each branch office is connected to the main office by a direct T1 line.
The network design requires that company IP addresses must be assigned from a single classful private IP address range. The network is assigned a class C private IP address range to allocate IP addresses for servers and client computers.

Certkiller acquires a company named Acme. The acquisition will increase the number of servers to 20 and the number of client computers to 200 in the main office. The acquisition is expected to increase the number of servers to 20 and the number of client computers to 200 in the branch offices. The acquisition will also add 10 more branch offices. After the acquisition, all branch offices will be the same size. Each branch office will be connected to the main office by a direct T1 line. The new company will follow the Certkiller network design requirements.
You need to plan the IP addressing for the new company. You need to comply with the network design requirement.
What should you do?

A. Assign the main office and each branch office a new class A private IP address range.
B. Assign the main office and each branch office a new class B private IP address range.
C. Assign the main office and each branch office a subnet from a new class B private IP address range.
D. Assign the main office and each branch office a subnet from the current class C private IP address range.

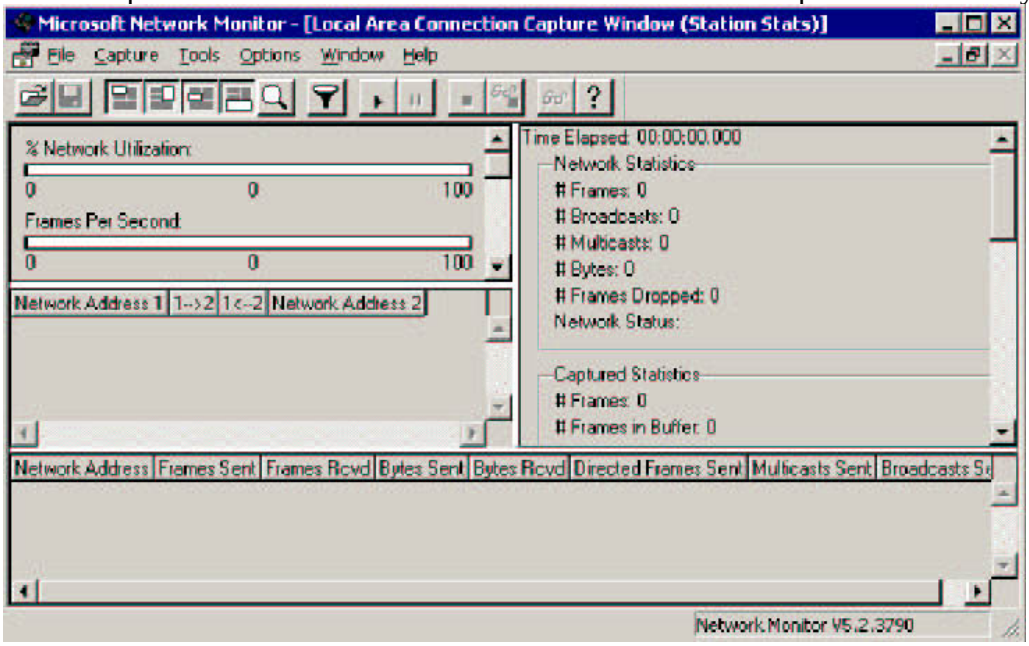
Answer: B
Explanation
After the expansion the situation will be:
• Main office
o Need 220 IP, 20 for servers and 200 for clients
• Branch Offices
o Need 220 IP, 20 for servers and 200 for clients
o We will have 12 branch offices
o 12 x 220 = 2640
Total for all offices is 2640 + 220 = 2860.
The network design requires that company IP addresses must be assigned from a single classful private IP address range. We can subnet a private Class B address range into enough subnets to accommodate each office. There are various ways of doing this, but one way would be to subnet the class B address into subnets using a 24 bit subnet mask. This would allow up to 254 IP addresses per subnet and up to 254 subnets.
Incorrect Answers:
A: The network design requires that company IP addresses must be assigned from a single classful private IP address range.
B: The network design requires that company IP addresses must be assigned from a single classful private IP address range.
D: The class C network doesn't have enough IP addresses to accommodate all the computers in all the offices.

QUESTION 27
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The network contains an application server running Windows Server 2003. Users report intermittent slow performance when they access the application server throughout the day. You find out that the network interface on the application server is being heavily used during the periods of slow performance. You suspect that a single computer is causing the problem.
You need to create a plan to identify the problem computer.
What should you do?

A. Monitor the performance monitor counters on the application server by using System Monitor.

B. Monitor the network traffic on the application server by using Network Monitor.
C. Monitor network statistics on the application server by using Task Manager.
D. Run network diagnostics on the application server by using Network Diagnostics.

Answer: B
Explanation:
Network Monitor Capture Utility
Network Monitor Capture Utility (Netcap.exe) is a command-line Support Tool that allows a system administrator to monitor network packets and save the information to a capture (.cap) file. On first use, Network Monitor Capture Utility installs the Network Monitor Driver.
You can use information gathered by using Network Monitor Capture Utility to analyze network use patterns and diagnose specific network problems.
This command-line tool allows a system administrator to monitor packets on a LAN and write the information to a log file. NetCap uses the Network Monitor Driver to sniff packets on local network segments.
Notes
• You must run NetCap from the command window.
• If the Network Monitor Driver is not installed, NetCap installs it the first time the tool is run. To remove the driver, use netcap /remove.
Corresponding UI
This tool provides a command-line interface to some of the capture functionality of Netmon.



Concepts
NetCap captures frames directly from the network traffic data stream so they can be examined. You can use it to create capture files for support personnel.
Frames are packages of information transmitted as a single unit over a network. Every frame follows the same basic organization and contains the following:
• Control information such as synchronizing characters
• Source and destination addresses
• Protocol information
• An error-checking value

• A variable amount of data
System Requirements
NetCap requires one of the following operating systems:
• Windows Server 2003
• Windows XP Professional
• Windows 2000
File Required
• Netcap.exe
References:
Resource Kit Windows XP:
• Appendix D - Tools for Troubleshooting
Server Help:
• Performance Monitoring and Scalability Tools
Network Monitor
Network Monitor captures network traffic information and gives detailed information about the frames being sent and received. This tool can help you analyze complex patterns of network traffic. Network Monitor can help you view the header information included in HTTP and FTP requests. Generally, you need to design a capture filter, which functions like a database query and singles out a subset of the frames being transmitted. You can also use a capture trigger that responds to events on your network by initiating an action, such as starting an executable file. An abbreviated version of Network Monitor is included with members of the Windows Server 2003 family. A complete version of Network Monitor is included with Microsoft Systems Management Server.

QUESTION 28
You are a network administrator for Certkiller . The internal network has an Active Directory-integrated zone for the Certkiller .org domain. Computers on the internal network use the Active Directory-integrated DNS service for all host name resolution.
The Certkiller Web site and DNS server are hosted at a local ISP. The public Web site for Certkiller is accessed at www. Certkiller .com. The DNS server at the ISP hosts the Certkiller .com domain.
To improve support for the Web site, Certkiller wants to move the Web site and DNS service from the ISP to the company's perimeter network. The DNS server on the perimeter network must contain only the host (A) resource records for computers on the perimeter network.
You install a Windows Server 2003 computer on the perimeter network to host the DNS service for the Certkiller .com domain. You need to ensure that the computers on the internal network can properly resolve host names for all internal resources, all perimeter resources, and all Internet resources.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. On the DNS server that is on the perimeter network, install a primary zone for Certkiller .com.
B. On the DNS server that is on the perimeter network, install a stub zone for Certkiller .com.
C. Configure the DNS server that is on the internal network to conditionally forward lookup requests to the DNS server that is on the perimeter network.
D. Configure the computers on the internal network to use one of the internal DNS servers as the preferred DNS server.
Configure the TCP/IP settings on the computers on the internal network to use the DNS server on the perimeter network as an alternate DNS server.
E. On the DNS server that is on the perimeter network, configure a root zone.

Answer: A, C

Explanation:
By configuring a primary zone for Certkiller .com on a DNS server in the perimeter network, we have a DNS server that can resolve requests for the www. Certkiller .com website. To enable users on the LAN to quickly resolve Certkiller .com resources, we can configure conditional forwarding on the internal Certkiller .org server so
that requests for Certkiller .com resources get forwarded straight to the perimeter network DNS server.
Incorrect Answers:
B: A stub zone is no good to us here. The perimeter DNS server must be authoritative for the Certkiller .com domain. Therefore, we need a primary zone on the perimeter DNS server.
D: As long as the internal DNS servers are working, the external DNS server will never be used. Internal clients will not be able to resolve www. Certkiller .com.
E: There is no need to configure a root zone on the perimeter network DNS server.

QUESTION 29
You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All domain controllers and member servers run Windows Server 2003, Enterprise Edition. All client computers run Windows XP Professional.
Certkiller has one main office and one branch office. The two offices are connected to a T1 WAN connection. There is a hardware router at each end of the connection. The main office contains 10,000 client computers, and the branch office contains 5,000 client computers.
You need to use DHCP to provide IP addresses to the Windows XP Professional computers in both offices. You need to minimize network configuration traffic on the WAN connection. Your solution needs to prevent any component involved in the DHCP architecture from becoming a single point of failure.
What should you do?

A. At the main office, configure two Windows Server 2003 computers as a DHCP server cluster.
Configure the branch office router as a DHCP relay agent.
B. At the main office, configure two Windows Server 2003 computers as a DHCP server cluster.
At the branch office, configure a Windows Server 2003 computer as a DHCP relay agent.
C. At the main office, configure two Windows Server 2003 computers as a DHCP server cluster.
At the branch office, configure two Windows Server 2003 computers as a DHCP server cluster.
D. At the main office, configure two Windows Server 2003 computers as DHCP servers.
Configure one DHCP server to handle 80 percent of the IP address scope and the other DHCP server to handle 20 percent.
Configure the branch office router as a DHCP relay agent.

Answer: C

Explanation: The best fault tolerant solution here would be to implement a DHCP server cluster in each office.
Cluster support for DHCP servers
The Windows Server 2003 DHCP Server service is a cluster-aware application
cluster-aware application
An application that can run on a cluster node and that can be managed as a cluster resource. Cluster-aware

applications use the Cluster API to receive status and notification information from the server cluster.
You can implement additional DHCP (or MADCAP) server reliability by deploying a DHCP server cluster using the Cluster service
Cluster service
The essential software component that controls all aspects of server cluster operation and manages the cluster database. Each node in a server cluster runs one instance of the Cluster service provided with Windows Server 2003, Enterprise Edition.
By using clustering support for DHCP, you can implement a local method of DHCP server failover, achieving greater fault tolerance. You can also enhance fault tolerance by combining DHCP server clustering with a remote failover configuration, such as by using a split scope configuration.
Other options for DHCP failover
Another way to implement DHCP remote failover is to deploy two DHCP servers in the same network that share a split scope configuration based on the 80/20 rule
Incorrect Answers:
A: The branch office router would be a single point of failure in this solution.
B: The server hosting the DHCP relay agent would be a single point of failure in this solution.
D: The branch office router would be a single point of failure in this solution.

QUESTION 30
You are the systems engineer for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. A Windows Server 2003 computer named Certkiller DNS1 functions as the internal DNS server and has zone configured as shown in the exhibit.

The network is not currently connected to the Internet. Certkiller maintains a separate network that contains publicly accessible Web and mail servers. These Web and mail servers are members of a DNS domain named Certkiller .com. The Certkiller .com zone is hosted by a UNIX-based DNS server named UNIX DNS, which is running the latest version of BIND.
The company plans to allow users of the internal network to access Internet-based resources. The company's written security policy states that resources located on the internal network must never be exposed to the Internet. The written security policy states that the internal network's DNS namespace must never be exposed to the Internet. To meet these requirements, the design specifies that all name resolution requests for Internet-based resources from computers on the internal network must be sent

from Certkiller DNS1. The current design also specifies that UNIX DNS must attempt to resolve any name resolution requests before sending them to name servers on the Internet.
You need to plan a name resolution strategy for Internet access. You need to configure Certkiller DNS1 so that it complies with company requirements and restrictions.
What should you do?

A. Delete the root zone from Certkiller DNS1.
Configure Certkiller DNS1 to forward requests to UNIX DNS.
B. Copy the Cache.dns file from the Windows Server 2003 installation CD-ROM to the C:\Windows\System32\Dns folder on Certkiller DNS1.
C. Add a name server (NS) resource record for UNIX DNS to your zone.
Configure UNIX DNS with current root hints.
D. On Certkiller DNS1, configure a secondary zone named Certkiller .com that uses UNIX DNS as the master server.
Configure UNIX DNS to forward requests to your ISP's DNS servers.

Answer: A

Explanation: We need to delete the root zone from the internal DNS server. This will enable us to configure the server to forward internet name resolution requests to the external DNS server (UNIX DNS).
A DNS server configured to use a forwarder will behave differently than a DNS server that is not configured to use a forwarder. A DNS server configured to use a forwarder behaves as follows:
1. When the DNS server receives a query, it attempts to resolve this query using the primary and secondary zones that it hosts and its cache.
2. If the query cannot be resolved using this local data, then it will forward the query to the DNS server designated as a forwarder.
3. The DNS server will wait briefly for an answer from the forwarder before attempting to contact the DNS servers specified in its root hints.
Incorrect Answers:
B: The Cache.dns file contains the IP addresses of the internet root DNS servers. We don't want the internal DNS server to query the root DNS servers, so we don't need the cache.dns file.
C: Unix dns already has root hints. An NS record on the internal DNS server won't fulfil the requirements of the question.
D: We don't need a secondary zone on the internal DNS server. All external resolution requests must be forwarded to the external DNS server.