070-293

Planning and Maintaining
a Microsoft Windows Server 2003 Network Infrastructure

Version 10.0

..

Leading The Way
in IT Testing And Certification Tools

www.testking.com

Important Note, Please Read Carefully

Study Tips
This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Further Material
For this exam TestKing also provides:
* Online Testing. Practice the questions in an exam environment.
Try a demo: http://www.testking.com/index.cfm?pageid=724
* Study Guide. Concepts and labs. Provides a foundation of knowledge.

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestKing an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Member zone/Log in**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Copyright
Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular pdf file is being distributed by you, TestKing reserves the right to take legal action against you according to the International Copyright Laws.

QUESTION NO: 1
You are a network administrator for TestKing. 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 TestKing1.**
- **One Windows Server 2003, Standard Edition computer named TestKing2.**
- **One Windows Server 2003, Enterprise Edition computer named TestKing3.**
- **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: TestKing2, TestKing3
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 (testking2 and testking3).

Reference: MS training kit 70-290 chapter one lesson 1;"the server belongs to a domain but cannot be a domain controller"

QUESTION NO: 2
You are a network administrator for TestKing. The network consists of a single Active Directory domain and contains Windows Server 2003 computers.

You install a new service on a server named TestKing3. The new service requires that you restart TestKing3. When you attempt to restart TestKing3, the logon screen does not appear. You turn off and then turn on the power for TestKing3. 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 TestKing3 by using the Safe Mode Startup options. All Safe Mode options are unsuccessful.

You restore TestKing3. TestKing3 restarts successfully. You discover that TestKing3 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 NO: 3
You are a network administrator for TestKing. The network contains a Windows Server 2003 application server named TestKingSrv. TestKingSrv has one processor. TestKingSrv has been running for several weeks.

You add a new application to TestKingSrv. Users now report intermittent poor performance on TestKingSrv. You configure System Monitor and track the performance of TestKingSrv for two hours. You obtain the performance metrics that are summarized in the exhibit.

\\TESTKINGSRV		
Memory		
% Committed Bytes In Use	99.503	
Pages/sec	1014.316	
Network Interface	AMD PCNET Family PCI Ethernet Adapter	
Bytes Total/sec		21230.359
Paging File	\??\C:\pagefile.sys	
% Usage	86.670	
PhysicalDisk	_Total	
% Disk Time	93.610	
Processor	_Total	
% Processor Time	69.444	

The values of the performance metrics are consistent over time.

You need to identify the bottleneck on TestKingSrv and upgrade the necessary component. You need to minimize hardware upgrades.

What should you do?

A. Install a faster CPU in TestKingSrv.
B. Add more RAM to TestKingSrv.
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.

For tuning and upgrade suggestions, see Solving performance problems.

Resource	Object\Counter	Suggested threshold	Comments
Disk	Physical Disk\% Free Space Logical Disk\%	15%	

	Free Space		
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; 1000 interrupts per second is a good starting point	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 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.

QUESTION NO: 4
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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 adapater. 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 NO: 5
You are the network administrator for TestKing. 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 and-line tool: "Non-existent domain".**

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:
- Their direction, either outbound or inbound
- The transport protocol, either TCP or UDP
- Their contents: queries/transfers, updates, or notifications
- Their type, either requests or responses
- Their 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 NO: 6
You are a network administrator for TestKing. 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.

Possible first actions
Stop the Cluster service on all nodes
Pause the Cluster service on all nodes
TestKing.com
Place first action here
Possible second actions
Start the Cluster service on all nodes by using the /resetquorum switch.
Start the Cluster service on all nodes by using the /fixquorum switch.
Place second action here
Possible third actions
Configure a different disk as the quorum location.
Run the chkdsk.exe /f /r command on drive Q.
Place third action here
Possible fourth actions
Restart the cluster service on each node norm...
Resume the cluster service on each node.
Place fourth action here

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 NO: 7

You are a network administrator for TestKing. TestKing 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 NO: 8
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All computers on the network are members of the domain. The domain contains a Windows Server 2003 computer named TestKingA.

You are planning a public key infrastructure (PKI) for the company. You want to deploy an enterprise certification authority (CA) on TestKingA.

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 enrol 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 NO: 9
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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

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 autoenrollment

You can use autoenrollment 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 autoenrollment, 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 autoenrollment and manual requests, can be renewed automatically. These types of renewals do not require Autoenroll permission, even if they are renewed automatically.

Planning for autoenrollment deployment

Autoenrollment is a useful feature of certification services in Windows XP and Windows Server 2003, Standard Edition. Autoenrollment 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 autoenrollment, the administrator must plan the appropriate certificate template or templates to use. Several settings in the certificate template directly affect the behavior of subject autoenrollment.

- On the **Request Handling** tab of the selected certificate template, the selection of an autoenrollment user interaction setting will affect autoenrollment:
-

Setting	Affect on autoenrollment behavior
Enroll subject without requiring any user input	This setting will allow "silent" autoenrollment 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 enrollment and require user input when the private key is used	This setting prompts the user both during enrollment and whenever the private key is used. This is the most interactive autoenrollment 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 NO: 10

You are a network administrator for TestKing. 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 e-mail 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 CA. You open Certificate Templates on the enterprise subordinate CA, but you are unable to configure certificates templates for autoenrollment. The Certificate Templates administration tool is shown in the exhibit.

You need to configure Active Directory to support autoenrollment 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 autoenrollment 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 NO: 11
You are a network administrator for TestKing. 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 NO: 12
You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.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.

TestKing 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 NO: 13
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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 testking.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 testking.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 NO: 14
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The network contains a Windows Server 2003 member server named TestKingSrvA. 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 TestKingSrvA. However, the recent application of a custom security template disabled several services on TestKingSrvA.

You need to ensure that you can use MBSA to analyze TestKingSrvA.

Which two services should you enable?

To answer, select the appropriate services to enable in the dialog box.

Answer: The Remote Registry and Server services should be enabled.
Explanation: From the readmefile for MBSA
<u>The following are the requirements for a computer running the tool that is scanning remote machine(s):</u>

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.

<u>The following are the requirements for a computer to be scanned remotely by the tool:</u>

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 NO: 15
You are the network administrator for TestKing. 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 testking.com and two child domains named asia.testking.com and europe.testking.com. The asia.testking.com domain contains a member server named TestKing2. You configure TestKing2 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.testking.com and the europe.testking.com domains to enroll for user certificates.

You discover that the certificates for user accounts in the asia.testking.com domain are being published to Active Directory, but the certificates for user accounts in the europe.testking.com domain are not.

You want certificates issued by TestKing2 to europe.testking.com domain user accounts to be published in Active Directory.

What should you do?

A. Configure user certificate autoenrollment for all domain user accounts in the testking.com domain.
B. Configure user certificate autoenrollment for all domain user accounts in the europe.testking.com domain.
C. Add TestKing2 to the Cert Publishers group in the testking.com domain.
D. Add TestKing2 to the Cert Publishers group in the europe.testking.com domain.

Answer: D
Explanation: The problem here is that TestKingSrvC doesn't have the necessary permission to publish certificates for users in child2.testking.com. We can solve this problem by adding TestKingSrvC to the Cert Publisher group in the child2.testking.com domain.

Reference: http://support.microsoft.com/default.aspx?scid=kb;en-us;219059

QUESTION NO: 16
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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.

TestKing is deploying a Windows Server 2003 computer named TestKingA that has Routing and Remote Access installed. TestKingA 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 TestKingA 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: E
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® Windows® 98, Windows® Millennium Edition (Windows Me), or Windows NT® 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.
C: We need to do this, but we need to do this on the VPN server. We can do this by creating a Routing and Remote Access custom IPSec policy on the VPN server.
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.

Reference:

MS Windows Server 2003 Deployment Kit Deploying Network Services
Planning Security for a VPN
Selecting a VPN Protocol

QUESTION NO: 17
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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 autoenrollment 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 autoenrollment 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 autoenrollment 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 snap-in.
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:
   - **Data encryption (WEP enabled).** Select this option to require that a network key be used for encryption.
   - **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.
   - **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:
    - **Smart card.** Permits clients to use the certificate that resides on their smart card for authentication.
    - **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:
    - **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.
    - **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,	**Designing a Managed Environment**
Overview of Deploying a Wireless LAN	Creating Wireless Network Policies
WLAN Technology Background	Defining Wireless Configuration Options for Preferred Networks

QUESTION NO: 18
You are the senior systems engineer for TestKing. The network consists of a single Active Directory domain named testking.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 TestKing 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 NO: 19
You are the systems engineer for TestKing. 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 testking.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 adapater 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 NO: 20
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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.

TestKing.com

Answer:

TestKing.com

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 NO: 21
You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. Client computers run Windows 2000 Professional, Windows XP Professional, or Windows NT Workstation 4.0.

TestKing 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 Request Security Default Picture

Server Require 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 NO: 22
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All domain controllers run Windows Server 2003. All application servers run Windows Server 2003.

Client computers in the accounting department runs 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® 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 NO: 23
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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 analyse 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 NO: 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.

```
C:\WINDOWS\system32\cmd.exe
C:\>ping server5

Pinging server5.woodgrovebank.com [192.168.202.8] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.202.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.202.8

Pinging 192.168.202.8 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.202.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>nbtstat -c

Local Area Connection:
Node IpAddress: [192.168.202.6] Scope Id: []

                    NetBIOS Remote Cache Name Table

        Name               Type       Host Address    Life [sec]
    ---------------------------------------------------------------
    SERVER5         <20>  UNIQUE          192.168.202.8       512
```

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 NO: 25
You are a network administrator for TestKing. The network consists of multiple physical segments. The network contains two Windows Server 2003 computers named TestKingSrvA and TestKingSrvB, and several Windows 2000 Server computers. TestKingSrvA 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	TestKingSrvB
DNS Servers	(blank)
Primary WINS Server	(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 TestKingSrvB.
B. Increase the IP address range for the 10.250.100.0/24 scope on TestKingSrvA.
C. Add global DHCP scope options to TestKingSrvA for default gateway, DNS servers, and WINS servers.
D. Delete all IP address reservation in the scope on TestKingSrvA.
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 TestKingSrvB. We can also see that the IP configuration has no default gateway, WINS or DNS addresses. Obviously, TestKingSrvB is misconfigured. Other client computers have no problems; it is likely that they get their IP configuration from TestKingSrvA. We can either correctly configure the DHCP service on TestKingSrvB or we can disable it and just use TestKingSrvA as the DHCP server. The only option given is to disable the DHCP service on TestKingSrvB, 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 TestKingSrvA as their DHCP server.

Incorrect Answers:

B: The client computer received its IP configuration from TestKingSrvB. Therefore, the problem is likely to be with TestKingSrvB, not TestKingSrvA.
C: Some client computers have no problems; it is likely that they get their IP configuration from TestKingSrvA. Therefore, TestKingSrvA is correctly configured.
D: The client computer received its IP configuration from TestKingSrvB. Therefore, the problem is likely to be with TestKingSrvB, not TestKingSrvA.
F: The affected client computers have no DNS configuration; therefore this command will have no affect.

QUESTION NO: 26
You are the network administrator for TestKing. 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.

TestKing 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 TestKing 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
    - Need 220 IP, 20 for servers and 200 for clients

- Branch Offices
    - Need 220 IP, 20 for servers and 200 for clients
    - We will have 12 branch offices
    - 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 NO: 27
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.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
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 NO: 28

You are a network administrator for TestKing. The internal network has an Active Directory-integrated zone for the testking.com domain. Computers on the internal network use the Active Directory-integrated DNS service for all host name resolution.

The TestKing Web site and DNS server are hosted at a local ISP. The public Web site for TestKing is accessed at www.testking.com. The DNS server at the ISP hosts the testking.com domain.

To improve support for the Web site, TestKing 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 testking.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 testking.com.
B. On the DNS server that is on the perimeter network, install a stub zone for testking.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, E
Explanation:

By configuring a primary zone for testking.com on a DNS server in the perimeter network, we have a DNS server that can resolve requests for the www.testking.com website.

Incorrect Answers:
B: A stub zone is no good to us here. The perimeter DNS server must be authoritative for the testking.com domain. Therefore, we need a primary zone on the perimeter DNS server.
C: The internal DNS servers host a testking.com zone. You cannot configure conditional forwarding for a zone that the DNS server hosts.
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.testking.com.

QUESTION NO: 29
You are a network administrator for Test King. The network consists of a single Active Directory domain named testking.com. All domain controllers and member servers run Windows Server 2003, Enterprise Edition. All client computers run Windows XP Professional.

Test King 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 NO: 30
You are the systems engineer for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. A Windows Server 2003 computer named TESTKINGDNS1 functions as the internal DNS server and has zone configured as shown in the exhibit.

The network is not currently connected to the Internet. TestKing maintains a separate network that contains publicly accessible Web and mail servers. These Web and mail servers are members of a DNS domain named testking.com. The testking.com zone is hosted by a UNIX-based DNS server named UNIXDNS, 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 TESTKINGDNS1. The current design also specifies that UNIXDNS 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 TESTKINGDNS1 so that it complies with company requirements and restrictions.

What should you do?

A. Delete the root zone from TESTKINGDNS1.
   Configure TESTKINGDNS1 to forward requests to UNIXDNS.
B. Copy the Cache.dns file from the Windows Server 2003 installation CD-ROM to the C:\Windows\System32\Dns folder on TESTKINGDNS1.
C. Add a name server (NS) resource record for UNIXDNS to your zone.
   Configure UNIXDNS with current root hints.
D. On TESTKINGDNS1, configure a secondary zone named testking.com that uses UNIXDNS as the master server.
   Configure UNIXDNS 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 (UNIXDNS).
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: Unixdns 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.

QUESTION NO: 31
You are a network administrator for TestKing. The network consists of two Active Directory forests. No trust relationships exist between the two forests. All computers in both forests are configured to use a common root certification authority (CA).

Each forest contains a single domain. The domain named hr.testking.com contains five Windows Server 2003 computers that are used exclusively to host confidential human resources applications and data. The

domain named testking.com contains all other servers and client computers. A firewall separates the human resources servers from the other computers on the network. Only VPN traffic from testking.com to a remote access server in hr.testking.com is allowed through the firewall.

Managers need to access data on the servers in hr.testking.com from their Windows XP Professional computers. The company's written security policy requires that all communication containing human resources data must be secured by using the strongest IPSec encryption available.

You need to configure an IPSec policy for the servers that host the human resources data that complies with the written security policy and gives the managers in testking.com access to the data they need.

What should you do?

To answer, drag the appropriate configuration settings to the IPSec Policy Configuration.

Answer:

TestKing.com

Explanation:

We can not use Kerberos because there is no trust between the forests; we must use certificates, we must affect all traffic, and the server must require security.

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.

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 NO: 32
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The functional level of the domain is Windows Server 2003. The domain contains a Windows Server 2003 computer named TestKing26 that is running Routing and Remote Access.

The domain contains a universal group named Managers and a global group named Operations. User accounts in the Managers group require remote access between the hours of 8:00 A.M. and 8:00 P.M. User accounts in the Operations group require remote access 24 hours per day.

You configure a remote access policy on TestKing26 named RA_Managers with the appropriate settings for the Managers group, and you configure a second remote access policy named RA_Operations on TestKing26 with the appropriate settings for the Operations group. The default remote access polices on TestKing26 remain unmodified.

Members of the Managers group report that they can establish a remote access connection to TestKing26, but members of the Operations group report that they cannot establish a remote access connection to TestKing26.

You open the Routing and Remote Access administrative tool and note that the remote access polices are in the order presented in the following table.

Remote access policy name	Order
RA_Managers	1
Connections to Microsoft Routing and remote Access server	2
RA_Operations	3
Connections to other access servers	4

You need to enable the appropriate remote access for the members of the Managers and Operations groups while restricting remote access to all other users.

What should you do?

A. Delete the **Connections to other access servers** policy.
B. Re-create the Operations global group as a universal group.
C. Move the **Connections to Microsoft Routing and Remote Access server** policy up so that it is the first policy in the order.
D. Move the **RA_Operations** policy up so that it is the second policy in the order.

Answer: D
Explanation: The remote access policies are processed in order. If a user meets a condition in a policy, the user is allowed or denied access according to that policy. No other policies are checked. The Connections to Microsoft Routing and Remote Access server policy is being processed before the RA-Operations policy. The users meet the condition in the Connections to Microsoft Routing and Remote Access server policy and are being denied access. The RA-Operations policy isn't being checked. Therefore, we need to move the RA-Operations policy above the Connections to Microsoft Routing and Remote Access server policy.

Incorrect Answers:
A: This policy isn't preventing the remote access. The Connections to Microsoft Routing and Remote Access server policy is preventing the access.
B: The global group is fine. Changing it won't help.
C: The Connections to Microsoft Routing and Remote Access server policy is preventing the access. The RA-Operations policy isn't being checked. Therefore, we need to move the RA-Operations policy above the Connections to Microsoft Routing and Remote Access server policy.

QUESTION NO: 33

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The network contains two IP subnets connected by a Windows Server 2003 computer running Routing and Remote Access. All servers run Windows Server 2003. All client computers run Windows XP Professional.

Each subnet contains a domain controller. Each subnet contains a DHCP server, which provides TCP/IP configuration information to the computers on only its subnet. The relevant portion of the network is shown in the exhibit.

You recently implemented a Microsoft Internet Security and Acceleration (ISA) Server 2000 array on the network to provide Internet connectivity. The ISA Server array uses Network Load Balancing on the internal adapters. The array's Network Load Balancing cluster address is 172.30.32.1. You configure the DHCP server on Subnet1 to provide the array's Network Load Balancing cluster address as the default gateway. You configure the DHCP server on Subnet2 to provide the IP address 172.30.64.1 as the default gateway for Subnet2.

Users on Subnet2 report that they cannot connect to Internet-based resources. They can successfully connect to resources located on Subnet1. Users on Subnet1 can successfully connect to Internet-based resources. You investigate and discover that no Internet requests from computers on Subnet2 are being received by the ISA Server array.

You need to provide Internet connectivity to users on Subnet2.

What should you do?

A. Configure the DHCP server on Subnet2 to provide the address 172.30.32.1 as the default gateway.
B. Configure the DHCP server on Subnet2 to provide the address 172.30.32.2 as the default gateway.
C. On the Routing and Remote Access server, add a default route to 172.30.32.1.
D. On the Routing and Remote Access server, add a default route to 131.107.72.17.

Answer: C
Explanation: The routing and remote access server knows how to route traffic between subnet 1 and subnet 2. However, it doesn't know how to route traffic to the internet. We can fix this by adding a default route on the routing and remote access server. The default route will tell the routing and remote access server that any traffic that isn't destined for subnet1 or subnet2 (i.e. any external destination) should be forwarded to the internal interface of the ISA server (172.30.32.1).

Incorrect Answers:
A: 172.30.32.1 isn't on the same subnet as subnet2. Therefore, the clients on subnet2 cannot use this address as their default gateway.
B: 172.30.32.2 isn't on the same subnet as subnet2. Therefore, the clients on subnet2 cannot use this address as their default gateway. Furthermore, this address isn't the internal address of the ISA server.
D: The default route needs to forward traffic to the internal interface of the ISA server.

QUESTION NO: 34
You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

The Active Directory domain contains three organizational units (OUs): Payroll Users, Payroll Servers, and Finance Servers. The Windows XP Professional computers used by the users in the payroll department are in the Payroll Users OU. The Windows Server 2003 computers used by the payroll department are in the Payroll Servers OU. The Windows Server 2003 computers used by the finance department are in the Finance Servers OU.

You are planning the baseline security configuration for the payroll department. The company's written security policy requires that all network communications with servers in the Payroll Servers OU must be secured by using IPSec. The written security states that IPSec must not be used on any other servers in the company.

You need to ensure that the baseline security configuration for the payroll department complies with the written security policy. You also need to ensure that members of the Payroll Users OU can access resources in the Payroll Servers OU and in the Finance Servers OU.

What should you do?

A. Create a Group Policy object (GPO) and assign the Secure Server (Require Security) IPSec policy setting.
Link the GPO to only the Payroll Servers OU.
Create a second GPO and assign the Client (Respond Only) IPSec policy setting.
Link the second GPO to the Payroll Users OU.
B. Create a Group Policy object (GPO) and assign the Secure Servers (Require Security) IPSec policy setting.
Link the GPO to the Payroll Servers OU and to the Finance Servers OU.
Create a second GPO and assign the Client (Respond Only) IPSec policy setting.
Link the second GPO to the Payroll Users OU.
C. Create a Group Policy object (GPO) and assign the Server (Request Security) IPSec policy setting.
Link the GPO to only the Payroll Servers OU.
Create a second GPO and assign the Client (Respond Only) IPSec policy setting.
Link the second GPO to the Payroll Users OU.
D. Create a Group Policy object (GPO) and assign the Server (Request Security) IPSec policy setting.
Link the GPO to the Payroll Serves OU and to the Finance Servers OU.
Create a second GPO and assign the Client (Respond Only) IPSec policy setting.
Link the second GPO to the Payroll Users OU.

Answer: A
Explanation: Assigning the Secure Server (Require Security) IPSec policy to the payroll servers will ensure that they will only communicate using IPSec. Assigning the Client (Respond Only) IPSec policy to the payroll clients will ensure that they are able to use IPSec when asked to do so by the payroll servers. All other network communications will not use IPSec.

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 NO: 35
You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. TestKing's main office is in Boston, and it has branch offices in Washington and Los Alamos. The company has no immediate plans to expand or relocate the offices.

The company wants to connect the office networks by using a frame relay WAN connection and Routing and Remote Access servers that are configured with frame relay WAN adapters. Computers in each office will be configured to use their local Routing and Remote Access server as a default gateway.

You are planning the routing configuration for the Routing and Remote Access servers.

You need to allow computers in Boston, Washington, and Los Alamos to connect to computers in any office. You want to minimize routing traffic on the WAN connection.

What should you do?

A. At each office, add the OSPF routing protocol to Routing and Remote Access, add the WAN adapater to the OSPF routing protocol, and deploy OSPF as a single-area internetwork.
B. At each office, add the RIP version 2 routing protocol to Routing and Remote Access, and configure the WAN adapter to use RIP version 2.
Configure the outgoing packet protocol as **RIP version 2 broadcast** and the incoming packet protocol as **RIP version 1 and 2**.
C. At each office, add the RIP version 2 routing protocol to Routing and Remote Access, and configure the WAN adapter to use RIP version 2.
Configure the outgoing packet protocol as **RIP version 2 multicast** and the incoming packet protocol as **RIP version 2 only**.

D. At each office, configure the Routing and Remote Access server with static routes to the local networks at the other two offices.

Answer: D
Explanation: We need to configure the routers to route traffic between the offices. As we only have three offices, we can use simple static routes. Once we have configured the routing tables with static routes, the offices will be able to communicate with each other. This solution is preferable to using a routing protocol such as RIP because there will be no routing information going over the WAN links.

Incorrect Answers:
A: We have a simple network configuration with just three offices. Using a routing protocol is unnecessary. Static routes will suffice.
B: We have a simple network configuration with just three offices. Using a routing protocol is unnecessary. Static routes will suffice.
C: We have a simple network configuration with just three offices. Using a routing protocol is unnecessary. Static routes will suffice.

QUESTION NO: 36
You are a network administrator for TestKing. The network consists of a single Active Directory forest. All domain controllers run Windows Server 2003.

The bank decides to provide access to its mortgage application services from a real estate agency that has offices throughout the country. You install a TestKing domain controller in each real estate agency office.

You need to further protect the domain controllers' user account databases from unauthorized access. You want to achieve this goal by using the minimum amount of administrative effort.

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

A. Use the system key utility (syskey) with the most secure security level on the domain controllers.
B. Create a Group Policy object (GPO), import the Securedc.inf security template, and apply the GPO to the domain controllers.
C. Create a Group Policy object (GPO), configure the **Network security: LAN Manager authentication level** security option to the **Send NTLMv2 response only\refuse LM** setting, and apply the GPO to the domain controllers.
D. Create a Group Policy object (GPO), import the DC security.inf security template, and apply the GPO to the domain controllers.

Answer: A, B

Using Syskey
On domain controllers, password information is stored in directory services. It is not unusual for password – cracking software to target the Security Accounts Manager (SAM) database or directory services to access passwords for user accounts.
The System Key utility (Syskey) provides an extra line of defense against offline password – cracking software. Syskey uses strong encryption techniques to secure account password information that is stored in directory services.

Table 4.19 Syskey Modes

System Key Option	Security Level	Description
Mode 1: System Generated Password, Store Startup Key Locally	Secure	Uses a computer – generated random key as the system key and stores an encrypted version of the key on the local computer. This option provides strong encryption of password information in the registry, and enables the user to restart the computer without the need for an administrator to enter a password or insert a disk.
Mode 2: Administrator generated password, Password Startup	More secure	Uses a computer – generated random key as the system key and stores an encrypted version of the key on the local computer. The key is also protected by an administrator – chosen password. Users are prompted for the system key password when the computer is in the initial startup sequence. The system key password is not stored anywhere on the computer.
Mode 3: System Generated Password, Store Startup Key on Floppy Disk	Most secure	Uses a computer-generated random key and stores the key on a floppy disk. The floppy disk that contains the system key is required for the system to start, and it must be inserted at a prompt during the startup sequence. The system key is not stored anywhere on the computer.

Syskey is enabled on all Windows Server 2003 servers in Mode 1 (obfuscated key). There are many reasons to recommend using Syskey in Mode 2 (console password) or Mode 3 (floppy storage of Syskey password) for any domain controller that is exposed to physical security threats.
From a security standpoint, this appears sensible at first, as the domain controller would be vulnerable to being restarted by an attacker with physical access to it. Syskey in Mode 1 allows an attacker to read and alter the contents of the directory.
However, the operational requirements for ensuring that domain controllers can be made available through restarts tend to make Syskey Mode 2 or Mode 3 difficult to support. To take advantage of the added protection provided by these Syskey modes, the proper operational processes must be implemented in your environment to meet specific availability requirements for the domain controllers.
The logistics of Syskey password or floppy disk management can be quite complex, especially in branch offices. For example, requiring one of your branch managers or local administrative staff to come to the office at 3 A.M. to enter the passwords, or insert a floppy to enable other users to access the system is expensive and makes it very challenging to achieve high availability service level agreements (SLAs).

Alternatively, allowing your centralized IT operations personnel to provide the Syskey password remotely requires additional hardware — some hardware vendors have add – on solutions available to remotely access server consoles.
Finally, the loss of the Syskey password or floppy disk leaves your domain controller in a state where it cannot be restarted. There is no method for you to recover a domain controller if the Syskey password or floppy disk is lost. If this happens, the domain controller must be rebuilt.
Nevertheless, with the proper operational procedures in place, Syskey can provide an increased level of security that can greatly protect the sensitive directory information found on domain controllers.
For these reasons, Syskey Mode 2 or Mode 3 is recommended for domain controllers in locations without strong physical storage security. This recommendation also applies to domain controllers in any of the three environments described in this guide.
To create or update a system key:
Click **Start**, click **Run**, type **syskey**, and then click **OK**.
Click **Encryption Enabled**, and then click **Update**.
Click the desired option, and then click **OK**.

Secure (Secure*.inf) Template
The Secure templates define enhanced security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings.
Additionally, the Secure templates limit the use of LAN Manager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LAN Manager responses.

QUESTION NO: 37
You are a network administrator for TestKing. All domain controllers run Windows Server 2003. The network contains 50 Windows 98 client computers, 300 Windows 2000 Professional computers, and 150 Windows XP Professional computers.

According to the network design specification, the Kerberos version 5 authentication protocol must be used for all client computers on the internal network.

You need to ensure that Kerberos version 5 authentication is used for all client computers on the internal network.

What should you do?

A. On each domain controller, disable Server Message Block (SMB) signing and encryption of the secure channel traffic.
B. Replace all Windows 98 computers with new Windows XP Professional computers.
C. Install the Active Directory Client Extension software on the Windows 98 computers.
D. Upgrade all Windows 98 computers to Windows NT workstation 4.0.

Answer: B
Explanation:

By default, in a Windows 2003 domain, Windows 2000 and Windows XP clients use Kerberos as their authentication protocol. Windows 98 doesn't support Kerberos authentication; therefore, we need upgrade the Windows 98 computers.

Incorrect Answers:
A: This won't enable the Windows 98 clients to use Kerberos authentication.
C: The Active Directory Client Extension software doesn't enable Windows 98 clients to use Kerberos authentication.
D: Windows NT 4.0 doesn't support Kerberos authentication.

QUESTION NO: 38
You are the network administrator for TestKing. The company has a main office and 20 branch offices. You recently completed the design of the company network. The network design consists of a single Active Directory domain named testking.com. All domain controllers will run Windows Server 2003. The main office will contain four domain controllers, and each branch office will contain one domain controller. The branch office domain controllers will be administered from the main office.

You need to ensure that the domain controllers are kept up-to-date with software updates for Windows Server 2003 after their initial deployment. You want to ensure that the domain controllers automatically install the updates by using the minimum amount of administrative intervention. You also want to configure the settings by using the minimum amount of administrative effort.

What should you do?

A. In System Properties, on the **Automatic Update** tab, enable **Keep my computer up to date**, and then select **Download the updates automatically and notify me when they are ready to be installed**.
B. In the Default Domain Controllers Policy Group Policy object (GPO), enable **Configure Automatic Updates** with option 3 **– Auto download and notify for install**.
C. In the Default Domain Controllers Policy Group Policy object (GPO), enable **Configure Automatic Updates** with option 4 **– Auto download and schedule the install**.
D. In System Properties, on the **Automatic Updates** tab, enable **Keep my computer up to date**, and then select **Automatically download the updates, and install them on the schedule that I specify**.

Answer: C

Explanation: The question states that **You want to ensure that the domain controllers automatically install the updates by using the minimum amount of administrative intervention.** The way to do this is to configure the automatic updates with the option to **Auto download and schedule the install.** The easiest way to configure the domain controllers with this setting is to configure a group policy object for the domain controllers.

The problem with this solution is that the domain controllers may automatically restart after the updates are installed. Scheduling the updates to install out of business hours will minimize any disruption.

Incorrect Answers:
A: It is easier to configure the domain controllers using group policy.
B: This solution will download the updates, but it won't install them until an administrator manually clicks the install button in the notification dialog box. Answer C automates the procedure more by scheduling the installation to occur at a set time without any further administrative intervention.
D: It is easier to configure the domain controllers using group policy.

QUESTION NO: 39
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com.

The company plans to deploy 120 Windows Server 2003 member servers as file servers in the domain. The new file servers will be located in a single organizational unit (OU) named File Servers.

The security department provides you with a security template that must be applied to the new file servers.

You need to apply and maintain the security settings contained in the security template to the new file servers. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do?

A. On a reference computer, use the Local Security Settings console to import the security template.
   Use imaging technology to install and configure the new file servers based on the configuration of the reference computer.
B. On a reference computer, run the **secedit** command to apply the security template.
   Use imaging technology to install and configure the new file serves based on the configuration of the reference computer.
C. Create a new Group Policy object (GPO).
   Import the security template into the Security Settings of the Computer Configuration section of the GPO.

Link the GPO to the File Servers OU.

D. On the PDC emulator master in the domain, run the **secedit** command to apply the security template.

Answer: C
Explanation: We have a security template with the required security settings. We can simply import the template into a Group Policy Object and apply the settings to the File Servers OU.

Incorrect Answers:
A: This would work, but there is a catch in the question. The question states that you need to apply **and maintain** the security settings contained in the security template to the new file servers. Using a GPO, the settings will be periodically refreshed, ensuring that the security settings 'maintained'.
B: This would work, but there is a catch in the question. The question states that you need to apply **and maintain** the security settings contained in the security template to the new file servers. Using a GPO, the settings will be periodically refreshed, ensuring that the security settings 'maintained'.
D: This would have no effect on the file servers.

QUESTION NO: 40
You are a network administrator for TestKing. You install Windows Server 2003 on two servers named TestKing1 and TestKing2. You configure TestKing1 and TestKing2 as a two-node cluster.

You configure a custom application on the cluster by using the Generic Application resource, and you put all resources in the Application group. You test the cluster and verify that it fails over properly and that you can move the Application group from one node to the other and back again.

The application and the cluster run successfully for several weeks. Users then report that they cannot access the application. You investigate and discover that TestKing1 and TestKing2 are running but the Application group is in a failed state.

You restart the Cluster service and attempt to bring the Application group online on TestKing1. The Application group fails. You discover that TestKing1 fails, restarts automatically, and fails again soon after restarting. TestKing1 continues to fail and restart until the Application group reports that it is in a failed state and stops attempting to bring itself back online.

You need to configure the Application group to remain on TestKing2 while you research the problem on TestKing1.

What should you do?

A. On TestKing2, configure the failover threshold to **0**.

B. On TestKing2, configure the failover period to **0**.
C. Remove TestKing1 from the Possible owners list.
D. Remove TestKing1 from the Preferred owners list.

Answer: C
Explanation: We don't want the application group to move to TestKing1 – we want the application group to remain on TestKing2. We can do this by removing TestKing1 from the possible owners list.

QUESTION NO: 41
You are a network administrator for TestKing. The network contains two Windows Server 2003 computers named TestKingA and TestKingB. These servers host an intranet application. Currently, 40 users connect to TestKingA and 44 users connect to TestKingB.

The company is adding 35 employees who will need access to the intranet application. Testing shows that each server is capable of supporting approximately 50 users without adversely affecting the performance of the application.

You need to provide a solution for supporting the additional 35 employees. The solution must include providing server fault tolerance. You need to minimize the costs and administrative effort required by your solution.

You add a new server named TestKingC to the network and install the intranet application on TestKingC.

What else should you do?

A. Use Network Load Balancing Manager to configure TestKingA, TestKingB, and TestKingC as a Network Load Balancing cluster.
B. Use Cluster Administrator to configure TestKingA, TestKingB, and TestKingC as a three-node server cluster.
Use the Majority Node Set option.
Configure the cluster so that all three nodes are active.
C. Use Cluster Administrator to configure TestKingA, TestKingB, and TestKingC as a three-node server cluster.
Configure the cluster so that two nodes are active and one node is a hot standby node.
D. Use DNS load balancing to utilize all three servers by using the same virtual server name.

Answer: A
Explanation: We can use Network Load Balancing to balance the load on the three web servers.

Reference: Deploying Network Load Balancing

Overview of the NLB Deployment Process
A Network Load Balancing cluster comprises multiple servers running any version of the Microsoft® Windows® Server 2003 2003 family, including Windows Server 2003 2003 Standard Edition, Windows Server 2003 2003 Enterprise Edition, Windows Server 2003 2003 Datacenter Edition, and Windows Server 2003 2003 Web Edition.
Clustering allows you to combine application servers to provide a level of scaling, availability, or security that is not possible with an individual server. Network Load Balancing distributes incoming client requests among the servers in the cluster to more evenly balance the workload of each server and prevent overload on any one server. To client computers, the Network Load Balancing cluster appears as a single server that is highly scalable and fault tolerant. The Network Load Balancing deployment process assumes that your design team has completed the design of the Network Load Balancing solution for your organization and has performed limited testing in a lab. After the design team tests the design in the lab, your deployment team implements the Network Load Balancing solution first in a pilot environment and then in your production environment.
Upon completing the deployment process presented here, your Network Load Balancing solution (the Network Load Balancing cluster and the applications and services running on the cluster) will be in place. For more information about the procedures for deploying Network Load Balancing on individual servers, see the appropriate Network Load Balancing topics in Help and Support Center for Windows Server 2003 2003.

Incorrect Answers:
B: We already have three servers. A cluster would require different hardware and would thus be more expensive.
C: We already have three servers. A cluster would require different hardware and would thus be more expensive.
D: Round Robin DNS would load balance the servers, but if one server failed, clients would still be directed to the failed server.

QUESTION NO: 42
You are a network administrator for TestKing. The company consists of a single Active Directory domain named testking.com. All client computers run Windows XP Professional.

The company's main office is located in Dallas. You are a network administrator at the company's branch office in Boston. You create a Group Policy object (GPO) that redirects the Start menu for users in the Boston branch office to a shared folder on a file server.

Several users in Boston report that many of the programs that they normally use are missing from their Start menus. The programs were available on the Start menu he previous day, but did not appear when the users logged on today.

You log on to one of the client computers. All of the required programs appear on the Start menu. You verify that users can access the shared folder on the server.

You need to find out why the Start menu changed for these users.

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

A. In the Group Policy Management Console (GPMC), select the file server that hosts the shared folder and a user account that is in the Domain Admins global group and run Resultant Set Of Policy (RSoP) in planning mode.
B. In the Group Policy Management Console (GPMC), select one of the affected user accounts and run Resultant Set of Policy (RSoP) in logging mode.
C. On one of the affected client computers, run the **gpresult** command.
D. On one of the affected client computers, run the **gpupdate** command.
E. On one of the affected client computers, run the **secedit** command.

Answer: B, C
Explanation: We need to view the effective group policy settings for the users or the computers that the users are using. We can use gpresult of RSoP.

Gpresult

Displays Group Policy settings and Resultant Set of Policy (RSoP) for a user or a computer.

RSoP overviewResultant Set of Policy (RSoP) is an addition to Group Policy

RSoP provides details about all policy settings that are configured by an Administrator, including Administrative Templates, Folder Redirection, Internet Explorer Maintenance, Security Settings, Scripts, and Group Policy Software Installation.

RSoP consists of two modes:

Planning mode and logging mode. With planning mode, you can simulate the effect of policy settings that you want to apply to a computer and user.

Logging mode reports the existing policy settings for a computer and user that is currently logged on.

Incorrect Answers:
A: We need to test the effective policy from a user's computer, not the file server.
D: Gpudate, is the tool used to refresh the policy settings in Windows XP and Windows Server 2003.
E: Secedit is the tool used to refresh the policy in Windows 2000 professional and server editions.

QUESTION NO: 43
You are the systems engineer for TestKing GmBh. The network consists of three Windows NT 4.0 domains in a master domain model configuration. The servers on the network run either Windows NT Server 4.0 or Windows 2000 Server. All domain controllers run Windows NT Server 4.0.

The network also contains 10 UNIX-based application servers. All host name resolution services are provided by a UNIX-based server running the latest version of BIND, which currently hosts the zone for the testking.com domain. All NetBIOS name resolution services are provided by two Windows 2000 Server WINS servers.

The company is in the process of migrating to a single Windows Server 2003 Active Directory domain-based network. The new domain is named testking-ad.com, and it will be hosted in an Active Directory-integrated zone that is stored on the domain controllers. Servers that are not domain controllers will not be updated at this time. The migration plan requires that all computers must use DNS to resolve host names and computer redundancy for the Windows-based DNS servers.

You upgrade the domain controllers in the master domain to Windows Server 2003. You also migrate all user and computer accounts to the new Active Directory domain. The DNS zone on the Windows Server 2003 computers is configured as shown in the exhibit.

You now need to configure the required redundancy between the Windows-based DNS servers and the UNIX-based DNS server. You need to ensure that there will be no service interruption on any of the DNS server computers.

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

A. On a Windows Server 2003 DNS server, create a secondary zone that uses the UNIX-based DNS server as the master server.
B. On the UNIX-based DNS server, create a secondary zone that uses a Windows-based DNS server as the master server.
C. On a Windows Server 2003 DNS server, create a stub zone that uses the UNIX-based DNS server as the master server.
D. Add a delegation in the testking.com zone that delegates authority of the testking-ad.com zone to a Windows Server 2003 DNS server.
E. Configure the testking-ad.com zone to not replicate WINS-specific resource records during zone transfers.

Answer: B, E
Explanation: This is a trick question because it is asking for redundancy for the Windows 2003 DNS servers. We can provide this by configuring the UNIX DNS server to resolve names in the testking-ad.com domain. With a secondary zone on the UNIX DNS server, the UNIX DNS server will be able to resolve host name resolutions requests in the testking-ad.com domain. The testking-ad.com DNS is configured to query WINS if required. When configuring a UNIX DNS server with a secondary zone, we should configure the zone to not replicate WINS-specific resource records during zone transfers.

Incorrect Answers:
A: This would provide redundancy for the UNIX server; the question isn't asking for that.
C: This won't provide any redundancy.
D: Testking-ad.com isn't a subdomain of testking.com so no delegation is required.

QUESTION NO: 44
You are the network administrator for TestKing. The network consists of an internal network and a perimeter network. The internal network is protected by a firewall. The perimeter network is exposed to the Internet.

You are deploying 10 Windows Server 2003 computers as Web servers. The servers will be located in the perimeter network. The servers will host only publicly available Web pages.

You want to reduce the possibility that users can gain unauthorized access to the servers. You are concerned that a user will probe the Web servers and find ports or services to attack.

What should you do?

A. Disable File and Printer Sharing on the servers.
B. Disable the IIS Admin service on the servers.
C. Enable Server Message Block (SMB) signing on the servers.

D. Assign the Secure Server (Require Security) IPSec policy to the servers.

Answer: A
Explanation: We can secure the web servers by disabling File and Printer sharing.

File and Printer Sharing for Microsoft Networks
The File and Printer Sharing for Microsoft Networks component allows other computers on a network to access resources on your computer by using a Microsoft network.
This component is installed and enabled by default for all VPN connections. However, this component needs to be enabled for PPPoE and dial-up connections. It is enabled per connection and is necessary to share local folders. The File and Printer Sharing for Microsoft Networks component is the equivalent of the Server service in Windows NT 4.0.

File and Printer sharing is not required on web servers because the web pages are accesses over web protocols such as http or https, and not over a Microsoft LAN.

Incorrect Answers:
B: This is needed to administer the web servers. Whilst it could be disabled, disabling File and Printer sharing will secure the servers more.
C: SMB signing is used to verify, that the data has not been changed during the transit through the network. It will not help in reducing the possibility that users can gain unauthorized access to the servers.
D: This will prevent computers on the internet accessing the web pages.

QUESTION NO: 45
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. TestKing's perimeter network contains 50 Web servers that host the company's public Internet site. The Web servers are not members of the domain.

The network design team completed a new design specification for the security of servers in specific roles. The network design requires that security settings must be applied to Web servers. These settings include password restrictions, audit settings, and automatic update settings.

You need to comply with the design requirements for securing the Web servers. You also want to be able to verify the security settings and generate a report during routine maintenance. You want to achieve these goals by using the minimum amount of administrative effort.

What should you do?

A. Create a custom security template named Web.inf that contains the required security settings.

Create a new organizational unit (OU) named WebServers and move the Web servers into the new OU. Apply Web.inf to the WebServers OU.

B. Create a custom security template named Web.inf that contains the required security settings, and deploy Web.inf to each Web server by using Security Configuration and Analysis.
C. Create an image of a Web server that has the required security settings, and replicate the image to each Web server.
D. Manually configure the required security settings on each Web server.

Answer: B
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 using the Security Configuration and Analysis tool.

Incorrect Answers:
A: The web servers aren't members of the domain. Therefore they cannot be moved to an OU in Active Directory.
C: We cannot use imaging in this way.
D: This is a long way of doing it. A security template would simply the task.

QUESTION NO: 46
You are the network administrator for TestKing. The network contains a Windows Server 2003 Web server that hosts the company intranet.

The human resources department uses the server to publish information relating to vacations and public holidays. This information does not need to be secure.

The finance department wants to publish payroll information on the server. The payroll information will be published in a virtual directory named Payroll, which was created under the default Web site on the server. The company's written security policy states that all payroll-related information must be encrypted on the network.

You need to ensure that all payroll-related information is encrypted on the network. To preserve performance, you need to ensure that other information is not encrypted unnecessarily. You obtain and install a server certificate.

What else should you do?

A. Select the **Require secure channel (SSL)** check box for the default Web site.
B. Assign the Secure Server (Require Security) IPSec policy option for the server.

C. Select the **Encrypt contents to secure data** check box for the Payroll folder.
D. Select the **Require secure channel (SSL)** check box for the Payroll virtual directory.

Answer: D
Explanation: Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

Incorrect Answers:
A: This will encrypt all data from the web server. We only need to encrypt the payroll data.
B: This will encrypt all data from the web server. We only need to encrypt the payroll data.
C: This will encrypt the data on the hard disk using EFS. It won't encrypt the data as it is transferred over the network.

QUESTION NO: 47
You are a network administrator for TestKing Inc. The network consists of a single Active Directory forest as shown in the exhibit.

TestKing's written security policy requires that all domain controllers in the child1.testking.com domain must accept a LAN Manager authentication level of only NTLMv2. You also want to restrict the ability to start a domain controller to the Domain Admins group.

You need to configure the domain controllers in the child1.testking.com domain to meet the new security requirements.

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

A. Import the Rootsec.inf security template into the Default Domain Controllers Policy Group Policy object (GPO) on the child1.testking.com domain.
B. Import the Rootsec.inf security template into the Default Domain Policy Group Policy object (GPO) in the child1.testking.com domain.
C. Import the Securedc.inf security template into the Default Domain Controllers Policy Group Policy object (GPO) in the child1.testking.com domain.
D. Import the Securedc.inf security template into the Default Domain Policy Group Policy object (GPO) in the child1.testking.com domain.
E. Run the system key utility (syskey) on each domain controller in the child1.testking.com domain. In the **Account Database Key** dialog box, select the **Password Startup** option.
F. Run the system key utility (syskey) on each domain controller in the child1.testking.com domain. In the **Account Database Key** dialog box, select the **Store Startup Key Locally** option.

Answer: C, E
Secure (Secure*.inf) Template
The Secure templates define enhanced security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings.
Additionally, the Secure templates limit the use of LAN Manager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LAN Manager responses.

- In order to apply Securews.inf to a member computer, all of the domain controllers that contain the accounts of all users that log on to the client must run Windows NT 4.0 Service Pack 4 or higher.

The system key utility (SYSKEY)
A security measure used to restrict logon names to user accounts and access to computer systems and resources. By running the syskey utility with the Password startup option, the account information in the directory services is encrypted and a password needs to be entered during system start. The start of the Domain Controllers is therefore restricted to everybody with this password.

Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/syskey_concept.asp

System key option	Relative security level	Description
System Generated Password, Store Startup Key Locally	Secure	Uses a computer-generated random key as the system key and stores an encrypted version of the key on the local computer. This option provides strong encryption of password information in the registry, and it enables the user to restart the computer without the need for an administrator to enter a password or insert a disk.
Administrator generated password, **Password Startup**	More secure	Uses a computer-generated random key as the system key and stores an encrypted version of the key on the local computer. The key is also protected by an administrator-chosen password. Users are prompted for the system key password when the computer is in the initial startup sequence. The system key password is not stored anywhere on the computer.
System Generated Password, Store Startup Key on Floppy Disk	Most secure	Uses a computer-generated random key and stores the key on a floppy disk. The floppy disk that contains the system key is required for the system to start, and it must be inserted at a prompt during the startup sequence. The system key is not stored anywhere on the computer.

Incorrect Answers:
A: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
B: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
D: We need to apply the policy to the domain controllers container, not the entire domain.
F: The System Key Utility (syskey) is used to encrypt the account password information that is stored in the SAM database or in the directory services. By selecting "Store Key locally" the computer stores an encrypted version of the key on the local computer. This doesn't help in controlling the start of the Domain Controllers.

QUESTION NO: 48
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All computers on the network are members of the domain. The domain contains a Windows Server 2003 computer named TestKing5.

You are planning a public key infrastructure (PKI) for the company. You want to deploy a certification authority (CA) on TestKing5.

You create a new global security group named Cert Administrators. You need to delegate the tasks to issue, approve, and revoke certificates to members of the Cert Administrators group.

What should you do?

A. Add the c group in the domain.
B. Configure the Certificates Templates container in the Active Directory configuration naming context to assign the Cert Administrators group the **Allow – Write** permission.
C. Configure the CertSrv virtual directory on TestKing5 to assign the Cert Administrators group the **Allow – Modify** permission.

D. Assign the Certificate Managers role to the Cert Administrators group.

Answer: D
Explanation: To be able to issue, approve and revoke certificates, the Cert Administrators group needs to be assigned the role of Certificate Manager. The following table describes different roles and their associated permissions.

Roles and groups	Security permission	Description
CA Administrator	**Manage CA** permission	Configure and maintain the CA. This is a CA role and includes the ability to assign all other CA roles and renew the CA certificate.
Certificate Manager	**Issue and Manage Certificates** permission	Approve certificate enrollment and revocation requests. This is a CA role. This role is sometimes referred to as CA Officer.
Backup Operator	**Back up file and directories** and **Restore file and directories** permissions	Perform system backup and recovery. This is an operating system role.
Auditor	**Manage auditing and security log** permission	Configure, view, and maintain audit logs. This is an operating system role.
Enrollees	Authenticated Users	Enrollees are clients who are authorized to request certificates from the CA. This is not a CA role.

QUESTION NO: 49
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All computers on the network are members of the domain. All servers run Windows Server 2003 and all client computers run Windows XP Professional.

You are planning a security update infrastructure.

You need to find out which computers are exposed to known vulnerabilities. You need to collect the information on existing vulnerabilities for each computer every night. You want this process to occur automatically.

What should you do?

A. Schedule the **secedit** command to run every night.
B. Schedule the **mbsacli.exe** command to run every night.
C. Install Microsoft Baseline Security Analyzer (MBSA) on one of the servers.
Configure Automatic Updates on all other computers to use that server.
D. Install Software Update Services (SUS) on one of the servers.
Configure the SUS server to update every night.

Answer: B
Explanation: We can schedule the mbsacli.exe command to periodically scan for security vulnerabilities.

Running a Scan Against All Computers in a Domain Using a Batch File:

Create a batch file called *mbsascan.cmd* with the following text:

```
@Echo Off
CLS
Set MBSA_Install_Path="C:\Program Files\Microsoft Baseline Security Analyzer"
cls
cd %MBSA_Install_Path%
mbsacli.exe /d edc /n password
Echo Scan complete
Pause
Exit
```

To run the tool from the command line (from the MBSA installation folder), type mbsacli.exe, and use the following parameters.

To Select Which Computer to Scan

- no option - Scan the local computer.
- r /c *domainname\computername*- Scan the named computer.
- /i *xxx.xxx.xxx.xxx* - Scan the named IP address.
- /r *xxx.xxx.xxx.xxx* - *xxx.xxx.xxx.xxx* - Scan the range of IP addresses.
- /d *domainname* - Scan the named domain.

To Select Which Scan Options to Not Perform
Note You can concatenate these options. For example, you can use/n OS + IIS + *Updates*.

- /n IIS - Skip IIS checks.
- /n OS - Skip Windows operating system checks.
- /n Password - Skip password checks.
- /n SQL - Skip SQL checks.
- /n Updates - Skip security update checks.

Security Update Scan Options

- /sus *SUS server* - Check only for security updates that are approved at the specified SUS server.
- /s 1 - Suppress security update check notes.
- /s 2 - Suppress security update check notes and warnings.
- /nosum - Security update checks will not test file checksums.

To Specify the Output File Name Template

- /o *domain* - *computername* (*date*)

To Display the Results and Details

- /e - List the errors from the latest scan.
- /l - List all the reports that are available.
- /ls - List the reports from the latest scan.
- /lr *report name* - Display an overview report.
- /ld *report name* - Display a detailed report.

Miscellaneous Options

- /? - Usage help.
- /qp - Do not display progress.
- /qe - Do not display error list.
- /qr - Do not display report list.
- /q - Do not display progress, error list, or report list.
- /f - Redirect the output to a file.

MBSA is the graphical interface of Mbsacli.exe.

This can be installed and run on Microsoft® Windows® 2000 Server, Windows 2000 Professional, Windows XP Home Edition, Windows XP Professional, and Windows Server 2003. The tool can be run over the network against Microsoft Windows NT® 4.0 Server and Windows NT 4.0 Workstation, Windows 2000 Server, Windows 2000 Workstation, Windows XP Professional and Home Edition, and Windows Server 2003. MBSA does not run on or against Windows 95, 98 or Me systems.

- You can use MBSA by using the graphical user interface (GUI) or from the command line. The GUI executable is Mbsa.exe and the command line executable is Mbsacli.exe.
- MBSA uses ports 138 and 139 to perform its scans.
- MBSA requires administrator privileges on the computer that you scan. The options /u (username) and /p (password) can be used to specify the username to run the scan. Do not store user names and passwords in text files such as command files or scripts.
- MBSA requires the following software:
    - Windows NT 4.0 SP4 and above, Windows 2000, or Windows XP (local scans only on Windows XP computers that use simple file sharing)
    - IIS 4.0, 5.0 (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
- The section Additional Information later in this How To includes tips on working with MBSA.

Scanning for Security Updates and Patches
You can run Mbsa.exe and Mbsacli.exe with options to verify the presence of security patches.

QUESTION NO: 50
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All computers on the network are members of the domain. The network contains a Windows Server 2003 computer named TestKingCA.

The company uses an enterprise certification authority (CA) on TestKingCA to issue certificates. A certificate to encrypt files is autoenrolled to all users. The certificate is based on a custom Encryption File System (EFS) certificate template. The validity period if the certificate is set to two years.

Currently, the network is configured to use data recovery agents. You are planning to implement key archival for the keys that users use to decrypt files.

You configure the CA and the custom EFS certificate template to enable key archival of the encryption private keys.

You need to ensure that the private EFS key of each user who logs on to the domain is archived.

What should you do?

A. Configure a new issuance policy for the custom EFS certificate template.
B. Configure the custom EFS certificate template to reenroll all certificate holders.
C. Select the **Automatically Enroll Certificates** command in the Certificates console.
D. Configure a logon script that runs the **gpupdate.exe /force** command for the users.

Answer: B
Explanation: The question states **A certificate to encrypt files is autoenrolled to all users.** We have now modified the custom EFS certificate template to enable key archival of the encryption private keys. Therefore, we now need to reenroll all certificate holders so that they get new certificates based on the new template, and their keys are archived.

Key Archival and Management in Windows Server 2003

Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/kyacws03.asp

EFS always attempts to enroll for the Basic EFS template. The EFS driver generates an autoenrollment request that Autoenrollment tries to fulfill. For customers that want to ensure that a specific template is used for EFS (such as to include **key archival)**, the new template should supercede the Basic EFS template. This will ensure that Autoenrollment will not attempt enrollment for Basic EFS any more.

Key Archival

The private key database is the same as the database used to store the certificate requests. The Windows Server 2003 Certification Authority database has been extended to support storing the encrypted private key along with the associated encrypted symmetric key and issued certificate. The recovery blob will be stored in the same row as the signed certificate request and any other information the CA persists in its database for each request transaction. The actual encrypted blob is stored as an encrypted PKCS #7 blob.
The Microsoft Certification Authority uses the JET database engine upon which various JET utilities may be used for maintenance purposes.

QUESTION NO: 51
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All member servers run Windows Server 2003. All client computers run Windows XP Professional. All client computer accounts in the domain are located in an organizational unit (OU) named Workstations.

You need to distribute a new application to all client computers on the network. You create a Group Policy object (GPO) that includes the application package in the software installation settings of the Computer Configuration section of the GPO. You assign the GPO to the Workstations OU.

Several days later, users report that the new application is still not installed on their client computers.

You need to ensure that the application is installed on all client computers.

What should you do?

A. Instruct users to restart their client computers.
B. Instruct users to run Windows Update on their client computers.
C. Instruct users to force a refresh of the computer policy settings on their client computers.
D. Instruct users to force a refresh of the user policy settings on their client computers.

Answer: A

Explanation: When an application is assigned to a computer, the software is deployed when it is safe to do so (that is, when the operating system files are closed). This generally means that the software will be installed when the computer starts up, which ensures that the applications are deployed prior to any user logging on. For this scenario, we need to tell the users to restart their client computers.

Incorrect Answers:
B: Windows Update is used to update the operating system with the latest security patches etc.
C: You applied the policy several days ago. The client computers should have the GPO by now.
D: The setting isn't in the user section of the group policy.

When you assign applications to users or computers, the applications are automatically installed on their computers at logon (for user-assigned applications) or startup (for computer-assigned applications.)

When assigning applications to users, the default behavior is that the application will be advertised to the computer the next time the user logs on. This means that the application shortcut appears on the Start menu, and the registry is updated with information about the application, including the location of the application package and the location of the source files for the installation.

With this advertisement information on the user's computer, the application is installed the first time the user tries to use the application. In addition to this default behavior, Windows XP Professional and Windows Server 2003 clients support an option to fully install the package at logon, as an alternative to installation upon first use. Note that if this option is set, it is ignored by computers running Windows 2000, which will always advertise user-assigned applications.

When assigning applications to computers, the application is installed the next time the computer boots up. Applications assigned to computers are not advertised, but are installed with the default set of features configured for the package. Assigning applications through Group Policy requires that the application setup is authored as a Windows Installer (.msi) package.

Reference:

Group Policy Help

QUESTION NO: 52
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com

TestKing merges with a company named Acme. You need to create new user accounts for all of the Acme employees.

The e-mail address format for all users at Acme is *alias*@acme.com. The users need to continue to use their e-mail addresses after the merger. To decrease confusion, these users also need to be able to use their e-mail addresses as their user logon names when logging on to the company network.

You need to ensure that new users can log on by using their e-mail addresses as their logon names. You want to achieve this goal by incurring the minimum cost and by using the minimum amount of administrative effort.

What should you do?

A. Create a new domain tree named acme.com in the testking.com forest.
   Create user accounts for all of the users in the acme.com domain.
B. Create a new forest named acme.com.
   Create user accounts for all of the users in the acme.com domain.
   Configure a forest trust relationship between the two forests.
C. Create user accounts for all of the new users in the testking.com domain.
   Configure the e-mail addresses for all of the Acme users as *alias*@acme.com.
D. Configure acme.com as an additional user principal name (UPN) suffix for the testking.com forest.
   Configure each user account to use the acme.com UPN suffix.

Answer: D
Explanation:

Enabling UPN Logon
You can simplify the logon process for users by enabling UPN logon. When UPN logon is enabled, all users use the same UPN suffix to log on to their domains. This might be users' e-mail address. For example, a user, Bob, in the Reskit domain enters bob@Reskit.com for his UPN logon name. In this way, he does not have to select a domain from a long list. UPN names are comprised of the user's logon name and the DNS name of the domain. When you enable UPN logon, users' logon names remain the same even when their domains change.
You might choose to enable UPN logon if your system meets the following criteria:

- Domain names in your enterprise are complex and difficult to remember.
- Users in your organization might change domains as a result of domain consolidation or other organizational changes.
- All domains in the forest are in native mode.
- User logon names are unique within the forest.
- A global catalog server is available to match the UPN to the correct domain account.

You can use one UPN suffix for all users in the forest. For example, alice@Reskit.com might be a member of the noam domain, a child domain of the Reskit domain. In this way, when Alice logs on, she does not need to

know which domain she is logging on to because a global catalog will find the domain that contains her user account. If Alice moves to another domain, she still logs on with the same UPN suffix.
To enable UPN logon for all accounts, use Active Directory Users and Computers to edit the user's account to select a specific UPN suffix, such as the forest root of a domain.

To enable UPN logon

1. In **Active Directory Users and Computers**, right-click the user's account.
2. Click **Properties**, and click the **Account** tab.
3. Select one of the UPN suffixes from the **User logon name** drop down combo box.

Reference: MS White paper Designing an Authentication Strategy

QUESTION NO: 53
You are the network administrator for TestKing. The company consists of two subsidiaries named Contoso, Ltd, and City Power & Light. The network contains two Active Directory forests named contoso.com and cpand1.com. The functional level of each forest is Windows Server 2003.

A two-way forest trust relationship exists between the forests.

You need to achieve the following goals:

- **Users in the contoso.com forest must be able to access all resources in the cpand1.com forest.**
- **Users in the cpand1.com forest must be able to access only resources on a server named HRApps.contoso.com.**

You need to configure the forest trust relationship and the resources on HRApps.contoso.com to achieve the goals.

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

A. On a domain controller in the contoso.com forest, configure the properties of the incoming forest trust relationship to use selective authentication.

B. On a domain controller in the contoso.com forest, configure the properties of the incoming forest trust relationship to use forest-wide authentication.

C. On a domain controller in the cpand1.com forest, configure the properties of the incoming forest trust relationship to use selective authentication.

D. On a domain controller in the cpand1.com forest, configure the properties of the incoming forest trust relationship to use forest-wide authentication.

E. Modify the discretionary access control list (DACLs) on HRApps.contoso.com to allow access to the Other Organization security group.

F. Modify the discretionary access control lists (DACLs) on HRApps.contoso.com to deny access to This Organization security group.

Answer: A, D, E

Authentication between Windows Server 2003 forests
When all domains in two forests trust each other and need to authenticate users, establish a forest trust between the forests. When only some of the domains in two Windows Server 2003 forests trust each other, establish one-way or two-way external trusts between the domains that require interforest authentication.

Selective authentication between forests
Using Active Directory Domains and Trusts, you can determine the scope of authentication between two forests that are joined by a forest trust
You can set selective authentication differently for outgoing and incoming forest trusts. With selective trusts, administrators can make flexible forest-wide access control decisions.
If you use forest-wide authentication on an incoming forest trust, users from the outside forest have the same level of access to resources in the local forest as users who belong to the local forest. For example, if ForestA has an incoming forest trust from ForestB and forest-wide authentication is used, users from ForestB would be able to access any resource in ForestA (assuming they have the required permissions).
If you decide to set selective authentication on an incoming forest trust, you need to manually assign permissions on each domain and resource to which you want users in the second forest to have access. To do this, set a control access right *Allowed to authenticate* on an object for that particular user or group from the second forest.

When a user authenticates across a trust with the **Selective authentication** option enabled, an *Other Organization* security ID (SID) is added to the user's authorization data. The presence of this SID prompts a check on the resource domain to ensure that the user is allowed to authenticate to the particular service. Once the user is authenticated, then the server to which he authenticates adds the *This Organization* SID if the *Other Organization* SID is not already present. Only one of these special SIDs can be present in an authenticated user's context.

QUESTION NO: 54
You are a network administrator for TestKing. The network consists of a single Active Directory forest that contains one root domain and multiple child domains. The functional level of all child domains is Windows Server 2003. The functional level of the root domain is Windows 2000 native.

You configure a Windows Server 2003 computer named TestKing1 to be a domain controller for an existing child domain. TestKing1 is located at a new branch office, and you connect TestKing1 to a central data center by a persistent VPN connection over a DSL line. TestKing1 has a single replication connection with a bridgehead domain controller in the central data center.

You configure DNS on TestKing1 and create secondary forward lookup zones for each domain in the forest.

You need to minimize the amount of traffic over the VPN connection caused by logon activities.

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

A. Configure the DNS zones to be Active Directory-integrated zones.
B. Configure TestKing1 to be the PDC emulator for the domain.
C. Configure TestKing1 to be a global catalog server.
D. Configure universal group membership caching on TestKing1.

Answer: C, D
Explanation:
Logon traffic over the VPN is caused by the local domain controller retrieving universal group information from a global catalog server. We can reduce this traffic by either configuring TestKing1 to be a global catalog server, or by enabling universal group membership caching on TestKing1.

Global catalog server
A global catalog server is a domain controller that stores information about all objects in the forest, but not their attributes, so that applications can search Active Directory without referring to specific domain controllers that store the requested data. Like all domain controllers, a global catalog server stores full, writable replicas of the schema and configuration directory partitions and a full, writable replica of the domain directory partition for the domain that it is hosting.

Universal group membership caching
Universal group membership caching allows the domain controller to cache universal group membership information for users. You can enable domain controllers that are running Windows Server 2003 to cache universal group memberships by using the Active Directory Sites and Services snap-in.
Enabling universal group membership caching eliminates the need for a global catalog server at every site in a domain, which minimizes network bandwidth usage because a domain controller does not need to replicate all of the objects located in the forest. It also reduces logon times because the authenticating domain controllers do not always need to access a global catalog to obtain universal group membership information.

Reference

MS Windows Server 2003 Deployment Kit
Designing and Deploying Directory and Security Services
Active Directory Replication Concepts

Incorrect Answers:
A: Logon traffic over the VPN is caused by the local domain controller retrieving universal group information from a global catalog server. It is not cause by DNS replication.
B: The PDC emulator isn't used in the logon process (except for down-level clients).

QUESTION NO: 55
You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The Active Directory database contains 500 MB of information.

TestKing has its main office in Moscow and a branch office in Minsk. The two offices are connected by a 56-Kbps WAN connection that is used only for Active Directory replication. The Moscow office has 450 users, and the Minsk office has 15 users.

The Minsk office has a single Windows Server 2003 domain controller and two Windows Server 2003 file and print servers. The hard disk containing the operating system on the domain controller in Minsk fails and cannot be recovered.

You need to re-establish a domain controller that contains a current copy of Active Directory in the Minsk office. You need to achieve this goal as quickly as possible.

What should you do?

A. Replace the hard disk on the domain controller.
Install Windows Server 2003 on the domain controller.
Install Active Directory from restored backup files.
B. Install Active Directory on a file and print server.
Force replication.
C. Install Active Directory on a file and print server from restored backup files.
D. Replace the hard disk on the domain controller.
Install Windows Server 2003 on the domain controller.
Force replication.

Answer: C
Explanation: We need to re-establish a domain controller in the Minsk office as quickly as possible. Therefore, we should install Active Directory from restored backup files. Answer A is the recommended answer, but answer C is quicker.

We can use the new dcpromo /adv command to promote the DC from a backup of the system state data of an existing domain controller.

The /adv switch
Is only necessary when you want to create a domain controller from restored backup files. It is not required when creating an additional domain controller over the network.

For additional domain controllers in an existing domain, you have the option of using the install from media feature, which is new in Windows Server 2003. Install from media allows you to pre-populate Active Directory with System State data backed up from an existing domain controller. This backup can be present on local CD, DVD, or hard disk partition.

Installing from media drastically reduces the time required to install directory information by reducing the amount of data that is replicated over the network. Installing from media is most beneficial in large domains or for installing new domain controllers that are connected by a slow network link.

Incorrect Answers:
A: This would work but answer C is quicker.
B: We don't want to replicate a 500MB Active Directory database over a 56Kbps WAN link.
D: We don't want to replicate a 500MB Active Directory database over a 56Kbps WAN link.

QUESTION NO: 56
You are the network administrator for TestKing. The network consists of a single Active Directory domain that contains only one domain controller. The domain controller is named TestKingSrvA. The domain contains only one site named Valencia.

You are adding a new site named Barcelona. You need to promote an existing Windows Server 2003 member server named TestKingSrvB to be an additional domain controller of the domain. A 56Kbps WAN connection connects the Valencia and Barcelona sites.

You need to install TestKingSrvB as a new domain controller on the Barcelona site. You need to minimize the use of the WAN connection during this process.

What should you do?

A. Set the site link cost between the Valencia and Barcelona sites to 50.
   Promote TestKingSrvB to be an additional domain controller in the Barcelona site.
B. Restore the backup files from the system state data on TestKingSrvA to a folder on TestKingSrvB and install Active Directory by running the **dcpromo /adv** command.
C. Promote TestKingSrvB to be an additional domain controller by running the **dcpromo** command over the network.

D. Promote TestKingSrvB to be an additional domain controller by using an unattended installation file.

Answer: B
Explanation:
We want to minimize the use of the WAN link. We can use the new dcpromo /adv command to promote the DC from a backup of the system state data of an existing domain controller.

The /adv switch
Is only necessary when you want to create a domain controller from restored backup files. It is not required when creating an additional domain controller over the network.

For additional domain controllers in an existing domain, you have the option of using the install from media feature, which is new in Windows Server 2003. Install from media allows you to pre-populate Active Directory with System State data backed up from an existing domain controller. This backup can be present on local CD, DVD, or hard disk partition.

Installing from media drastically reduces the time required to install directory information by reducing the amount of data that is replicated over the network. Installing from media is most beneficial in large domains or for installing new domain controllers that are connected by a slow network link.

To use the install from media feature, you first create a backup of System State from the existing domain controller, then restore it to the new domain controller by using the Restore to: Alternate location option.

In this scenario, we can restore the system state data to a member server, then use that restored system state data to promote a member server to a domain controller.

Reference
Server Help

QUESTION NO: 57
You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. Each client computer runs either Windows XP Professional or Windows 2000 Professional.

The company requires that all users log on by using smart cards. You deploy Certificate Services and smart card readers. You configure auto-enrollment to issue certificates to users. Users report that they cannot log on by using a smart card.

You need to ensure that all users can log on by using a smart card.

What should you do?

A. In Active Directory Users and Computers, configure all user accounts to require a smart card for interactive logon.
B. Configure the domain security policy to require smart cards for interactive logon.
C. Use the Certificate Services Web site to enroll each user for a smart card certificate.
D. Add a copy of the enterprise root certificate to the trusted root certification authorities store on each client computer.

Answer: C
Explanation:
Although the question says "you configure auto-enrollment to issue certificates to users", it doesn't say what type of certificates were auto-enrolled. You can use the Certificate Services Web site to enroll each user for a smart card certificate.

Incorrect answers:

A: This is not necessary. With this setting disabled, the users can log on using any method.
B: This is not necessary. With this setting disabled, the users can log on using any method.
D: In a single domain, the Certificate Authority would be trusted by the client computers in the domain. Therefore, it is not necessary to add a copy of the enterprise root certificate to the trusted root certification authorities store on each client computer.

Enrolling for a smart card certificate
A domain user cannot enroll for a Smart Card Logon certificate (which provides authentication) or a Smart Card User certificate (which provides authentication plus the capability to secure e-mail) unless a system administrator has granted the user access rights to the certificate template stored in Active Directory. Enrollment for a smart card certificate must be a controlled procedure, in the same manner that employee badges are controlled for purposes of identification and physical access.

The recommended method for enrolling users for smart card-based certificates and keys is through the Smart Card Enrollment station that is integrated with Certificate Services in Windows 2000 Server and Windows 2000 Advanced Server.

When an enterprise certification authority (CA) is installed, the installation includes the Smart Card Enrollment station. This allows an administrator to act on behalf of a user to request and install a Smart Card Logon certificate or Smart Card User certificate on the user's smart card. Prior to using the Smart Card Enrollment station , the smart card issuer must have obtained a signing certificate based on the Enrollment Agent certificate template. The signing certificate will be used to sign the certificate request generated on behalf of the smart card recipient.

By default, only domain administrators are granted permission to request a certificate based on the Enrollment Agent template. A user other than a domain administrator can be granted permission to enroll for an Enrollment Agent certificate by means of Active Directory Sites and Services. It's very important to note that once someone has an Enrollment Agent certificate, they can enroll for a certificate and generate a smart card on behalf of anyone in the organization. The resulting smart card could then be used to log on to the network and impersonate the real user.

Group Policy
Interactive logon: Require smart card

- Description

This security setting requires users to log on to a computer using a smart card.
The options are:

- Enabled. Users can only log on to the computer using a smart card.
- Disabled. Users can log on to the computer using any method.

Default: Disabled.

Planning Smart Card Certificate Templates
You can use any of the following types of Windows Server 2003 certificate templates to enable smart card use in the Windows Server 2003 PKI:

- Enrollment Agent. Allows an authorized user to serve as a certificate request agent on behalf of other users.
- Smart Card User. Enables a user to log on and sign e-mail.
- SmartCardLogon. Enables a user to log on by using a smart card.

Establishing Enrollment Agents
If you decide to control smart card issuance from a central location, you need to authorize one or more individuals within the organization to be enrollment agents.
The enrollment agent needs to be issued an Enrollment Agent certificate, which makes it possible for the agent to enroll for certificates on behalf of users.

Server help
Certificate Services

Security Policy
Configurations settings

MS Windows Server 2003
Smarts Card Deploy

QUESTION NO: 58

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

User accounts are configured as local administrators so that users can install software. A desktop support team supports end users. The desktop support team's user accounts are all members of a group named Support.

You create a software restriction policy that only prevents users from running registry editing tools by file hash rule. You apply the policy to all user accounts in the domains.

The desktop support team reports that when they attempt to run registry editing tools, they receive the following error message:

"Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator".

You need to ensure that only the desktop support team can run registry editing tools.

What should you do?

A. Configure the software restriction policies to be enforced for all users except local administrators.
B. Make users members of the Power Users group instead of the Administrators group.
C. Use a logon script to copy the registry editing tools to the root of drive C.
   Assign the Domain Admins group the **Allow – Read** permission for the registry editing tools in the new location.
D. Filter the software restriction policy to prevent the Support group from applying the policy.

Answer: D
Explanation:
We can prevent the software restriction policy from applying to the support group by simply assigning the support group the Deny – Read and/or the Deny – Apply group policy permission.

Incorrect answers:
A: The users are local administrators. The policy must apply to the local administrators.
B: The policy applies to all users. It will still apply to the support group. Changing the local users group membership will have no effect on the policy.
C: The software restriction policy is using a hash rule to prevent the use of the registry editing tools. It doesn't matter where the tools are located, they still won't run.

QUESTION NO: 59
You are the network administrator for TestKing. Your user account is a member of the Schema Admins group. The network consists of a single Active Directory forest that contains three domains. The functional level of the forest is Windows Server 2003. A Windows Server 2003 domain controller named TestKingA holds the schema master role.

An application named Application1 creates additional schema classes. You notice that this application created some classes that have incorrect class names.

You need to correct the class names as quickly as possible.

What should you do?

A. Deactivate the Application1 classes that have the incorrect class names.
Set the default security permission for the Everyone group for those schema classes to **Deny**.
B. Deactivate the Application1 classes that have the incorrect class names.
Create the Application1 classes with the correct class names.
C. Rename the description of the Application1 classes to the correct class name.
Instruct the developers of Application1 to change the code of the application so that the renamed schema classes can be used.
D. Instruct the developers of Application1 to change the code of the application so that the application creates the new schema classes with the correct class names.
Reinstall Application1 and select **Reload the schema** in the Active Directory Schema console.

Answer: B
Explanation: We need to deactivate the Application1 classes that have the incorrect class names. This is because you cannot delete or rename a class. We can only deactivate the incorrect classes and recreate the classes with the correct class names.

Incorrect Answers:
A: It is not necessary to deny access to the classes after deactivating them. We need to recreate the classes with the correct names.
C: Changing the description of a class doesn't rename the class. It is not possible to rename a class.
D: We need to deactivate the classes that have the incorrect class names.

Extending the schema
When the set of classes and attributes in the base Active Directory schema do not meet your needs, you can extend the schema by modifying or adding classes and attributes. You should only extend the schema when absolutely necessary. The easiest way to extend the schema is through the Schema Microsoft Management Console (MMC) snap-in. You should always develop and test your schema extensions in a test lab before moving them to your production network.

Schema extensions are not reversible
Attributes or classes cannot be removed after creation. At best, they can be modified or deactivated.

Deactivating a class or attribute
Domain controllers running Windows Server 2003 do not permit the deletion of classes or attributes, but they can be deactivated if they are no longer needed or if there was an error in the original definition. A deactivated class or attribute is considered *defunct*. A defunct class or attribute is unavailable for use; however, it is easily reactivated.

If your forest has been raised to the Windows Server 2003 functional level, you can reuse the object identifier (governsId and attributeId values), the ldapDisplayName, and the schemaIdGUID that were associated with the defunct class or attribute. This allows you to change the object identifier associated with a particular class or attribute. The only exception to this is that an attribute used as a rdnAttId of a class continues to own its attributeId, ldapDisplayName, and schemaIdGuid values even after being deactivated (for example, those values cannot be reused).

If your forest has been raised to the Windows Server 2003 functional level, you can deactivate a class or attribute and then redefine it.

For example, the Unicode String syntax of an attribute called SalesManager could be changed to Distinguished Name. Since Active Directory does not permit you to change the syntax of an attribute after it has been defined in the schema, you can deactivate the SalesManager attribute and create a new SalesManager attribute that reuses the same object identifier and LDAP display name as the old attribute, but with the desired attribute syntax. You must rename the deactivated attribute before it can be redefined.

Reference Server Help

QUESTION NO: 60
You are a network administrator for TestKing. The network consists of single Active Directory forest that contains two domains and four sites. All servers run Windows Server 2003. You are responsible for administering domain controllers in one site. Your site contains four domain controllers. The hard disk that contains the Active Directory database fails on a domain controller named TESTKING2.
You replace the failed disk.

You need to recover TESTKING2. You need to achieve this goal without affecting existing Active Directory data.

What should you do?

A. Perform a nonauthoritative restoration of the Active Directory database.

B. Perform an authoritative restoration of the Active Directory database.
C. Use the Ntdsutil utility to run the **semantic database analysis** command.
D. Use the Ntdsutil utility to run the **restore subtree** command.

Answer: A
Explanation: You have four domain controllers in your site. You can simply perform a non-authoritative restore of the Active Directory database. Any changes to the Active Directory database since the data was backed up will be replicated from another domain controller.

Incorrect Answers:
B: This is not necessary. This will overwrite the Active Directory database on the other domain controllers. The other domain controllers will have the most recent copies of the Active Directory database. These changes can be replicated to the failed machine.
C: You can use this process to generate reports on the number of records present in the Active Directory database, including deleted and phantom records. It is not used to restore the Active Directory database.
D: We need to restore the entire Active Directory database, not just a subtree of it.

QUESTION NO: 61
You are the administrator for TestKing. The network consists of a single active directory domain named TestKing.com. All servers run windows server 2003

When the network was designed, the design team set design specifications. After the network was implemented, the deployment team set baseline specifications. The specifications for broadcast traffic are:

- **The design specifications requires that broadcast traffic must be 5 percent or less of total network traffic**
- **The baseline specifications showed that the broadcast traffic is always 1 percent or less of the total network traffic during normal operation**

You need to monitor the network traffic and find out if the level of broadcast traffic is within the design and baseline specs. You decide to use network monitor. After monitoring for 1 hour, you observe the results shown in the exhibit:

You need to report the results of your observations to management.

Which 2 actions should you take?

A. report that broadcast traffic is outside of the baseline specs
B. report that the broadcast traffic is outside of the design specs

C. report that the broadcast traffic is within the design specs
D. report that the broadcast traffic is within the baseline specs

Answers: Pending. Send your suggestion to feedback@testking.com.

QUESTION NO: 62
Your network contains Terminal servers that host legacy applications that require users to be members of the Power Users group in order to run them.

A new company policy states that the Power Users Group must be empty on all servers. You need to maintain the ability to run legacy applications on your servers when the new security requirement is enabled.

What should you do?

A. Add the domain users global group to the Remote Desktop Users built-in group in the domain
B. Add the domain users global group to the Remote Desktop Users local group on each terminal server
C. Modify the compatws.inf security template settings to allow members of the local users group to run the applications. Import the security settings into the default Domain Controllers Group Policy Object.
D. Modify the compatws.inf security template settings to allow members of the local users group to run the applications. Apply the modified template to each terminal server

Answer: D
Explanation: The default Windows 2000 security configuration gives members of the local Users group strict security settings, while members of the local Power Users group have security settings that are compatible with Windows NT 4.0 user assignments. This default configuration enables certified Windows 2000 applications to run in the standard Windows environment for Users, while still allowing applications that are not certified for Windows 2000 to run successfully under the less secure Power Users configuration. However, if Windows 2000 users are members of the Power Users group in order to run applications not certified for Windows 2000, this may be too unsecure for some environments. Some organizations may find it preferable to assign users, by default, only as members of the Users group and then decrease the security privileges for the Users group to the level where applications not certified for Windows 2000 run successfully. The compatible template (compatws.inf) is designed for such organizations. By lowering the security levels on specific files, folders, and registry keys that are commonly accessed by applications, the compatible template allows most applications to run successfully under a User context. In addition, since it is assumed that the administrator applying the compatible template does not want users to be Power Users, all members of the Power Users group are removed.

QUESTION NO: 63
You are the network admin for Contoso. The network consists of a single active directory domain named contoso.com. The domain is supported by an active directory integrated zone that allows only secure updates.

The contoso.com domain is configured as two active directory sites named Mainoffice and Branch1. Branch1 contains a single windows server 2003 domain controller named server1 that is not a DNS server. There is a single subnet of 192.168.10.0/24 in branch1 that contains all client computers and servers in the site.

Branch 1 is connected to Mainoffice by a single low bandwidth WAN connection that is often saturated. Users in Branch1 are normally authenticated by server1. Users in Branch1 report that they are experiencing unusually long logon times. You discover that Branch1 users are being authenticated by domain controllers in MainOffice. You run the nslookup command to query the SRV records for Branch1 and receive the output shown in the following table:

Server hostname	Server1.contoso.com
Server1.contoso.com internet address	192.168.10.65

You run the ipconfig command on server1 and receive the following:

IP address	192.168.10.32
Subnet mask	255.255.255.0
Default Gateway	192.168.10.1

You want server1 to resume authenticating all clients in Branch1. What should you do?

A. Run the ipconfig.exe registerdns command on server1
B. Run the ipconfig.exe /flushdns command on server1
C. Stop and restart the Netlogon service on server1
D. Stop and restart the Netlogon service on clients in Branch1

Answer: C
Explanation: The DNS record shows the wrong IP address for Server1. We need to configure the DNS with the correct information. Because server1 is a domain controller, we need to register the A records and the SRV records. The Net Logon service on a domain controller registers the DNS resource records required for the domain controller to be located in the network every 24 hours. To initiate the registration performed by Net Logon service manually, you can restart the Net Logon service.

Incorrect Answers:
A: This command will only register the A records. The client computers locate the domain controller by querying SRV records.
B: This will flush the local DNS client cache. This won't solve the problem.
D: We need to restart the Netlogon service on server1, not the clients.

QUESTION NO: 64
You are the network admin for TestKing. Your network contains 3 subnets. All servers have manually assigned IP addresses while all clients are configured to receive an address from a DHCP server. The DHCP server is located in Site 1. The DHCP server has a scope configured for each subnet.

Users in site 2 and site 3 are complaining that periodically they cannot connect to resources located on any subnet. You discover that during times of peak usage users are receiving an IP address in the 169.254.x.x address range.

You need to ensure that all client computers receive an address from their subnet even during times of peak usage.

What should you do?

A. Install one DHCP server in site 2 and site 3. On each DHCP server, configure identical scopes for each subnet
B. Install one DHCP server in Site 2 and Site 3. On each DHCP server configure a single subnet specific scope
C. Configure a DHCP Relay agent on Site 2 and Site 3
D. Configure a GPO on the domain that disables APIPA

Answer: B
Explanation: It appears that during times of peak usage, the DHCP server and/or the subnet containing the DHCP server cannot cope with the load. The clients in sites 2 and 3 are unable to receive an IP configuration from the DHCP server and so configure themselves with an APIPA configuration. We can ease the load on the DHCP server and subnet 1 by installing DHCP servers in Site 2 and Site 3. The DHCP servers must be configured with a single scope specific to the subnet.

Incorrect Answers:
A: We cannot have DHCP servers with identical scopes. This would lead to duplicate IP addresses on the network.
C: The clients can connect to the DHCP server during less busy times. Therefore, a DHCP Relay Agent is either already installed or isn't required.
D: Disabling APIPA won't ease the load on the DHCP server.

QUESTION NO: 65
You are the network admin for TestKing. The network contains Windows Server 2003 and Windows XP professional clients. All computers are members of the same active directory forest.

The company uses a Public Key Infrastructure (PKI) enabled application to manage marketing data. Certificates used with this application are managed by the application administrators. You install certificate services to create an offline stand alone root CA on one Windows Server 2003 server. You configure a 2nd Windows Server 2003 server as a stand alone sub CA

You instruct users in the marketing department to enroll for certificates by using the web enrollment tool on the stand alone Sub CA. Some users report that when they attempt to complete the enrollment process., they receive an error message on their certificate stating : This certificate cannot be verified up to a trusted certification authority". Other users in the Marketing department do not report the error.

You need to ensure that users in the marketing department do not continue to receive this error. You also need to ensure that users in the marketing department trust certificates issued by this CA. You create a new OU name Marketing. What else should you do?

A. Place all marketing department computer objects in the Marketing OU. Create a new GPO and link it to the Marketing OU. Publish the root CA's root certificate in the Trusted Root Certification Authorities Section of the GPO
B. Place all marketing department user objects in the Marketing OU. Create a new GPO and link it to the marketing OU. In the user configuration section of the GPO, configure a certificate trust list (CTL) that contains the sub's CA certificate
C. Place all marketing department computer objects in the Marketing OU. Create a new GPO and link it to the Marketing OU. In the computer configuration section of the GPO, configure a certificate trust list (CTL) that contains the sub's CA certificate
D. Place all marketing department user objects in the Marketing OU. Create a new GPO and link it to the marketing OU. In the user configuration section of the GPO, configure a certificate trust list (CTL) that contains the root's CA certificate

Answer: A

QUESTION NO: 66
You are the network admin for litware, inc. The company's written security policy requires that you maintain a copy of all private keys issued by TestKing's enterprise root CA

You create a duplicate of the user template named Employee and configure the template as shown in the Employee Properties exhibit:
*****MISSING*****

You configure the CA to archive private keys by using a Key Recovery Agent Certificate.

You create a test user account named peter and request a new employee certificate. You issue the certificate to Peter. You reinstall the OS on your test computer and attempt to recover Peter's private key. Your attempt fails and generates the following error message:

C:\ certutil –Getkey
CertUtil: - GetKeycommand failed
CertUtil: Cannot find object or property.

You need to ensure that future attempts to recover private keys associated with Employee certificates succeed

What should you do?

A. Using Group Policy, deploy a copy of the key recovery agent certificate to all client computers
B. In the Employee template, select the Archive subject's encryption private key check box
C. In the employee template, select the Allow private key to be exported check box
D. Run the certutil – dspublish command to publish the Key Recovery Agent certificate to Active Directory

Answer: Pending. Send your suggestion to feedback@testking.com.

QUESTION NO: 67
You are the network admin for contoso. The network consists of a single active directory domain named TestKing.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 deploy smart cards for all users in the domain. You want the members of a new group named Smartcard Agents to be able to issue smart cards for all users.

You create a new global group named Smartcard Agents. You install an Enterprise Certificate Authority (CA) on a Windows Server 2003 computer named Server1.

You create a duplicate of the enrollment agent certificate template and change the validity period of the new certificate template to three years.

The name of the new certificate template is SmartCard Enrollment. The configuration of the permission for the certificate template is shown in the exhibit.
*****MISSING**'**

You want to ensure that members of the Smartcard Agents group can request smartcard enrollment certificates. What should you do?

A. Assign the Smartcard Agents group the Allow Autoenroll permission for the Smartcard Enrollment certificate template
B. Add the enrollment agent certificate template to the list of superseded templates on the smartcard enrollment certificate template
C. Configure the enterprise CA to enable the Smartcard Enrollment certificate template
D. Configure the enterprise CA to assign the Certificate Managers to the Smartcard Agents Group
E. Instruct the members of the Smartcard Agents group to connect to the enterprise CA Web enrollment pages to request certificates

Answer: Pending. Send your suggestion to feedback@testking.com.

QUESTION NO: 68
D/D 1 You are the network admin for TestKing. The network consists of a single active directory domain named TestKing.com. All servers run windows server 2003 and clients run XP Pro.

You need to implement the capabilities and requirements in the following table for the users and computers:

Type of user or computer	Capability or requirement
Domain users	Smart card logon required for all users
Security global group	Ability to issue smart cards to all domain users
Human recourses servers	Certificate based IPSec encryption required for all data transmissions
VPN Server	L2TP Required

All client computers are portable computers and need to connect to the VPN servers and to the HR resource servers

You configure a PKI to support the domain users and computers. You need to specify which type of certificate, if any each type of user or computer requires

What should you do?

Answer:

QUESTION NO: 69
You are the network admin for TestKing. You need to test a new application.

The application requires 2 processors and 2 GB of RAM. The application also requires shared folders and installation of software on client computers.

You install the application on a Windows Server 2003 Web Edition computer and install the application on 20 test client computers.

You then discover that only some of the client computers can connect and run the application. You turn off some computers and discover that the computer that failed to open the application can now run the application. You need to identify the cause of the failure and update your test plan.

What should you do?

A. Increase the maximum number of worker processes to 20 for the default application pool
B. use add/remove programs to add the application server windows component
C. change the application pool to identity to local service for the default application pool
D. change the test server OS to Window Server 2003 Standard Edition or Enterprise

Answer: D
Explanation: Although Windows Server 2003 Web Edition supports up to 2GB of RAM, it reserves 1GB of it for the operating system; only 1GB of RAM is available for the application. Therefore, we need to install Window Server 2003 Standard Edition or Enterprise Edition to support enough RAM.

QUESTION NO: 70
You are the network administrator for Costos, Ltd. . The network contains a single Active Directory domain named Contoso.com. All computers on the network are members of the domain.

Contoso, Ltd. has a main office and 20 branch offices. Each branch office has a connection to the main office. Only the main office has a connection to the Internet.

You are planning a security update infrastructure for your network. You deploy a central Software Update Services (SUS) server at the main office and an SUS server at each branch office. The SUS server at the main office uses Windows Update to obtain security patches.

You want to minimize the amount of bandwidth used on the connection to the Internet and on the connection between the offices to download security patches.

Which two actions should you take?

A. Configure the SUS servers at the branch office to use Windows Update to obtain security patches.
B. Configure the SUS servers at the branch offices to use the central SUS server for updates.
C. Configure Automatic Updates on the SUS servers at the branch offices to use the central SUS server for updates.
D. Configure Automatic Updates on all computers to use the SUS server on the local network.
E. Configure Automatic Updates on all computers to use the default update service location.

Answer: B, D
Explanation: We must set up the SUS branch offices server to pickup the updates form the server in the main office. By configuring a SUS server in the main office you save network bandwidth, because the branch office servers will not need to use the internet connection. With this solution, the main office SUS server downloads the updates from Microsoft; the branch office SUS servers download the updates from the main office SUS server and the client computers download the updates from the local SUS server.

Incorrect Answers:
A: This is an unnecessary use of the internet connection.
C: You need to configure the SUS server software to download the updates, not automatic updates.
E: The default update service location is Microsoft. This is an unnecessary use of the internet connection.

QUESTION NO: 71
You are the network administrator for Contoso, Ltd. All servers run Windows Server 2003. All client computers run Windows XP Pro. All computers are connected to the network by using wireless access points.

You configure a CA. You require certificate based IEEE 802.1X authentication on the wire access point.

You need to enable all computers to communicate on the wireless network.

What are two possible ways to complete this task?

A. Enter a 128 bit WEP key on the wireless access point and on the computers
B. I(n the Wireless Network Connection properties on each computer, select the The key is provided for me automatically check box
C. Temporarily connect each computer to an available Ethernet port on the wireless access point and install a computer certificate
D. Install a computer certificate on each computer by using a floppy

Answers: A, B

QUESTION NO: 72
You are the systems engineer for Contoso, Ltd.. The network consists of a single Active Directory domain named Contoso.com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

The servers on the network are located in a physically secured room, which is located in a central data center building on the company campus. All servers have the Recovery Console installed and support firmware-based console redirection by means of their serial ports, which are connected to a terminal concentrator. The terminal concentrator is connected to the company network by means of a standard LAN connection.

It is required that all servers can be managed remotely. All IT staff in the company can establish connections to the servers by means of either a Remote Desktop connection or the Windows Server 2003 Administration Tools, which are installed locally on their client computers.

Company management now requires that several servers that have high-availability requirements must also be remotely managed in the event of system failures and when the Recovery Console is used.

Company management also requires that these servers can be remotely managed when the servers are slow or are not responding to normal network requests. You need to plan a remote management solution that complies with the new requirements. What should you do?

A. On each highly available server, enable Emergency Management Services by adding the Redirect=COM1 and /redirect parameters to the Boot.ini file on each server and the EMSPort=COM1 and EMSBaudRate=9600 parameters to the Winnt.sif file on each server.
B. On each highly available server, configure the Telnet service with a startup parameter of Automatic. Set the number of maximum Telnet connections to match the number of administrators in the company. Add the administrator's user accounts to the TelnetClients security group.
C. Install IIS on each highly available server. Select the Remote Administration (HTML) check box in the properties for the World Wide Web Service. Add the administrator's user accounts to the HelpServicesGroup security group.
D. Use the netsh command to create an offline configuration script that contains the network parameters for outof-band remote management. Copy this script to the C:\Cmdcons folder on each highly available server.

Answer: A

To enable Emergency Management Services after setting up a Windows Server 2003 operating system, you must edit the Boot.ini file to enable Windows loader console redirection and Special Administration Console (SAC). The Boot.ini file controls startup; it is located on the system partition root.

Unattend.txt and Winnt.sif files
These files are necessary in order to fully automate the process of installing Windows Server 2003 remotely. A sample Unattend.txt file is on the operating system CD. You can use default settings or customize your installations by modifying or adding parameters. When editing Unattend.txt files, insert the parameters in the **[Data]** section, as shown in the table, below.

[Data] Parameter	Possible Values
EMSPort={com1|com2|usebiossettings}	**Com*x*** (where *x* specifies serial port 1 or 2). This option is valid for x86-based systems only.
	UseBIOSSettings. This instructs the operating system to detect firmware that supports Emergency Management Services and uses SPCR settings. If an SPCR table is not present, Emergency Management Services is not enabled. This is the default setting for Advanced Configuration and Power Interface (ACPI) systems.
EMSBaudRate=*value*	9600 baud is the default, with other values of 19200, 57600, and 115200 possible, depending on the capabilities of the serial port. This must be used with **EMSPort=**, or the parameter is ignored.

QUESTION NO: 73
You are a network administrator for TestKing. The company has a main office and one branch office. The network consists of a single active directory domain named TestKing.com. All servers run windows server 2003

The company needs to connect the main office network and the branch office network by using RRAS servers at each office the networks will be connected by a VPN connection over the internet.

The company's written security policy includes the following requirements for VPN connections over the internet:

- **All data must be encrypted with end to end encryption**
- **VPN connection authentication must be at the computer level**
- **Credential information must not be transmitted over the internet as part of the authentication process.**

You need to configure security for VPN connections between the main office and the branch office. You need to comply with the written policy.

What should you do?

A. use a PPTP connection with EAP-TLS authentication
B. use a PPTP connection with MS-CHAP v2 authentication
C. Use an L2TP connection with EAP-TLS authentication
D. Use an L2TP connection with MS-CHAP v2 authentication

Answer: C
Explanation: Strictly speaking, this answer is incomplete, because it doesn't mention IPSec. For computer level authentication, we must use L2TP/IPSec connections.
To establish an IPSec security association, the VPN client and the VPN server use the Internet Key Exchange (IKE) protocol to exchange either computer certificates or a preshared key. In either case, the VPN client and server authenticate each other at the computer level. Computer certificate authentication is highly recommended, as it is a much stronger authentication method. Computer-level authentication is only done for L2TP/IPSec connections.

Incorrect Answers:
A: PPTP uses user-level authentication over PPP. The question states that computer-level authentication is required; therefore we must use L2TP/IPSEC.
B: PPTP uses user-level authentication over PPP. The question states that computer-level authentication is required; therefore we must use L2TP/IPSEC.
D: For computer certificate authentication, we must use EAP-TLS, not MS-CHAP v2.

QUESTION NO: 74
You are the systems engineer for TestKing. TestKing has 20,000 users in a large campus environment located in London. Each department in the company is located in its own building. Each department has its own IT staff.

The company's network is divided into several IP subnets that are connected to one another by using dedicated routers. Each building on the company's main campus contains at least one subnet, and possibly up to five subnets. Each building has at least one router. All routers use RIP v2 broadcasts.

A new office in Dortmund has 25 users. Dortmund is connected to the main office with a Frame Relay line. Dortmund installs a server with RRAS and implements RIP v2.

Later the Dortmund admin reports that his router is not receiving routing table updates from the routers at the main office. He must manually add routing entries to the routing table to enable connectivity between the locations. You investigate and discover that the RIPv2 broadcasts are not being received at the Dortmund office. You also discover that no routing table announcements from the Dortmund office are being received at the main office.

You need to ensure that the network in the Dortmund office can communicate with the main campus network and can send and receive automatic routing table updates as network conditions change.

What should you do to the router in the Dortmund office?

A. Configure the router to use RIPv1 broadcasts
B. Configure the router to use auto-static update mode
C. Add the IP address ranges of the main campus network to the routers accept list and announce list
D. Add the IP addresses of the main campus routers to the router's neighbors list

Answer: D
Explanation: It looks like the Dortmund router is configured to use neighbors. Therefore, we need to add the IP addresses of the main campus routers to the router's neighbour's list.

QUESTION NO: 75
You are the network admin for TestKing. All servers run Windows Server 2003.

Every week, you run the mbsacli.exe /hf command to ensure that all servers have the latest critical updates installed. You run the mbsaclie.exe /hf command from a server named server1.

When you scan a server named TestKingB you receive the following error message stating Error 200, System not found, Scan failed.

When you ping TestKingB you receive a reply.

You need to ensure that you can scan TestKingB by using the mbsacli.exe /hf.

What should you do?

A. Copy the latest version of the Mssecure.xml to the program files\microsoft baseline security analyzer folder on server1
B. Ensure that the Server service is running on TestKingB
C. Install IIS common files on Server1
D. Install the latest version of IE on TestKingB

Answer: B
Explanation: From Microsoft: Error: 200 - System not found. Scan not performed.
This error message indicates that mbsacli /hf did not locate the specified computer and did not scan it. To resolve this error, verify that this computer is on the network and that the host name and IP address are correct. We know that the computer is on the network because we can successfully ping it. Therefore, the cause of the problem must be that the Server service isn't running.

Incorrect Answers:

A: We can successfully scan other computers from Server1. Therefore, the problem is unlikely to be with Server1.
C: We can successfully scan other computers from Server1. Therefore, the problem is unlikely to be with Server1.
D: The version of IE that comes with Windows Server 2003 is sufficient, and therefore does not need to be upgraded.

Reference:
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q303/2/15.asp&NoWebContent=1

QUESTION NO: 76
You are the network administrator for TestKing. The network consists of a single active directory domain named TestKing.com. All servers run Windows Server 2003. A server named TestKing2 functions as the mail server for the company. All users use Microsoft Outlook Express as their email client.

An update to the company's written security policy specifies that users must use encrypted authentication while they are retrieving email messages from TestKing2

You need to comply with the updated policy. What should you do? (Choose three)

A. Configure the POP3 service on TestKing2 to use Active Directory Integrated Authentication
B. Configure the SMTP virtual server on TestKing2 to use Integrated Windows Authentication
C. Configure Outlook Express to use the Secure Password Authentication (SPA)
D. Configure the SMTP virtual server on TestKing2 to use Basic Authentication with Transport Layer Security (TLS) encryption
E. Configure the POP3 service on TestKing2 to require secure password authentication (SPA for all connections

Answers: A, C, E
Explanation: You can use Active Directory Authentication to incorporate the POP3 service into your existing Active Directory domain. Active Directory integrated authentication supports both plaintext and Secure Password Authentication (SPA) e-mail client authentication. Because plaintext transmits the user's credentials in an unsecured, unencrypted format, however, the use of plaintext authentication is not recommended. SPA does require e-mail clients to transmit both the user name and password using secure authentication; it is therefore recommended over plaintext authentication.
We need to configure the POP3 service on TestKing2 to require secure password authentication, and we need to configure the email clients to use Secure Password Authentication (SPA).

Incorrect Answers:
B: We need to configure the POP3 service, not the SMTP virtual server.
D: We need to configure the POP3 service, not the SMTP virtual server.

QUESTION NO: 77
You are the network admin for TestKing. Your network contains 50 application servers that run Windows Server 2003.

The security configuration of the application servers is not uniform. The application servers were deployed by local administrators who configured the setting for each of the application servers differently based on their knowledge and skill. The application servers are configured with different authentication methods, audit settings and account policy settings.

The security team recently completed a new network security design. The design includes a baseline configuration for security settings on all servers. The baseline security settings use the hisecws.inf predefined security template. The design also requires modified settings for servers in an application server role. These settings include system service startup requirements, renaming the administrator account, and more stringent account lockout policies. The security team created a security template named application.inf that contains the required settings.

You need to plan the deployment of the new security design. You need to ensure that all security settings for the application servers are standardized, and that after the deployment, the security settings on all application servers meet the design requirements. What should you do?

A. Apply the setup security.inf template first, the hisecws.inf template next, and then the application.inf template
B. Apply the Application.inf template and then the Hisecws.inf template.
C. Apply the Application.inf template first, then setup.inf template next, and then the hisecws.inf template
D. Apply the Setup.inf template and then the application.inf template

Answer: A.
Explanation: The servers currently have different security settings. Before applying our modified settings, we should reconfigure the servers with their default settings. This is what the security.inf template does. Now that our servers have the default settings, we can apply our baseline settings specified in the hisecws.inf template. Now we can apply our custom settings using the application.inf template.

Incorrect Answers:
B: The hisecws.inf template would overwrite the custom application.inf template.
C: Same as answer A. Also, the setup.inf security template doesn't exist. To return a system to its default security settings, we use the security.inf template.

D: The setup.inf security template doesn't exist. To return a system to its default security settings, we use the security.inf template.

QUESTION NO: 78
You are the network administrator for TestKing's Active Directory domain. TestKing's written security policy was updated and now requires a minimum of NTLM v2 for LAN manager authentication.

You need to identify which Operating Systems on your network do not meet the new requirement

Which OS would require an upgrade to the OS or software to meet the requirement?

A. Windows 2000 Professional
B. Windows Server 2003
C. Windows XP Professional
D. Windows NT Workstation with service pack 5
E. Windows 95

Answer: E.
Explanation: Windows 95 does not natively support NTLM v2 authentication. To enable it, you would need to install the Directory Services Client software.

QUESTION NO: 79
TestKing has a single active directory domain named TestKing.com.

The company's written security policy requires that computers in a file server role must have a minimum file size for event log settings. In the past, logged events were lost because the size of the event log files was too small. You want to ensure that the event log files are large enough to hold history. You also want the security event log to be cleared manually to ensure that no security information is lost. The application log must clear events as needed.

You create a security template named fileserver.inf to meet the requirements. You need to test each file server and take the appropriate corrective action if needed. You audit a file server by using fileserver.inf and receive the resules shown in the exhibit.
*****MISSING*****

You want to make only the changes that are required to meet the requirements. Which two actions should you take?

A. Correct the maximum application log size setting on the file server

B. Correct the maximum security log size setting on the file server
C. Correct the maximum system log size setting on the file server
D. Correct the retention method for application log setting on the file server
E. Correct the retention method for the security log setting on the file server
F. Correct the retention method for the system log setting for the file server

Answers: Pending. Send your suggestion to feedback@testking.com.

QUESTION NO: 80
You are the network administrator for TestKing. The network contains Window Server 2003 servers configured in a 4 node server cluster.

The cluster provides file services to 5,000 users and contains several terabytes of datafiles. Several thousand shared folders have been created on 16 virtual server groups by using dynamic File Share cluster resources. Many data files are updated, created, or deleted each day.

You need to create a backup strategy for both user data and the cluster configuration. You need to ensure that your strategy limits the potential loss of data and the cluster configuration to one week and provides the quickest means of recovery. What should you do?

A. Perform a weekly ASR of the cluster node that owns the quorum resource. Perform a weekly backup of all data files to tape.
B. Perform a weekly ASR of every node in the cluster. Perform a weekly backup of all data files to tape
C. Perform a weekly ASR on each cluster node that currently owns cluster groups containing data files
D. Configure daily shadow copies of all volumes on cluster nodes
E. Configure weekly shadow copies of all volumes on all cluster nodes

Answer: Pending. Send your suggestion to feedback@testking.com.

QUESTION NO: 81
Your network contains a Windows Server 2003 computer named TestKingC. TestKingC has a single CPU, 512 MB of RAM, and a single 100MB network adapter.

All network user's home folders are stored on TestKingC. Users access their home folders by using a mapped network drive that connects to a shared folder on TestKingC

After several weeks, users report that accessing home folders on TestKingC is extremely slow at certain times during the day. You need to identify the resources bottleneck that is causing the poor performance.

What should you do?

A. Capture a counter log by using LogicalDisk, PhysicalDisk, Processor, Memory and Network Interface performance objects and view the log data information that is captured during period of poor performance
B. Configure alerts on TestKingC to log entries in the event logs for the LogicalDisk, PhysicalDisk, Processor, Memory and Network Interface performance objects when the value of any object is more than 90
C. Capture a trace log that captures Page faults, File details, Network TCP/IP, and Process creations/deletions events
D. Implement Auditing on the folder that contains the user's home folders. Configure Network Monitor on TestKingC

Answer: A
Explanation: The problem is most likely to be caused by a hardware bottleneck. This could be a disk problem or a problem with the processor, RAM or network card. We can monitor these hardware resources by using a System Monitor counter log. The Windows Performance tool is composed of two parts: System Monitor and Performance Logs and Alerts. With System Monitor, you can collect and view real-time data about memory, disk, processor, network, and other activity in graph, histogram, or report form. The output from the counter log will show us which hardware resource in unable to cope with the load and needs to be upgraded or replaced.

Incorrect Answers:
B: We cannot use a generic value of 90 for the different hardware resources because different hardware resources have different acceptable performance counters.
C: We need to monitor the hardware resources listed in answer A, not the software resources listed in this answer.
D: The problem is most likely to be caused by a hardware bottleneck. Auditing and network monitoring won't give us any useful information about the hardware.

QUESTION NO: 82
Your network consists of a single Active Directory domain. TestKing has a main office in Denver and branch offices in Paris and Bogota. Each branch office contains a Windows Server 2003 DC. All client computers run Windows XP Professional.

Users in the Bogota office report intermittent problems authenticating to the domain. You suspect that a specific client computer is causing the problem.

You need to capture the authentication event details on the domain controller in the Bogota office so that you can find out the IP address of the client computer that is the source of the problem.

What should you do?

A. Configure System Monitor to monitor authentication events
B. Configure Performance Logs and Alerts with a counter log to record the authentication events
C. Configure Network Monitor to recorded the authentication events
D. Configure Performance Logs and Alerts with an alert to trigger on authentication events

Answer: Pending. Send your suggestion to feedback@testking.com.

QUESTION NO: 83
You have just installed two Windows Server 2003 computers. You configure the servers as a two node server cluster. You install WINS on each Node of the cluster. You create a new virtual server to support WINS.

You create a new cluster group named WINSgroup. When you attempt to create the Network Name resource, you receive an error message. You need to make the proper changes to the cluster to complete the installation of WINS.

What should you do?

A. Create a Generic Service resource in the WINSgroup cluster group
B. Configure the network priorities for the cluster
C. Create an IP address resource in the WINSgroup cluster group
D. Add the proper DNS name for the WINS Server in the DNS database

Answer: C
Explanation: You need to create an IP address resource before you can create the network name resource.

Name	State	Owner	Group	Resource Type
Disk Q:	Online		Cluster Group	Physical Disk
Disk R:	Online		RightFax Group	Physical Disk
Cluster IP Address	Online		RightFax Group	IP Address
Cluster Name	Online		RightFax Group	Network Name

QUESTION NO: 84
TestKing uses WINS and DNS for name resolution. The LMHosts and Hosts files are not used.

A user Tess on a server named TestKing2 reports that when she runs a script to transfer files to a server named TestKing5, she receives the following error stating "Unknown Host TestKing5"

You use TestKing2 to troubleshoot the problem. The results of your troubleshooting show that the nslookup utility replies with an address of 192.168.1.8. When you try to ping TestKing5, the reply times out and shows a different IP address.

You need to allow Tess on TestKing2 to use the script on TestKing5.

What should you do?

A. Re register TestKing5 with WINS
B. On TestKing5 run the ipconfig /registerdns command
C. On TestKing2 run the ipconfig /flushdns command
D. On TestKing2, purge and reload the remote NetBIOS cache name table

Answer: A
Explanation: The nslookup utility replies with an address of 192.168.1.8. This is probably the correct address. When you ping TestKing5, it times out and shows a different IP address. This is an incorrect address that was resolved using a WINS lookup. As the address in the WINS database is wrong, we need to re-register TestKing5 with WINS.

Incorrect Answers:
B: The address of TestKing5 stored in DNS is likely to be correct, so it doesn't need to be re-registered.
C: Nslookup returns an address of TestKing5 that is likely to be correct. We know this because the ping test fails with a different IP address. Therefore, the locally cached IP address is likely to be correct, so the cache doesn't need to be cleared.
D: We would need to purge the local NetBIOS name cache, not the remote cache.

QUESTION NO: 85
You are the network administrator for TestKing. There is a single active directory domain named TestKing.com. All computers on the network are members of the domain. All domain controllers run Windows Server 2003.

You are planning a Public Key Infrastructure (PKI). The PKI design documents for TestKing specify that certificates that users request to encrypt files must have a validity period of two years.

The validity period of the Basic EFS certificate is one year. In the certificates Templates console, you attempt to change the validity period for the Basic EFS certificate template. However, the console does not allow you to change the value.

You need to ensure that you can change the value of the validity period of the certificate that users request to encrypt files. What should you do?

A. Install an enterprise CA in each domain.
B. Assign the Domain Admins group the Allow Full control permission for the Basic EFS certificate Template
C. Create a duplicate of the basic EFS certificate template. Enable the new template for issuing certificate authorities
D. Instruct users to connect to the CA Web Enrolment pages to request a Basic EFS certificate.

Answer: C
Explanation: The question states that the validity period of the Basic EFS certificate is one year. This suggests that we are using a standalone CA (the default validity period for an enterprise CA is two years). We cannot change the validity period of the Basic EFS template. We can however, make a copy of the Basic EFS template. This would enable us to make changes to the copy of the template.

Incorrect Answers:
A: The default validity period for an enterprise CA is two years. This would satisfy the requirement that the certificates have a validity period of two years. However, it does not satisfy the requirement that "you need to ensure that you can change the value of the validity period of the certificate that users request to encrypt files". Therefore, answer C is a better solution.
B: This is not a permissions issue. We cannot change the values in the template because they are hardcoded into the templates.
D: We need to edit the template before the users receive the certificates.

Reference: http://support.microsoft.com/?id=254632

www.testking.com